SELINUS UNIVERSITY
BUSINESS SCHOOL

Optimizing Ethical Dimensions in Banking Compliance and Cybersecurity for Digital Currency

By Issiaka Dao

A DISSERTATION

Presented to the Department of
Financial & Computer Management
program at Selinus University Business School

Faculty of Business & Media
in fulfilment of the requirements
for the degree of Doctor of Business Administration in
Financial & Computer Management

2024

Table of Contents

Acknowledgements

I am deeply grateful for the support I received during this research, especially from my thesis supervisor, **Professor Salvatore Fava** who provided invaluable advices, guidance, and encouragements.

I'd like to offer my genuine thanks to my academic guides, **Dr. Irene Difalco and Dr. Adriana Nifosì,** for their significant contributions to this academic achievement and their invaluable assistance with administrative processes.

It is with immense pleasure that I dedicate this work, the culmination of my studies, as an expression of my deep gratitude to my **parents** and **family**.

Finally, I give thanks to Almighty GOD.

In loving memory of my revered Father

(An icon who has always been there for us)

En mémoire de mon vénéré Père

(Une icône qui a toujours été là pour nous)

Abstract

The digitalization of money is a significant moment in monetary history, whereby innovative technologies introduce the world to new forms of digital money, such as cryptocurrencies, stablecoins, and Central Bank Digital Currencies (CBDCs). These new emerging innovations are changing the shape of finance through new opportunities but also great ethical and cybersecurity concerns. This study addresses two key aspects of e-money ecosystems: banking compliance and cybersecurity. It aims to optimize ethical considerations within these frameworks by tackling challenges related to KYC protocol, AML, CFT, and cybersecurity resilience. Under comprehensive research, it investigates ethical approaches, conglomeration, and regulative compliance linked to online protections while using advanced fintech levels in the field. These findings underline the disruptive potential of blockchain and CBDC but emphasize that proactive ethical alignment is paramount to security and compliance. This research concludes by stating that sustained innovation and agility are required in order to ensure the continued credibility, transparency, and reliability of digital financial systems, given the continuously emerging threats and ever-changing landscape of financial technology.

List of Tables

List of Figures

List of Acronyms and Abbreviations

- ✓ **AI** – Artificial Intelligence
- ✓ **AML** – Anti-Money Laundering
- ✓ **AML/CFT** – Anti-Money Laundering and Combating the Financing of Terrorism
- ✓ **AML/FT** – Anti-Money Laundering and Financing of Terrorism
- ✓ **BCEAO** – Banque Centrale des États de l'Afrique de l'Ouest
- ✓ **BIS** – Bank for International Settlements
- ✓ **CBDC** – Central Bank Digital Currency
- ✓ **CDD** – Customer Due Diligence
- ✓ **CENTIF** – Cellule Nationale de Traitement des Informations Financières
- ✓ **CFA** – Communauté Financière Africaine Franc
- ✓ **CFT** – Combating the Financing of Terrorism
- ✓ **CPF** – Counter Proliferation Financing
- ✓ **DCEP** – Digital Currency Electronic Payment
- ✓ **ECOWAS** – Economic Community of West African States
- ✓ **EDD** – Enhanced Due Diligence
- ✓ **ESIF** – European Structural and Investment Funds
- ✓ **EU** – European Union
- ✓ **FATF** – Financial Action Task Force
- ✓ **GDPR** – General Data Protection Regulation
- ✓ **IMF** – International Monetary Fund
- ✓ **IOU** – "I Owe You," Promise to Pay
- ✓ **KYC** – Know Your Customer
- ✓ **MFA** – Multi-Factor Authentication
- ✓ **ML** – Machine Learning
- ✓ **MTN** – Mobile Telecommunications Network
- ✓ **OTP** – One-Time Password
- ✓ **PEP** – Politically Exposed Person
- ✓ **R&D** – Research and Development
- ✓ **SMPC** – Small and Medium-sized Payment Corporations
- ✓ **UEMOA** – Union Économique et Monétaire Ouest-Africaine
- ✓ **UN** – United Nations
- ✓ **UNSC** – United Nations Security Council
- ✓ **USA** – United States of America
- ✓ **USD** – United States Dollar
- ✓ **WAEMU** – West African Economic and Monetary Union
- ✓ **WAMZ** – West African Monetary Zone
- ✓ **WMD** – Weapons of Mass Destruction
- ✓ **ZKP** – Zero-Knowledge Proof

SECTION ONE: INTRODUCTION AND BACKGROUND

I. INTRODUCTION AND AIM OF STUDY

In this foundational chapter of the thesis titled "Optimizing Ethical Dimensions in Banking Compliance and Cybersecurity for Digital Currency (CBDC)," the reader learns about the expanding field of Cybersecurity for Digital Currencies (CBDCs) and the ethical challenges and opportunities that accompany it. The "Introduction" section leads the way, providing a preliminary overview of the world of digital currencies and their intersection with banking compliance and cybersecurity. Moving forward, the "Study Background" delves deeper into the evolution of digital currencies, particularly CBDCs, and the critical moments that make this study timely and relevant. The following section, "Research Rationale," outlines the urgency and importance of the investigation, highlighting the complexities surrounding ethical considerations in the CBDC landscape. The "Research Objectives" segment states the specific aims and purposes that the study intends to achieve, ensuring clarity of purpose for the

reader. Finally, the “Scope of the Study” delineates the boundaries, illustrating areas we will explore and what aspects it will not explore. Together, this chapter paints a holistic picture, setting the tone for the in-depth exploration that follows.

1.1. Introduction

For centuries, governments and their institutions held the exclusive right to issue banknotes and coins, ensuring their authenticity through legal enforcement. Money as a form of exchange is an IOU (promise to pay) that performs an important role in the society; it acts as a unit of account, a medium of exchange and a store of value. The physical form of fiat currency that we use currently has taken a long road to reach the place where it currently stands, from being an alternative to the barter system and to get evolved into multiple forms like coins, currency notes and cryptocurrencies[1]. The emergence of

[1] Blockchain for Industry 4.0 - Emergence, Challenges, and Opportunities. Edited by Anoop V. S., Asharaf S., Justin Goldston, and Samson Williams - Year 2023 – p216

commercial banks, notably coinciding with the Renaissance's advent of print technology, marked a paradigm where payment mechanisms largely rested upon paper. Checks became the populace's choice for transactions, while central banks took to circulating paper banknotes. However, as the 20th century progressed, a new era dawned. Electronic innovations revolutionized financial transactions, paving the way for wire transfers, ATMs, and the ubiquity of credit and debit cards. Amidst the whirlwind of the 2008 global financial crisis, another groundbreaking shift was on the horizon. 2007 heralded the age of smartphones with the introduction of the iPhone, an innovation that, as cited by Yamaoka[2], marked the beginning of a digital revolution. Subsequently, smartphones permeated global markets. Highlighting this, a 2017 World Bank Group survey revealed that of the 1.7 billion adults without banking amenities, an overwhelming 1.1 billion owned mobile devices.[3]

Internet and computing devices together made business and every aspect of life easier. The realm of monetary transactions has witnessed a transformative journey. From paper-based instruments, emblematic of state authority, to the intricate web of digital currencies, the financial landscape has continually evolved, mirroring technological and societal advancements. Global non-cash transactions reached 708.5 billion transactions in 2019, surged by 80% since 2014. Despite cash being the most used payment instrument in the world, technological innovation and new consumer preferences are radically transforming the way consumers pay and manage money[4].

Fast-changing events in virtual technologies have created fresh avenues that facilitate inclusion in the economy: mobile devices act as access channels to a range of payment services from third-party providers. The Internet of Things has inspired cryptocurrencies such as Bitcoin, which ensures an easily affordable and more uncomplicated way to engage in transactions. Innovations in concert with blockchain have further cemented the position of digital currencies, providing a stable platform upon which new economic behaviors, such as crowdfunding, can thrive. CBDCs have also emerged, which blend historic currency stability with the critical bank endorsement. While CBDCs could support an increase in financial inclusivity, this assumption has to be set against existing digital divides. Does the existing infrastructure support such inclusivity, and will all demographics be equally prepared for transition to digital currencies?

---

[2] Yamaoka, H. (2019). The Future of Financial Systems in the Digital Age: Perspectives from Europe and Japan by Markus Heckel, Franz Waldenberger – 2022 – p51

[3] 1.7 Billion People Don't Have a Bank Account But Mobile Banking Could Change Their Lives - August 9, 2021. https://www.brinknews.com/bridging-the-digital-divide-to-widen-financial-services-in-central-asia/

[4] The (Near) Future of Central Bank Digital Currencies Risks and Opportunities for the Global Economy and Society - Volume 7. Edited by Prof. Lorenzo Kamel, University of Turin's History Department, and Istituto Affari Internazionali (IAI)

Historically, central banks operated in two great monetary domains: public transaction-focused banknotes and central bank deposits designed for high-value interbank settlements. This dualism is replicated in the CBDC framework, distinguishing between general-purpose CBDCs for the masses and large-value CBDCs serving major interbank settlements. Digital currencies, as such, are just different electronic value mechanisms, from the very common gift cards to mobile vouchers. Within this spectrum, virtual currencies, distinct from traditional fiat currencies, chart their course. Cryptocurrencies, a subset of this domain, ride on the back of cryptographic protocols that render transactions possible without any central regulatory entity. Bitcoin, with its decentralized public ledger or blockchain, stood testimony to this revolution when it made its debut in 2008. Today, digital money offers an unparalleled level of convenience, catering to a whole slew of transactional needs across e-commerce and purchases at brick-and-mortar stores. While many hail it as a flag bearer of financial innovation, others view it as a leverage tool for geopolitics. Its rapid rise and intrinsic decentralization, however, give rise to the most serious ethical and security concerns, placing banks at the very center of such challenges. Regulatory bodies such as the Financial Action Task Force (FATF) have provided strong frameworks that deal with money laundering, terrorist financing, and proliferation of weapons of mass destruction. While countries worldwide have harmonized their laws with FATF's recommendations, the complex nature of the digital currency ecosystem poses unexpected issues.

Banks, on the other hand, placed in the role of guardians of financial activity, face multivariate challenges. The preservation of the integrity of the financial system requires compliance with regulatory requirements, including **Anti-Money Laundering** (AML), **Counter Financing of the Proliferation of Weapons of Mass Destruction** (CFT), **Counter-Proliferation Financing** (CPF), and **Know Your Customer** (KYC) regulations, and highly effective data protection measures. In the digital age, amidst rapidly moving targets of cyber threats, banks are busy fortifying their cybersecurity armor. Beyond this, they bear an ethical commitment to their clientele, prioritizing their welfare and ensuring their trust remains inviolable.

This thesis ventures into an in-depth analysis of the confluence of ethics, banking regulations, and cybersecurity within the CBDC milieu. It tries to tease out the challenges that banks face in navigating the complex waters of regulatory compliance with AML-CFT, cybersecurity, and ethical obligations in the realm of digital currency. In its discourse, it proposes ways through which the ethical dimensions of banking compliance may be furthered and CBDC cybersecurity safeguards fortified.

1.2. Research Questions

The confluence of digital currencies, especially CBDCs, with traditional banking gives rise to a complex web that interweaves technology, finance, ethics, and global geopolitics. Most of the existing research

has failed to provide a proper framework to understand the depth and breadth of these intertwined threads. With this in mind and in line with our approach, the following research questions were formulated:

1) **Regulatory Environment and CBDCs:**
   - ✓ How have global regulations been tailored to address the unique challenges and opportunities that CBDCs pose?
   - ✓ What are the ethical implications of these regulatory shifts with regard to financial equity and access?
2) **Cybersecurity and CBDCs:**
   - ✓ What unique cybersecurity threats arise for CBDCs, given their digitized nature?
   - ✓ How are these threats both challenging and refining the ethical standards of cybersecurity in the banking domain?
3) **Comparative Analysis of CBDCs:**
   - ✓ How do CBDCs from different national and regional central banks compare in terms of ethical considerations, compliance requirements, and cybersecurity measures?
   - ✓ What can be learned from the different approaches, successes, and challenges each CBDC presents?

This research tries to systematically answer these questions by exploring them diligently, with the aim of bringing to light the complex ethical landscape of CBDCs and providing a comprehensive understanding and roadmap for stakeholders from policymakers to financial professionals.

1.3. Background of the Study

The very fabric of monetary and financial systems has changed dramatically over time. From the tangible nature of coins and banknotes to the intangible digital forms of today's currencies, this change is in itself the confluence of both technological advancement and societal changes. In general, digital currencies started to gather attention with the development of Bitcoin in 2008, which is characterized as a ***decentralized currency***, *since there is no central authority to issue them* (Nakamoto, 2008). The market for cryptocurrency has, therefore, flourished over the years and is characterized by many players with their specific features and value propositions. Thus, state central banks have also embarked on the digital race by launching CBDCs. While these decentralized digital currencies gained traction, they also highlighted issues related to volatility, regulatory concerns, and security vulnerabilities[5].

[5] Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system.

CBDCs could dominate the digital transaction sphere, bringing transformative impacts to the global financial landscape. CBDCs are digital monetary instruments issued and backed by central banks, embodying key functions like a medium of exchange, store of value, and unit of account. Unlike the general public, which primarily holds physical cash, only select financial entities can currently hold central bank reserves. However, CBDCs offer a digital fiat currency solution that could become widely adopted across individuals and institutions, especially in a world trending towards cashless economies. As defined by Kiff et al. (2020), CBDCs represent the digital version of a country's standard money, marked as a liability on its central bank's balance sheet[6].

However, like any type of currency, CBDCs have characteristics that would suggest that they would be an opportunity for money launderers. Money laundering is fundamentally a three-stage process comprising placement, layering, and integration. ***Placement*** involves introducing cash into the financial system. ***Layering*** involves somehow disguising the true origins of the proceeds of crime to mislead law enforcement and regulators. ***Integration*** is where the criminal(s) acquires wealth generated from what appears to be a legitimate source. Converting fiat money or valuable objects into cryptocurrency is the placement stage and stage allowing criminal to hide origin of the money.

Additionally, money laundering has been constrained by physical limitations; it is difficult to transmit an illicit volume of cash without it getting stolen or noticed, especially when crossing international borders. A standard pallet piled with cash “typically contains 640,000 bills” (Hellerstein and Ryan, 2011); denominated in USD 20 bills, it amounts to USD 12.8 million, certainly not the easiest cargo to conceal or transport. Cryptocurrency, in contrast, lives in the digital ether, making it hard to trace and easy to move. Money laundering via cryptocurrency is a relatively modern area of financial crime; foundationally, there is a requirement to translate value from the physical word, like diamonds or dollars, into something fungible in the digital ecosystem.

This study is an analysis of cash-to-crypto methodologies, exploring the number of opportunities a criminal actor could use to bypass AML, CFT, CPF, and KYC regulations with variable levels of effectiveness. While there are a number of individual methods of bypassing regulations and cybersecurity aspects, a diversified strategy using multiple methods would be the most resilient and

[6] Central Bank Digital Currencies and the Global Financial System - Theory and Practice - by Muhammad Ashfaq, Rashedul Hasan, Jost Mercon. Edition © 2023 Walter de Gruyter GmbH, Berlin/Boston

fault-tolerant process for criminals with large volumes of cash. Thus, it is even more important for automated compliance and fraud prevention to be employed in the fight against criminal actors [7].
There are three main cyber payment typologies. The first is **Internet payment services**, such as mobile payments, micro payments, or digital precious metals; the second is **store value cards and smart cards**; and the third is **online banking** (Nathalie Rébé – 2023). Criminals can easily disguise their transactions, send Bitcoins anywhere, convert them into cash, and deposit them in banks. With all innovations, this digital financial renaissance presented its own set of challenges. While the potential of digital currencies, especially their ability to democratize financial transactions, was undeniable, it was also fraught with ethical dilemmas, security concerns, and regulatory ambiguities. Banks, the erstwhile custodians of financial systems, found themselves navigating a rapidly evolving landscape, balancing traditional fiduciary responsibilities with new-age challenges.

This study seeks to delve into the intricate tapestry of digital currencies, exploring their historical trajectory, current state, and potential future, especially in relation to their cybersecurity, interactions with banking systems, regulatory frameworks, and the overarching philosophy of financial transactions.

1.4. Rationale and Objectives for Research

One of the most pressing concerns highlighted is the digital nature of CBDCs. Being exclusively digital means these currencies operate in a realm that is vast, decentralized in many aspects, and riddled with technological nuances. Such a landscape inherently poses compliance challenges, ranging from transaction traceability, ensuring cross-border transactional compliance, to the prevention of illicit financial activities. Furthermore, the growing sophistication of cyber threats presents a considerable challenge. As global financial systems have seen, cyber-attacks are not limited to mere data breaches; they have the potential to disrupt entire financial ecosystems, lead to significant economic losses, and erode trust in financial systems. CBDCs, while harnessing the power of blockchain and cryptographic technologies, are not immune to these threats. Their decentralized nature, while a strength in many aspects, can also be a point of vulnerability if not appropriately safeguarded.

The aim of this paper is to chart a holistic way forward amidst these intertwined challenges. More

[7] Cyber-laundering : international policies and practices / edited by Nathalie Rébé - 2023
Names: Rébé, Nathalie, editor.
Description: Hackensack, New Jersey : World Scientific, [2023] - Copyright © 2023 by World Scientific Publishing Europe Ltd.

important than the challenges themselves is to devise and propose mechanisms that can make CBDCs operate within strong compliance frameworks by designing systems to ensure adherence to domestic and international financial regulations, guaranteeing transparency and increasing trust among users. In that respect, it could be said that for Central Banks in innovative and pioneering ways-trying to keep ahead of the pack-such currencies are becoming irreducible. While they represent a synthesis of traditional banking ethos with state-of-the-art digital technology, challenges in these converging domains remain considerable, in particular in the realms of compliance, cybersecurity, and ethical considerations.

1) **Emergence and Importance of CBDC:** While the digital revolution continues to flood the financial sector, the concept of CBDC has emerged of late as a potentially game-changing innovation. Ashfaq, Hasan, and Mercon's exhaustive exploration in "CBDCs and the Global Financial System - Theory and Practice" traces deep into the origins, development, and future trajectory of CBDCs (Ashfaq et al., 2023) [8]. The authors, in their deep analyses, explain at length the transformative possibilities of CBDCs, emphasizing how far they can reshape global financial dynamics. From the depth of their examination emerges the urgent and imperative need for political leaders, specialists in finance, and technologists alike to understand this new money format and the very many-faceted challenges it entails, in their quest to easily integrate it into the global financial infrastructure.

2) **Ethical Dimensions in Banking with CBDCs:** The world of finance is going increasingly digital in the future, where ethical consideration assumes center stage as perhaps one of those facets which is very relevant and is often blurred by the charm of technological advancements. Bilotta and Botti make an attempt to outline the ethical dimensions of the CBDC in their work "The (Near) Future of CBDCs". They highlight that the seamless integration of CBDCs into the banking sector isn't merely a technical challenge but also an ethical imperative (Bilotta & Botti, 2021)[9]. As emphasized, CBDC smooth integration into banking practices imposes much not only from an engineering perspective, but even a moral duty since Bilotta and Botti trace that issues that a digital currency system will naturally build around it raises problems concerning:

---

[8] Central Bank Digital Currencies and the Global Financial System - Theory and Practice - by Muhammad Ashfaq, Rashedul Hasan, Jost Mercon. Edition © 2023 Walter de Gruyter GmbH, Berlin/Boston

[9] The (Near) Future of Central Bank Digital Currencies - Risks and Opportunities for the Global Economy and Society. by Nicola Bilotta and Fabrizio Botti (eds)

privacy, access, and choice in respect to data security and, correspondingly call for a comprehensively integral concept of compliance with rules and cybersecurity aspects. Because CBDCs have the potential to reshape the global financial landscape, it is important that this be done in a manner that meets ethical standards and furthers principles of fairness, transparency, and inclusivity.

3) **Cybersecurity Implications for CBDCs:** Digital transformations at this time will no doubt bring fresh challenges to cybersecurity for CBDCs. Bindseil and Fotia, in their "Introduction to Central Banking", although providing a historical perspective, implicitly draw attention to the ever-evolving nature of banking systems and the continuous need for robust security mechanisms (Bindseil & Fotia)[10]. As CBDCs bridge the gap between traditional practices of banking and modern-day digital operations, so does the need for high-level cybersecurity measures increase. This, in turn, means that while we enter this modern phase of currency, the banking system needs to be properly fitted with the most state-of-the-art cybersecurity to secure not only the monetary value but the general public's confidence in this new system.

4) **Compliance and Cybersecurity in CBDCs:** The operation of regulatory compliance and cybersecurity in CBDCs goes along with their rising prominence. Bilotta and Botti emphasize the risks and opportunities of CBDCs, hinting towards the crucial need for optimized compliance in the financial sector (Bilotta & Botti, 2021)[8]. Ashfaq et Al. also lay the groundwork that elucidates the transformative capacity of CBDCs and the potential regulatory challenges (Ashfaq et al., 2023)[9]. It is, therefore, a matter of carving out the way in which banking compliance, led by ethics, in concert with cybersecurity, works in protecting, regulating, and enhancing the CBDC ecosystem on a strong framework for the future of digital finance.

The development of CBDC to mainstream financial flows has opened a whole set of challenges that come with equally great opportunities. More importantly, many of us can elaborate further on how an increasingly complex area is the compliance environment in which CBDC will need to interact. Because their nature is genuinely digital, new CBDC is entering into some of the most breathtakingly fast advances in technology as well as several regulatory environments currently in different nations.

Above all, perhaps, there is growing concern over various cyber threats perpetually shifting sand. In addition, our research will be channeled to the cybersecurity aspect: developing protocols and best practices that secure CBDC transactions, infrastructure, and users. This would involve a careful study

[10] Introduction to Central Banking by Ulrich Bindseil · Alessio Fotia - Edited by Springer

of the existing cybersecurity frameworks, understanding their strengths and vulnerabilities, and tailoring solutions that cater specifically to the unique nature of CBDCs.

This section of the research, therefore, seeks to ensure that CBDCs are introduced into our financial future in a secure and compliant method, inspiring confidence in all stakeholders.

1.5. Scope of the Study

The core interest of this study, therefore, goes toward the exploration, analysis, and investigation of ethical dimensions concerning banking compliance and cybersecurity, particularly with respect to CBDCs. This is done in view of crediting difficulties that have been encountered, identifying best practices, and proposing optimizations that stand up to both operational efficiency and moral robustness. To be sure that this study covers what it claims to deal with and captures all that it is supposed to address comprehensively, its scope was then defined, based on the following parameters:

1) **Geographic Scope:**

   The present study adopts an international perspective. Inasmuch as CBDC adoption has a worldwide bearing, all major financial global hubs, whose central banks have so far introduced or attained either advanced stages of piloting or studying its adoption, have been considered. However, of interest to us is an African story and thus the WAEMU zone (UEMOA). The same vein, other major markets that remain in our factor analysis include the US, EU, and China to highlight the correct trajectories in fast-growing emerging economies. This work methodology ensures exhaustive comprehension of various regional and worldly dynamics.

2) **Technological Framework:**

   The research focuses on distributed ledger technologies deployed or proposed with regard to the implementation of CBDC with a regard on the modern blockchain. The legacy systems and non-DLT-based digital currencies are not covered by this study.

3) **Ethical Domains:**

   - **Transparency and Accountability:** The transparency of transactions, data storage, and decision-making mechanisms within the banking compliance mechanism.
   - **Privacy and Confidentiality:** How user data is collected, stored, and distributed, and also how these practices respect or violate the users' data protection and privacy rights.
   - **Equity and Fairness:** To what extent does the deployment of CBDCs ensure equity and justice, including by taking into account underserved communities.
   - **Security and Trust:** Discussing what moral lessons may be identified in potential vulnerabilities and responsibilities that may be imposed on a central bank for the

assurance of trust in the digital economy.

4) **Stakeholders:**

The major stakeholders on which the study will focus include:

- The commercial banks & financial institutions
- The CBDC end-users
- The cybersecurity solution providers
- The Central Banks or regulatory bodies

5) **Methodological Framework:**

In the mixed approach, qualitative information from expert interviews and quantitative data from users surveyed via an online form, data and CBDC cybersecurity documentation and reports will be used.

6) **Time Frame:**

The research will analyze data and developments in the domain of CBDCs for the period of 2008-2024. The period will be updated, if required.

7) **Exclusions:**

Our research does not detail the technology of CBDCs or cryptographic techniques used in particular. It does not address the ethical issues of other digital tokens than CBDCs, such as cryptocurrencies. There is relatively less focus on the central banks of emerging markets or central banks that are in the early phases of researching CBDCs.

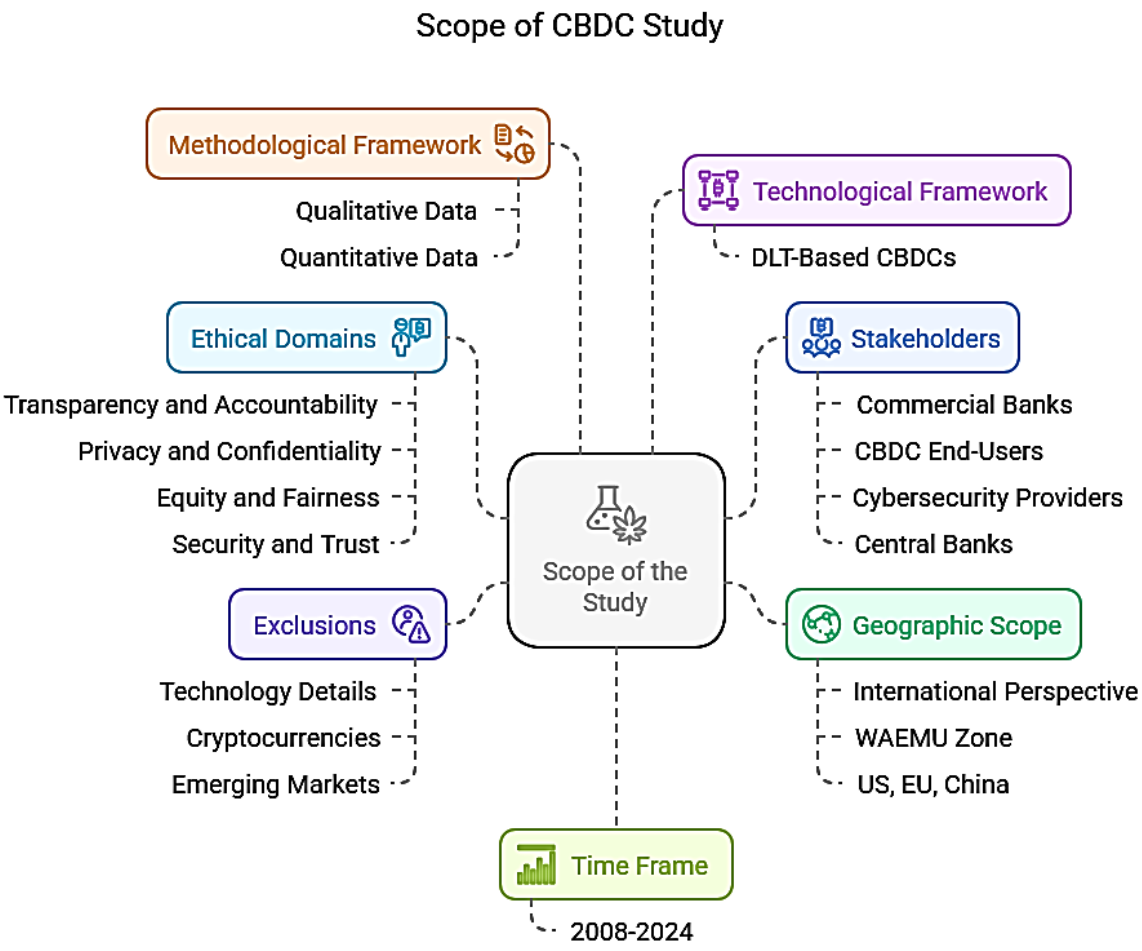


Figure 1: Scope of the Study

II. RELATED LITERATURE REVIEW

The landscape of digital currencies, particularly CBDCs, has undergone rapid evolution and has been the subject of extensive academic and industry research. To lay a solid foundation for our study, it is crucial to dig into the existing literature to understand the current state of knowledge and identify the gaps that this research aims to fill.

We then look at the development of modern banking products and services and explore how technology has come to play such an important role in modern-day banking. We shall ends with a review of the current state of banking. We have also discovered and it became apparent to us that what is accepted as historical fact is sometimes not correct, and sometimes there are conflicting or unsubstantiated claims for being the first to have done something. We have therefore provided extensive references in this chapter II and in some cases, we have qualified what we have written. There remains the risk that we have missed the actual first instance of a banking product or service because it isn't documented or because there were no references to it in the materials, we consulted[11].

By the end of this literature review, reader should have a robust understanding of the current landscape of CBDCs, the challenges and opportunities they present, and the areas that this thesis specifically aims to address.

2.1. Historical Overview of Digital Currencies, Including CBDCs

2.1.1. Evolution and Development of Banking

i. Emergence of Banking

"The Handbook of Banking Technology" by Tim Walker and Lucian Morris presents a story that takes us back thousands of years, closely linked to the need for economic and commercial interactions of early civilizations.

In the kingdoms of ancient Babylon, around 2000 BCE, we find not only the seeds but also the germination of the banking system in its nascent form. It is fascinating to consider how the majestic temples of this era, renowned for their spiritual significance, simultaneously

[11] The Handbook of Banking Technology by TIMWALKER and LUCIAN MORRIS. Edition Wiley
This edition first published 2021. © 2021 Tim Walker and Lucian Morris. Registered office. John Wiley & Sons Ltd, The Atrium, Southern Gate, Chichester, West Sussex, PO19 8SQ, United Kingdom

functioned as a nucleus of financial activity. These temples transcended their religious roles, becoming guardians of wealth, protecting not only grains and goods, but eventually evolving to store more valuable assets like precious metals. This pivotal instant marked the genesis of what we recognize today as the organized banking system – a multifaceted institution central to our economic infrastructure.

Looking to the classical civilizations of Greece and Egypt, we discover a dynamic expansion and sophistication of banking practices. The dynamic maritime trade of the great Greek cities required more sophisticated financial services. Foreign exchange, loans, and even maritime loans became commonplace, meeting the nuanced needs of traders and merchants sailing the high waters of the Mediterranean.

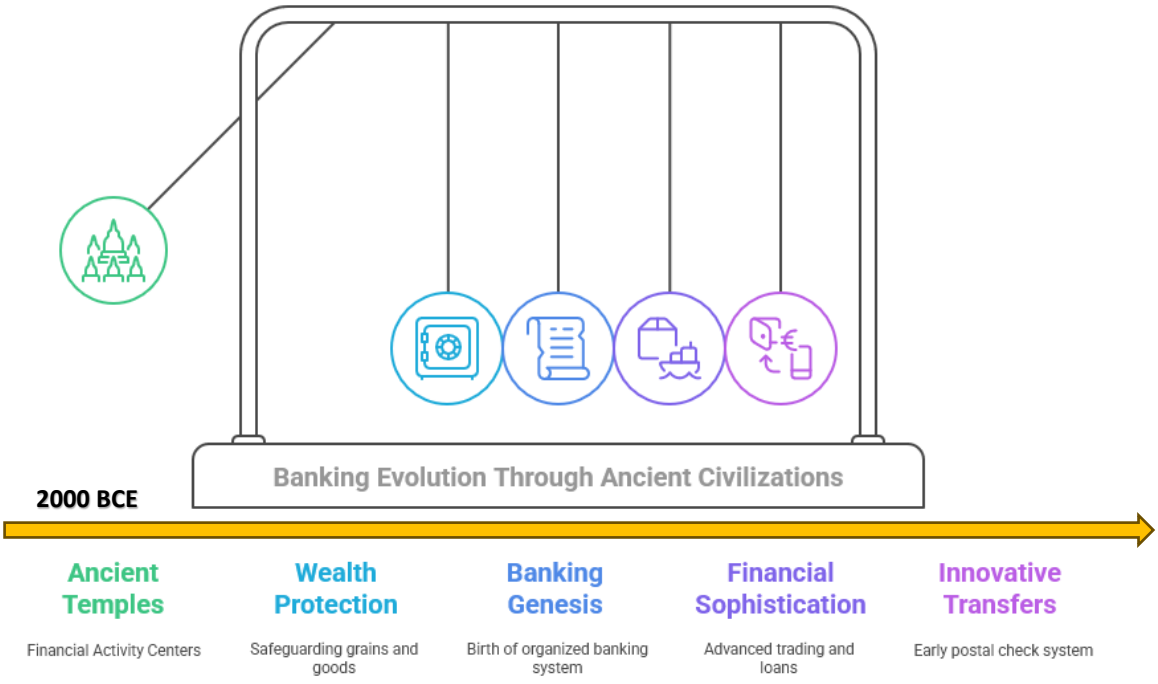


Figure 2: Emergence of Banking in History

At the same time, Egypt, especially during the flourishing Ptolemaic period, was not far behind in terms of financial ingenuity. The introduction of the postal check system by the royal cereal depositories bears witness to this. Here we see a striking resemblance to our contemporary mechanisms of transfers and check systems. The Egyptians' innovative approach to managing grain flows and credits between

different parties effectively established the principles of modern banking, emphasizing the management and transfer of funds without the need for physical exchange of cash[12].

ii. Banking Through Rome and the Medieval Tapestry

Exploring deeper into the annals of financial history, the Roman Empire emerges as a crucial episode in the evolution of banking. Here, we see Rome infusing a new level of sophistication and order into the banking realm. The Romans were pivotal in introducing a more formal structure to the operations of banks, complete with state involvement and an array of regulations. Yet, for all their advancements and organization, they stopped short of establishing what we might see as a precursor to the modern central banking system or crafting a unified payment network. This gap in their financial architecture, perhaps, hints at the limitations and the scope for future enhancements in banking systems.

As we journey past the fall of the Roman Empire, the landscape of European banking underwent a stark transformation. Walker and Morris point out that Europe, in the wake of Rome's decline, saw its banking system not so much advancing but rather retrenching to more basic functions. The focus shifted predominantly to money changing, a regression influenced significantly by the prevailing Christian norms that vociferously denounced usury (the charging of interest on loans).

In this scenario, where mainstream Christian beliefs stifled the development of diverse banking practices, Jewish financiers stepped into the breach. Their involvement became indispensable, particularly given the Christian laws against usury. Jewish lenders adeptly filled this crucial void, offering loan and credit facilities. However, this crucial role did not come without a cost. The Jewish financiers, while providing an essential service in the backdrop of stringent Christian usury laws, often faced severe societal backlash and repercussions, highlighting the intertwined nature of religion, society, and finance in shaping the banking structures of the era.

iii. Renaissance to Modernity

After the medieval tapestry, then comes the period of the Crusades which marks a pivotal phase in the development of the banking. This era, rife with conflicts and the movement of resources across vast distances, necessitated secure and efficient means of fund transfer. A notable innovation of this time was the introduction of letters of credit by the Knights Templar. This mechanism, an embryonic form of contemporary banking instruments, was crucial for the Crusaders, providing a safer, more reliable

[12] The Handbook of Banking Technology by TIMWALKER and LUCIAN MORRIS. Edition Wiley - Edition 2021.

method of carrying and transferring large sums of money, a vital function in the treacherous and unpredictable landscapes of medieval warfare and pilgrimage.

Moving into the Italian Renaissance, we witness a remarkable era of banking evolution, as highlighted by Walker and Morris. Italy, during this period, became the crucible of significant banking innovations. The adoption of double-entry bookkeeping marked a monumental leap in financial management, allowing for a more sophisticated, accurate, and transparent way of tracking and reporting financial transactions.

Simultaneously, the era saw the ascent of influential banking families and institutions, such as the Medici in Florence and the Rialto Bank in Venice. These entities weren't merely businesses; they were integral to the socio-economic fabric of their times, laying down the foundational structures and principles of what would evolve into modern banking. Their influence extended far beyond their financial prowess, affecting cultural, political, and social realms, thereby setting the stage for the development of modern financial systems and the eventual global banking network.

iv. Genesis of National Banking Systems

Then comes in history the types of banks called state-backed banks which mark the creation of important financial institutions, starting with the Banco della Piazza di Rialto, ancestor of this evolution[13]. The creation of such institutions has opened a new chapter in the financial landscape, characterized not only by the provision of secure financial services, but also by a profound structural change in the very nature of the banking sector.

Following the Banco della Piazza di Rialto, other notable institutions like the Bank of Sweden, the Bank of England, and the Bank of Scotland were founded. Each of these banks played a seminal role in shaping the early financial framework of their respective nations. Beyond their primary role of offering financial services, they were instrumental in laying the foundational elements for what we recognize today as modern central banks.

These early banks were more than mere repositories or lenders; they were integral to the broader economic strategies of their respective states. Their emergence signified a shift towards an era where financial stability, monetary policy, and economic development fell increasingly under the purview of national interests and governance. This transition was crucial in guiding the evolution of banking from

13 https://en.wikipedia.org/wiki/Banco_del_Giro

local, often fragmented entities into more centralized, state-oriented institutions, thereby shaping the trajectory of economic development and fiscal policy in the following centuries.

2.1.2. Gold, Cash and Currency in History

i. *Early Coins*

History of money and banking goes back a long way, from the primitive barter system to the sophisticated digital economy we know today. Initially, various objects such as animal teeth, livestock, feathers and precious stones served as a form of commodity money, allowing value to be stored and exchanged. This barter-like system evolved when societies began using specific weights of precious materials like silver to standardize trade, with one of the first known units of value being the shekel.

Around 550 BCE, the Kingdom of Lydia (modern-day western Turkey) introduced one of the first minted coins, a significant advancement in the history of money. These early coins, made from electrum (a natural blend of gold and silver), laid the foundations for a standardized monetary system. Although initially, the purity and weight of coins could vary, advancements in minting techniques eventually led to the creation of coins with a consistent value.

Coins initially had intrinsic value, being made from precious metals. Their worth was essentially tied to the material from which they were made. This system evolved into one where coins, and later banknotes, were viewed as representative money. Their value was not solely based on the material but also on the trust and backing of the issuing authority. Representative money required that the issuer maintain a reserve (often gold) to back the value of the currency, a concept that dominated until the mid-20th century.

ii. *The Rise of Paper Money*

The next phase in the evolution of currency was the invention of paper money. The first banknotes were issued in China during the reign of Emperor Hien Tsung (AD806-821), but not as a result of any great financial insight. The sole reason for their introduction was an acute copper shortage that precluded the striking of new coins. Eventually, China got carried away with the ease of producing this new form of cash. Too much of it was printed and this led to inflation. In 1455, the Chinese abandoned the use of paper money and did not return to it for several centuries.

The Chinese experience was repeated when Sweden became the first European nation to experiment with paper money. In 1661, a banker named Johan Palmstruch began to issue credit notes that could be exchanged at his Stockholm bank for stated numbers of silver coins. Unfortunately for Palmstruch, who had consulted the Swedish government before launching the scheme, he got carried away with his

licence to print money. He issued more notes than his bank had silver deposits to redeem, and in 1668 was prosecuted for fraud. He was initially sentenced to death, but the penalty was later commuted to imprisonment.

Despite the less than glorious outcomes to these early trials of paper money, the tide of history was firmly on the side of the new form of currency. As economic activity increased in Europe, it became apparent that the money supply needed to be expanded beyond the limits imposed by holdings of precious metals. This recognition led to the establishment of the first national central banks. People were much more likely to trust notes backed by government reserves than those issued by private institutions. They even proved willing to accept temporary governmental bans on the redemption of banknotes for silver, as happened in Britain during the "Restriction Period" of 1797 to 1821[14].

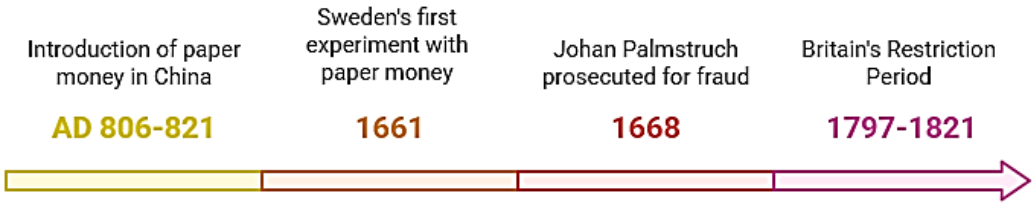


Figure 3: The Evolution of Paper Money

iii. *The Gold Standard*

By the 20th century, many countries moved away from the gold standard, especially during periods of economic stress like wars and the Great Depression. These pressures often led nations to adopt fiat money systems, where the currency's value is based more on governmental decree and less on a physical commodity like gold. Centralization of banknote issuance intended to prevent bankruptcy but introduced the risk of inflation, notably when too much currency was printed. This inflation threat led to the adoption of the Gold Standard, linking currency to gold quantities, thus stabilizing values domestically and internationally. It effectively maintained consistent money supplies and set stable exchange rates, for instance, defining the dollar-to-pound rate based on each country's gold pricing.

The Standard supported economic balance across nations, with price adjustments driven by shifts in production and supply. However, adherence to its rules was critical for success. World War I marked a turning point as countries abandoned these rules, printing money to fund the war, causing the Standard's

[14] https://www.independent.co.uk/money/spend-save/money-money-money-the-history-of-cash-5328684.html

failure. Although reinstated in the 1920s, the Gold Standard couldn't withstand the Great Depression's pressures.

By 1931, with Britain's exit due to significant gold outflows, the Bretton Woods system replaced the Gold Standard post-World War II, fixing exchange rates and basing international debts on the US dollar, convertible to gold. However, high demands on the US gold reserves endangered the system. President Nixon's 1971 decision to halt gold conversion for US dollars effectively ended the Gold Standard.

This marked a significant shift towards fiat currency, which is not backed by physical reserves but rather by the trust in and the economic stability of the issuing government. However, this trust-based system also has its drawbacks, as seen in cases of hyperinflation in countries like Zimbabwe and Venezuela, or even Sudan where excessive money printing led to severe economic consequences.

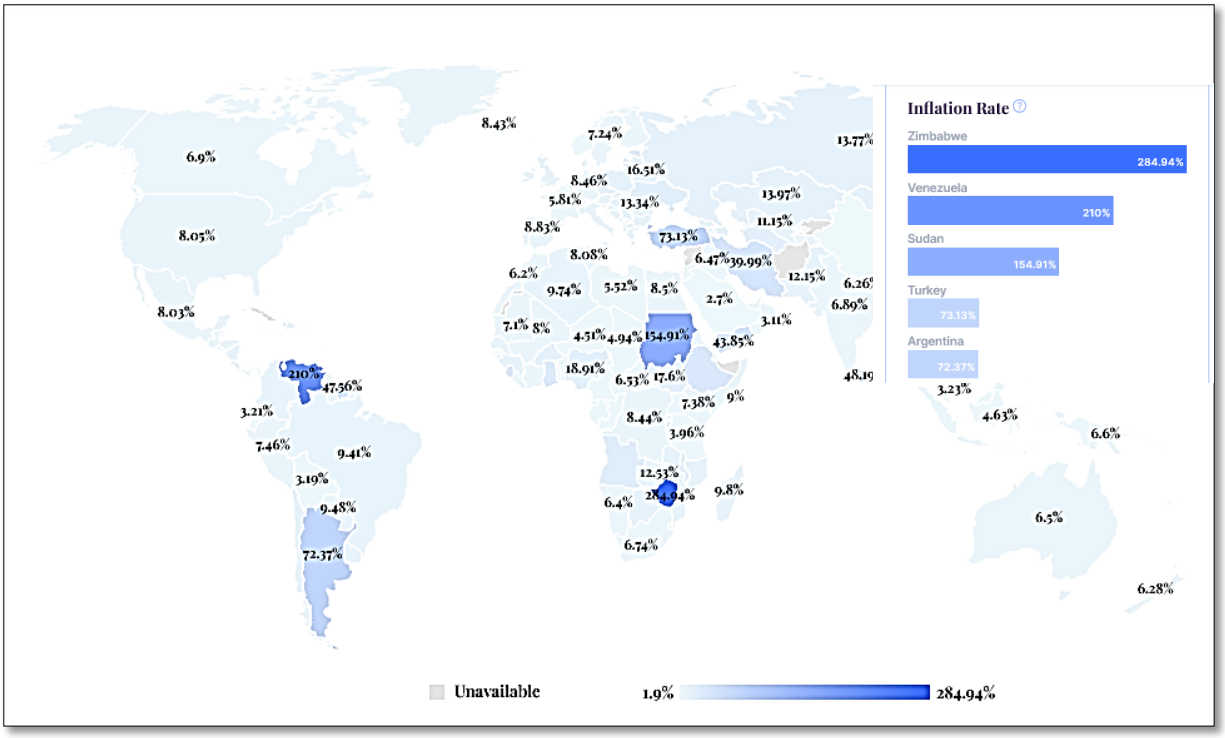


Figure 4: Inflation by Country

2.1.3. Digital Currencies

i. *Blockchain Technology evolution*

To start understanding digital currency, we will explore its essence as a revolutionary digital ledger technology. The word “blockchain” comes from the transactions being grouped into “blocks” (as a data

package), which are linked to the blocks that precede them to form a chronological "chain" of blocks. This blockchain provides a trail of the underlying transaction and, thus, represents a complete ledger of the transaction history (Holotiuk et al. 2017; Nofer et al. 2017)[15].

The idea for blockchain technology was put forward by research scientists Stuart Haber and W. Scott Stornetta in 1991. They were the pioneers in the computer programming concept of time- stamping digital documents so that they could not be backdated or manipulated[16]. Blockchain technology was first configured and implemented as a practical solution in 2008 by a pseudonymous group of developers, Satoshi Nakamoto. They designed and developed the technology using hash encryption to uniquely timestamp blocks of data without surfacing the identity of the entity that performed the transaction.

This approach was highly innovative in that it did not require a central governing body to provide confirmation and verification. Therefore, blockchain is sometimes referred to in computer science as a peer- to- peer trustless mechanism.

Far from the classic ledgers, blockchain presents a decentralized, distributed approach, capturing the essence of transactions and asset tracking across networks. Each transaction is meticulously grouped into blocks, forming a chain that chronicles all transactions in a historical sequence, offering both transparency and security.

Blockchain's technology development started with several distinctive features. Here's a look at its evolution and fundamental elements:

1) **Distributed Ledger Technology**: Distributed ledger technology (DLT) delivers a combination of distributed systems and advanced cryptography, enabling the transfer of immutable data recorded on the ledger among the counterparties. This ledger avails the companies of a transformative platform to organise settlement and trade of digital assets; it helps to insure, securitise, transfer, and finance businesses.
2) **Peer-to-Peer Technology:** Bitcoin works as a peer- to- peer (P2P) network where digital currency can be transferred between participants with no single entity solely in charge of approving transactions. But, as in any digital environment made up of bytes and files, data can still be copied and transferred to multiple other people and devices.

---

[15] Blockchain and Banking: How Technological Innovations Are Shaping the Banking Industry by Pierluigi Martino ; 2021 ; https://doi.org/10.1007/978-3-030-70970-9

[16] Blockchain Applied: Practical Technology and Use Cases of Enterprise Blockchain for the Real World ; Stephen Ashurst, Stefano Tempesta - 2022

3) **Cryptographic Security**: In blockchain, transactions within blocks are sealed cryptographically. This sealing employs hash functions, ensuring the data's integrity and security. Such cryptographic measures render the records within the blockchain irreversible, thereby building trust and robustness.
4) **Asymmetric Cryptography:** In blockchain, asymmetric cryptography, or public-key cryptography, is used to help authenticate transactions and secure digital property. It follows the private key-public key mechanisms that encrypt and decrypt the information, meaning only the owners holding those particular keys could have access, keeping the communication and transactions safe.

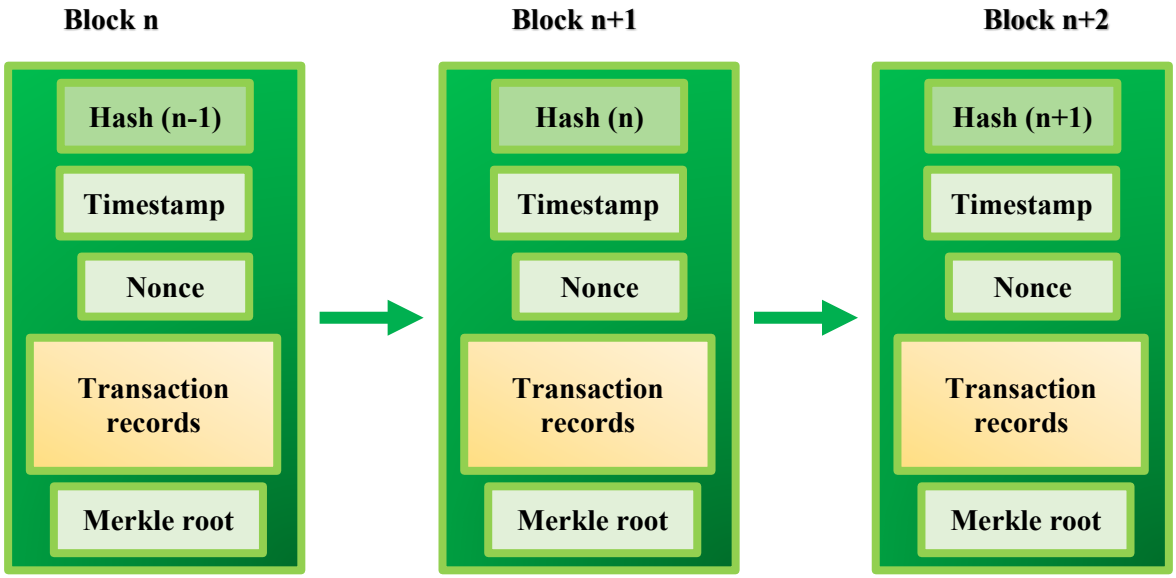


Figure 5: Example of a blockchain[17]

5) **Consensus Mechanisms:** blockchain heavily depends on consensus mechanisms in validating transactions. A transaction is only recorded if there is consensus across the network, hence ensuring accuracy and credibility in the ledger. This consensus-based approach has given rise to various methods like Proof of Work (PoW) and Proof of Stake (PoS), each with its unique advantages and challenges.

[17] Blockchain and Banking: How Technological Innovations Are Shaping the Banking Industry by Pierluigi Martino ; 2021 ; https://doi.org/10.1007/978-3-030-70970-9 - p12

- **Proof of Work (PoW):** Most notably used by Bitcoin, PoW requires miners to solve computationally difficult mathematical puzzles in order to validate transactions and add new blocks to the chain. While secure, this method is resource-intensive, leading to high electricity consumption.
- **Proof of Stake:** PoS and its variants, where the probability of validating a transaction is proportional to the ownership stake of the user in that currency, came as an energy-efficient successor to PoW. The mechanism further evolved into Delegated Proof of Stake, commonly known as DPOS, for more democratic and efficient validation through elected delegates.

6) **Transparency:** Blockchain offers transparency between the participants that makes it tough for hackers to release malware within the network in order to gather information or to transmit data to another database handled by a hacker.

As a result, blocks are "chained" together: the header of each block includes a hash function that reflects the contents of the previous block, which itself includes a hash function derived from its predecessor and so on all the way back to the first block in the chain. Furthermore, a block's transactions are hashed through the Merkle root—that is, the hash of all the hashes of all the transactions that are part of a block in a blockchain network. This means that cryptographic functions ensure the integrity and security of information on the blockchain. This ensures irreversibility of records, hence high robustness and high trust due to the fact that it would be impossible to delete or edit these blocks.

ii. Origin of Cryptocurrencies

As seen previously, various methods of exchanging goods and services have existed throughout history. All of them have been undergoing evolutions and changes, or, directly, they have disappeared. This is the case of barter or the use of precious materials, which gave way to the system that has worked until now, the bills and coins. In an age where technology is gaining more and more ground every day, a medium of exchange more adjusted to the times is necessary: cryptocurrency. In the wake of the cypherpunk movement in the 80s, cryptocurrency emerged. With hidden keys that could only be deciphered by those who knew how to decode them, this art defended the widespread use of writing.

David Chaun founded Digicash a decade later to establish a centralized electronic money system to allow for more safe and anonymous transactions. Adam Black proposed Hashcash, a method to monitor spam and denial-of-service attacks at the same time. Although Bitcoin, the first completely decentralized cryptocurrency, did not appear until 2009 (Richard Trend; 2021.).

What are their origins?

Cryptocurrencies, unlike fiat currencies, are not distributed by a central bank. Instead, they are "mined," a term that reflects the magnitude of the work involved in their production. Miners volunteer their time and use their computing power to verify cryptocurrency transactions and add them to the blockchain. As a reward, they receive new units. This procedure is costly because it necessitates specialized computer hardware and a significant amount of computing power.

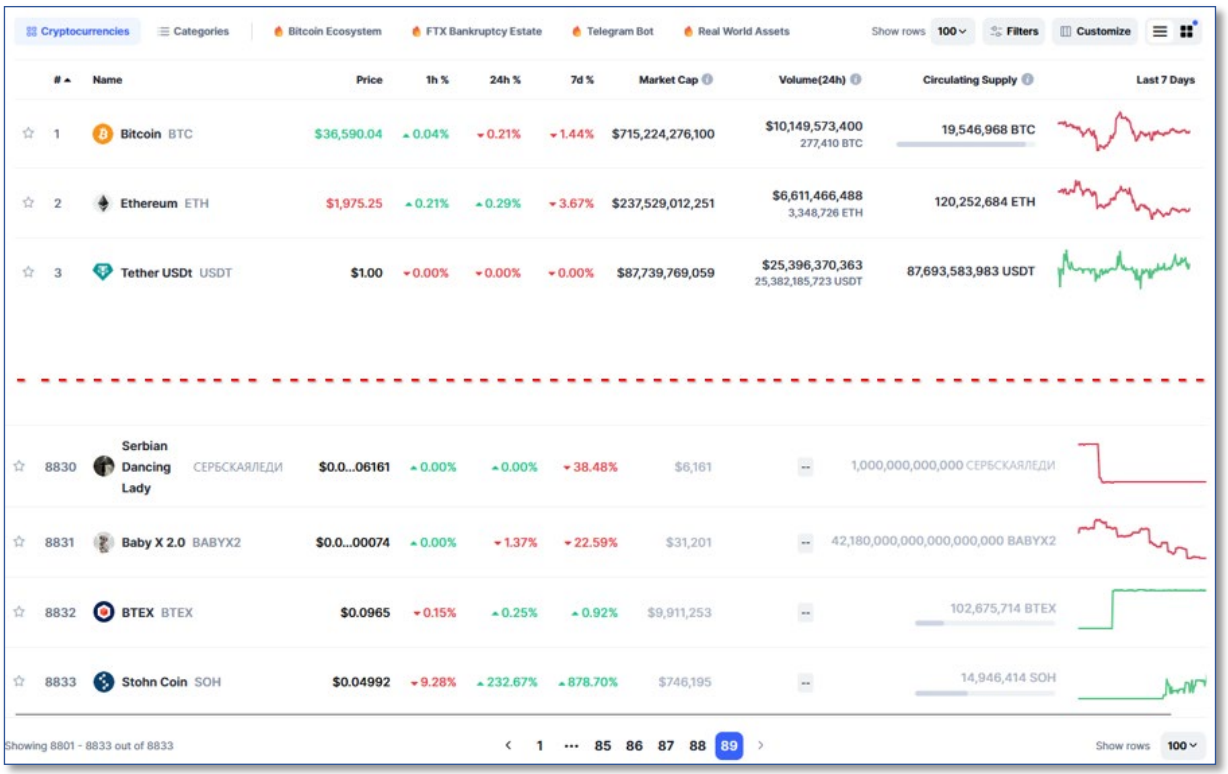


Figure 6: cryptocurrencies globally on CoinMarketCap, Nov 2023

Mining issues are likely to be resolved over time with technological innovations like the Lightning Network. The technology works like a payment protocol that can be added to a cryptocurrency's blockchain to speed up operations and use less energy[18]. Presently, cryptocurrency is primarily utilised for investing and trading purposes. More than 8,800 cryptocurrencies are traded in exchanges globally (CoinMarketCap, Nov 2023[19]). The most widely well-known cryptocurrencies are Bitcoin, Ethereum, Binance coin, Tether, and Solana.

[18] Cryptocurrency For Beginners - The Complete Guide for Beginners to Understand Bitcoin and Cryptocurrency Technologies, and Start Investing in Crypto Coins by Richard Trend; 2021.

[19] https://coinmarketcap.com/

The inception of Bitcoin by Satoshi Nakamoto was not an attempt to invent an entirely new payment method, but rather to solve existing problems in our current payment systems. Nakamoto's response to the 2008 financial crisis and subsequent central bank actions which involved substantial quantitative easing and bailout of failing banks was to propose a decentralized financial system. This system was perceived as a means to address the social injustice and economic instability caused by the overprinting of money and bailout of banks responsible for the crisis.

Bitcoin, fundamentally a digital currency, is underpinned by blockchain technology, an open-source and versatile platform and his vision for Bitcoin extended beyond merely serving as a currency; it was an ideological stance advocating for a financial infrastructure that is decentralized, empowering individuals rather than central authorities. In this peer-to-peer network, every user contributes to and benefits from the system. Its adaptability and potential have even caught the attention of traditional banks, intrigued by its underlying technology.

The core concept of Bitcoin which is the decentralization meant that every user's involvement was crucial, it thrived on collective participation rather than reliance on a centralized entity like a government or a bank. This digital currency invites everyone to participate, encouraging the use of Bitcoin in business transactions, either as a payment method or for accepting payments, showcasing its potential to expand economic opportunities globally. The ultimate success and acceptance of Bitcoin as a mainstream financial alternative, however, still remain a subject of ongoing observation and debate[20].

Blockchain technology records and confirms cryptocurrency trades, much like a digital ledger. A blockchain collects and stores the information when you buy, sell, or exchange cryptocurrency. Central banks in developed countries in general started studies on large-value CBDCs. Since central bank deposits have already been digitalized, large-value CBDCs are unlikely to cause issues related to financial stability or monetary policy. In other words, **large-value CBDCs could be understood as applying DLTs like blockchain** to already-digitalized central bank deposits. The European Central Bank (ECB) and the Bank of Japan started their joint research entitled Project Stella in 2016 (Bank of Japan, 2016)[21].

iii. CBDC

[20] Bitcoin For Dummies® Published by: John Wiley & Sons, Inc.

[21] The Future of Financial Systems in the Digital Age: Perspectives from Europe and Japan by Markus Heckel, Franz Waldenberger - 2022

The underlying technology used is Blockchain on cryptocurrency or CBDC, forms of virtual currencies. Traditionally, the economics of money and payments interested a rather closely guarded circle of experts in central banking, academia, and the financial industry. This has changed radically over the last 15 years or so: technological innovation began to disrupt the market for means of payments on an unprecedented scale; the resulting changes have become very tangible in daily life. Correspondingly, the strong growth of e-commerce was paralleled by a decline in the use of cash and a growing need for modes of electronic payments. Technology-driven start-ups ("Fintech") and large digital platforms ("BigTech") increasingly enter the market so far dominated by banks and credit card companies. In tandem, the same technology has enabled decentralized electronic transaction settlement and, by extension, the development of both fiat cryptocurrencies and stablecoins. All of these events have inspired central bankers to investigate the relative merits of issuing a digital version of cash-called CBDCs. This debate has intensified considerably in recent years as policy makers have become unsettled by prospects for abrupt and potentially irreversible changes to the financial system due to the existence of strong network effects in both payments and digital services. Although ultimately not realized, the initial Libra proposal by Facebook (now Meta) was widely perceived as a significant wake-up call and led to an intensification of research efforts throughout the central banking community. According to a recent survey, 90% of 81 respondent central banks were actively investigating the potential for a CBDC at the end of 2021 (Kosse and Mattei, 2022)[22].

[22] Working Paper Series: The economics of central bank digital currency
Toni Ahnert, Katrin Assenmacher, Peter Hoffmann, Agnese Leonello, Cyril Monnet, Davide Porcellacchia
No 2713 / August 2022

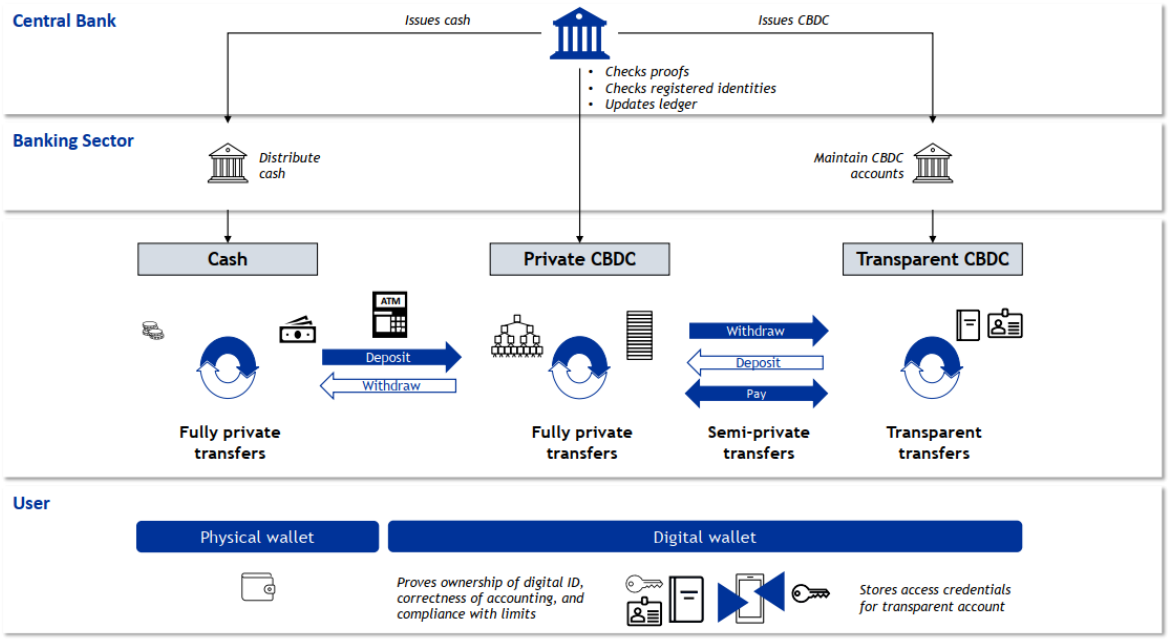


Figure 7: High level architecture of the proposed CBDC design

In the current monetary system, central banks' money has a physical form (bills and coins) and a digital form (as reserves held at central banks by financial institutions that can access this deposit facility for wholesale transactions). The introduction of a CBDC would then produce a new form of central bank money, creating a digitalised form of a sovereign currency that would be a liability of central banks. According to the Bank of England, a CBDC can be defined as electronic central bank money that

(i) can be accessed more broadly than reserves, (ii) potentially has much greater functionality for retail transactions than cash, (iii) has a separate operational structure to other forms of central bank money, allowing it to potentially serve a different core purpose, and (iv) can be interest bearing, under realistic assumptions paying a rate that would be different to the rate on reserves[23].

CBDCs are essentially currencies because they will be a digital version of the same money we use today, but instead of being managed by a payment service of a bank or card issuer, they will be managed directly by the central bank or by private companies contracted and duly authorized to manage the infrastructure necessary for their operation. Therefore, considering their use, we could say that CBDCs are a means of payment. CBDCs will be created in the image and likeness of cryptocurrencies, from an

[23] The (Near) Future of CBDCs: Risks and Opportunities for the Global Economy and Society By Nicola Bilotta and Fabrizio Botti; Series Edited by Prof. Lorenzo Kamel

application on our phone, tablet or computer, commonly called a wallet, we can pay with our mobile devices, as we can already do today, by placing our smartphone to an NFC reader in the box of a trade, or through a QR code generated by the seller's terminal that scans our phone to accept payment from the screen of our phone[24].

CBDC has also been a highly buzzed and searched word over the internet, particularly after March 2020. Figure 8 shows that the interest in CBDC (web search) has gradually risen in recent years. The number represents search interest relative to the highest point on the chart. In 1993, the Bank of Finland launched the Avant smart card, an electronic form of cash. Although the system was eventually dropped in the early 2000s, it can be considered the world's first CBDC.

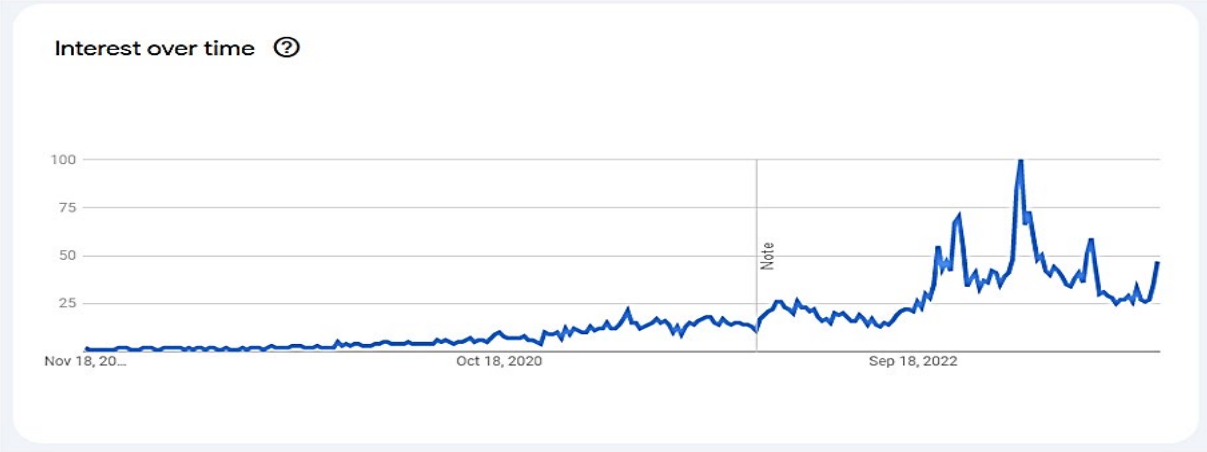


Figure 8: CBDC search trend in past decade

The interest-bearing design of CBDC and the obsolescence of paper currency would also contribute to greater macroeconomic stability, because interest rate adjustments would no longer be constrained by any effective lower bound in response to severe adverse shocks. That lower bound has been a key reason why many central banks currently aim at positive inflation rates of 2 percent or more, whereas CBDC will essentially eliminate the need to maintain such an "inflation buffer" or to deploy alternative monetary policy tools such as quantitative easing or credit subsidies. Moreover, in the event of a severe economic downturn, CBDC would facilitate the provision of money-financed fiscal stimulus. Indeed, Friedman (1948) highlighted the complementarities between monetary and fiscal expansion under such circumstances.

The initiation of CBDC would represent a fairly natural progression in light of current trends in monetary operations. For example, most central banks already pay interest on the reserves of commercial banks,

[24] Understanding CBDC - Money and Blockchain by Martin Mendo Antunez - info@bod.com.es - www.bod.com.es

which comprise a substantial portion of the total monetary base. The Federal Reserve has expanded its capacity to pay interest to an even wider range of counterparties by borrowing funds in the U.S. Treasury repo market. Moreover, the Federal Reserve Banks now maintain segregated deposit accounts for systemically important financial market utilities (FMUs), so that the customers of those FMUs may rest assured that their funds are secure, liquid, and interest-bearing[25].

Today, the world is getting more and more digital, so is the monetary system. Digital currencies and electronic transactions reduce our need for hard cash. Modern banking, especially the fractional-reserve banking concept wherein banks hold only a portion of their deposits in reserve, has allowed money creation through lending. This system, though effective, is heavily reliant on regulatory frameworks and interbank trust. So, we can confirm that CBDCs are the antithesis of a cryptocurrency like bitcoin. At the same time, all current ones, fiat currencies, like all current ones, are not backed by anything other than a legal imposition and the confidence we assume that the state authority will be able to exert whatever force is necessary to maintain that imposition.

The main differences according to **Martin Mendo Antunez** [26]are

1- a/b. Issuer/Issue: A CBDC coin is issued by a central bank, while Bitcoin is decentralized and has no central issuer.

2- Regulation: A CBDC coin is regulated by the government, while Bitcoin is not regulated by laws, only by its internal protocol published in its white paper.

3- Privacy: CBDC transactions are monitored by the central bank and/or the government, while Bitcoin transactions are pseudonymous.

4- Processing: CBDC transactions may be faster than bitcoin transactions due to centralization.

5- Volatility: The volatility of CBDC coins may be lower than Bitcoin due to regulation.

6- Permissioned System: CBDC coins must identify the user or company and may have restrictions on their use, while Bitcoin is non-permissioned and can be used freely.

7- Adoption: CBDC adoption will be enforced by the government and central banks, while Bitcoin adoption is entirely voluntary and driven by the community of its users.

Stablecoin tokens (Lyons & Viswanath, 2020) are primarily used for payment settlement and to ensure a stable exchange rate. A token's underlying asset can range from a single fiat currency (pegged 1:1) to

---

[25] CENTRAL BANK DIGITAL CURRENCY AND THE FUTURE OF MONETARY POLICY
Michael D Bordo and Andrew T Levin. Working Paper 23711 - http://www.nber.org/papers/w23711

[26] Understanding CBDC - Money and Blockchain by Martin Mendo Antunez - info@bod.com.es - www.bod.com.es

those that rely on algorithmic mechanisms to maintain price stability. Initially, stablecoin was introduced as a hedge against volatility in cryptocurrency values. Its primary purpose is to act as an intermediary between fiat currencies and cryptocurrencies.

Other challenges such as data privacy and governance pose threats in the financial ecosystem around blockchain-based assets. Also, investor protection, cyber security attacks and fraud, and vulnerabilities that affect global financial stability, as well as regulatory oversight issues more akin to AML and terror funding, are a few of the features of these threats. Governments, central banks, financial regulators, and policymakers are trying to strike a balance between threats and innovations associated with the use of DLTs to provide financial services[27].

iv. From Ancient Ledgers to Digital Wallets: The Evolutionary Path to CBDCs

We can therefore observe the huge evolution that currency and the banking enterprise have experienced at some point of records as much as state-of-the-art virtual platforms of today. This chronicle of progress charts a course from tangible cash to the conceptual currencies that outline our modern economies. As we stand on the edge of the CBDC technology, it is critical to delineate the historic continuum that has brought us to this position.

The concept of CBDCs represents a culmination of this historical trajectory, marrying the tried and tested believe in crucial banking with the innovations of the digital age. This evolution can be traced as a sequence of incremental advancements, each responding to the demands of its time for more secure, efficient, and on hand types of economic transactions.

From the grain banks of historical Mesopotamia to the gold-subsidized notes of yesteryears, each section in the evolution of currency has been driven by using a quest for stability and reliability in change and wealth garage. Today, CBDCs become the subsequent logical step, grounded in centuries of financial tradition but propelled by the potential of blockchain and cyber technology. The relevance of CBDCs today may be directly connected to their historical precedents. Just as the banking quarter has continuously tailored to new technologies from the arrival of paper money to electronic banking the emergence of CBDCs is a reaction to the digital revolution that seeks to redefine the essence of cash in on more and more virtualized world. By integrating robust cybersecurity features and

[27] Blockchain for Industry 4.0 - Emergence, Challenges, and Opportunities. Edited by Anoop V. S., Asharaf S., Justin Goldston, and Samson Williams - Yes 2023 - p124

capitalizing on the centralized supervision of principal banks, CBDCs are designed to offer a secure and robust digital foreign currency that meets modern demands in international finance.

In the development milieu of CBDCs, it is not a particular phenomenon but rather part of banking's ongoing story that changes with the need to fulfill increasingly complex demands in the 21st-century financial system. As we begin to consider the possibilities of CBDCs, it is far with the understanding that they might be the cutting-edge bankruptcy inside the lengthy history of banking innovation, promising to hold ahead the legacy of believe and efficiency which has continually been at the coronary heart of monetary change.

2.2. Ethical Implications in Banking Compliance

The issue of "business and ethics" has also been addressed by Milton Friedman (the first Nobel Prize winner of the many that will be mentioned), who introduces the "Friedman Doctrine" in his book Capitalism and Freedom (1962) by saying: "there is one and only one social responsibility of business: to use its resources and engage in activities designed to increase its profits so long as it stays within the rules of the game, which is to say, engages in open and free competition without deception or fraud" [28].

In banking ethics is a system of rules and standards of conduct for banking institution and its staff [29]. Ethics in the banking sector is designed to determine the standards of behaviour that prevent disruption of financial legislation, or at least dictate dignified way out of situations that put a professional in the offender.

2.2.1. Banking Ethics Concepts

During the development of banking were developed three general concepts of banking ethics (Eremia, Stancu, 2006) [30]:

- **Concept of general ethics;**
- **Concept banking professional ethics;**
- **Concept of ethical bank;**

[28] Ethics in Banking - Is It Possible? By Cristina Rovera - School of Management and Economy, University of Turin, Turin, Italy
[29] Banking Ethics: Main Conceptions And Problems Valentina Fetiniuc, Ivan Luchian - https://www.upet.ro/annals/economics/pdf/2014/part1/Fetiniuc-Luchian.pdf
[30] AN INVESTIGATION OF BUSINESS ETHICS PRACTICE AND ITS PERFORMANCE IN THE CASE OF LION INTERNATIONAL BANK (LIB) S.C - http://www.repository.smuc.edu.et/bitstream/123456789/4818/1/Final%20Thesis%20Print.pdf

i. The first concept is related to the promotion of the basic idea of the banking that there can be no moral standards other than generally accepted by society. This is the earliest conception of the ethics of banking rather be called general banking ethics and some basic rules. For example, customer relationships have been linked to training since antiquity.

In several countries, the prevailing religious beliefs shape various sectors, including the financial industry. A prime example is Islamic banking, which adheres to Sharia principles, integrating these religious precepts into the field of economic development. Islamic banking, also accurately described as Sharia-compliant financing, eschews traditional interest or fees for monetary loans, a practice known as Riba or usury, which is viewed as unethical.

This approach positions the bank not simply as a profit-driven entity, but as a collaborative partner in customers' daily lives and business ventures. In this partnership model, the bank contributes funding and, like any stakeholder in a successful venture, is entitled to a fair share of the profit. However, this philosophy does have its limitations in banking evolution. It restricts financing in businesses involved in activities deemed non-compliant with Islamic principles. This includes, but is not limited to, industries related to pork, alcohol, tobacco, gambling, and lotteries. Essentially, it bars all forms of speculative operations and transactions that contradict Islamic doctrine.

Similarly, the Orthodox Christian Church views banking as a form of entrepreneurial activity. It approves of banking operations as long as they align with Christian ethical standards. In this context, earning a profit is not seen as the sole objective. Rather, profits are a means to support and further Christian beliefs, encompassing charitable acts and initiatives. This perspective underscores a broader vision where banking and financial pursuits dovetail with, and actively support, religious and ethical values.

Christian Catholic Church, unlike the Orthodox, has long been an important participant of international banking and capital market investor, being, in fact, an active supporter of the so-called new world economic order, considering the ethical as operations all financial, recommending only a certain selectivity parishioners investment objects. Thus, in 2010 the Catholic Church has implemented a particular stock index Stoxx Europe Christian Index, which is intended to indicate the shares of company’s investments are deemed ethical.

Another conception is linked to the promotion of banking ethics opinion that once in different fields of human activity, such as medicine, justice, audit, state, etc., are allowed special rules of behaviour, then they should exist in banking. Hence, the ethical banking is a kind of professional ethics in finance,

which, in turn, is a specialized set of moral norms and rules to be followed in professional banking. Banking ethics governs relations between individual members of a bank collective of these members, the rest of society from corporate positions.

Banking ethics can be approached in two basic forms (Božović, 2007)[31]: collective and individual ethics.

- Collective ethics include applying ethical principles in making management decisions, which refers both to external entities and the environment, and ethical relationships within the bank.
- Individual ethics refers to joining the normal rules of morality. In the case where a person has a moral deficit means that it put personal interests before collective legal rules and moral standards before ordinary business which may affect the business climate. Individual ethics is the cornerstone of the group or collective ethics.

ii. **Professional banking ethical** standards is usually met by the Code of Ethics, which is an internal document prepared by professionals and approved by the bank voluntarily and / or banking community. By essence, the Code of Ethics is a formal declaration or ethical guide for the way in which people in an institution must act and make decisions.

Codes include the main responsibilities of the bank to:

- ✓ *Consumers (customers):* the importance of consumer satisfaction, quality, safety, consumer protection, price fairness, after-sales services;
- ✓ *Partners*: promptness in paying bills, compliance with all contractual provisions, cooperation in achieving quality and efficiency, not accepting any kind of bribe, commission or excess of hospitality.
- ✓ *Employees*: how the company leverages human resources, recruitment and selection, training and development, working conditions, equal opportunities, rewarding retirement, protection against discrimination and harassment.
- ✓ *Shareholders*: protecting investments made in the company, providing investment, efficiency, accuracy of information on economic and financial situation.
- ✓ *Community*: the company's obligation to protect the environment, involvement in the community interest in educational and charitable activities.

[31] Banking Ethics: Main Conceptions And Problems By Valentina Fetiniuc, Ivan Luchian
https://www.upet.ro/annals/economics/pdf/2014/part1/Fetiniuc-Luchian.pdf

Application of ethical codes should raise a good quality of banking, but international practice indicates the following behaviour problems of banks:

- Considering the above bank interest from the customer.
- Approaching weaknesses of the client must become the source of profits for the bank and presentation of errors and failure of moral behaviour as a by-product in the ultimate goal achieving.
- Inclination to take advantage of imperfect legislation. Leadership principle: which is not contrary to law, is entirely ethical.
- Refusing any accountability for their behaviour, by breach of trust and ignoring the existence of moral factors.
- Addressing the incorrect behaviour as insignificant violation if it does not lead to an obvious injury.
- Transferring responsibility to the consumer (client), which often lack the necessary qualifications (or did not wish to be informed) to understand the essence and consume complex banking products and, in their opinion, deserve such an attitude.

iii. New era of knowledge comes with a new concept of banking development, which is mainly related to the practice of banking in the virtual environment, in which regular personal contact with the customer in classical banking actually become an exceptional personal service for elite. This will lead to the emergence of new ethical problems. Implementation of ethical codes in UEMOA banks substantially raised the level of civility in the conduct of bank employees and, to some extent, the quality of provision of banking services.

Bank management must take into account that a well-managed complaint is a commercial act strongly contributing to the preservation and deepening customer relationships, to preserve the image of the bank and not least the continuous improvement of services. Concept of ethical bank (which in some sources is called **social civic, or sustainable banks**) activity is related to the financial institution that gives priority in its social and environmental impact of its investments and loans.

Promoting support for sustainable development in the banking sector is facing two main directions (Eremia, Stancu, 2006):

1) Integrating social and environmental responsibility in banking environmental initiatives (e.g. recycling programs or energy efficiency) or social responsibility initiatives (for example, providing support for cultural events, improving human and humanitarian donations).

2) Mainstreaming sustainable development into the core activities of the bank, by integrating environmental and social considerations into product design, policies and strategies.

A similar form of manifestation of banking ethics is the concept of socially responsible bank referring to an alleged bank debt (as a social actor) would have it to all parties involved in the conduct of banking. The concept of corporate social responsibility has been the first academic debates in the early 1950s. Yet, according to the literature, the banking sector showed a delay in considering issues of sustainable development, despite the exposure to risk this intermediate sector of the economy.

Since 2000 sustainable development issues beyond the scope of the banking sector by incorporating social and environmental issues into lending policies. The effort to adopt socially responsible practices includes adhering to a series of internationally recognized principles and practices. One such set of principles is promoted by The International Finance Corporation (part of the World Bank Group) as the Equator Principles, a complex risk management adopted by financial institutions to determine, assess and manage environmental and social risks in the investment projects and is designed firstly, providing the minimum standard of due diligence to support responsible risk making decisions (Equator Principles, n.d.).

2.2.2. Digital Banking Ethics Challenges

A global problem became the involvement of banking institutions in money laundering schemes, namely the legalization of funds obtained by illegal means, which is connected to the central role of banks in the money laundering dirty. So far, only the banking system can transform and make huge amounts of money transfer for cleaning.

The vulnerability of small states to the financial manipulation and money laundering should not be underestimated because in many of these state incomes is considerably less than the profits made by criminal organizations. The risk is that such countries where washing can be of huge amounts of money fraudulent origin. Many of these small states, seeking to become financial centers, although do not have financial and legal necessary infrastructures[32].

In a recent report by The Inter-Governmental Action Group against Money Laundering (GIABA) published in November 2022, a concerning trend was highlighted: at least eight instances of money

[32] BANKING ETHICS: MAIN CONCEPTIONS AND PROBLEMS by VALENTINA FETINIUC, IVAN LUCHIAN. Annals of the University of Petroşani, Economics, 14(1), 2014, 91-102 91

laundering and corruption within the banking operations of ECOWAS (Economic Community of West African States) were detected[33].

Consideration of the ethics of eBusiness has tended to focus on areas relating to the fragility of information collected and held electronically and transferred via computer-mediated communication. These include privacy of information about individuals, accuracy of information, ownership of information and intellectual property and accessibility of information held (see Mason 1986; Turban et al 2000). These perspectives focus very much on the individual consumer and disregard the significant area of electronic commerce that is business to business. In the B2B case privacy-based issues around information control are less critical at the personal level. By looking at a business-to-business case, we identify the moral precepts relevant to the case which may form a basis for further consideration of ethics. These relate to: freedom of choice; transparency; facilitating fraud (ethical/illegal activities of others).

So, for this literature review, we will refer to some ethical theories to help identify rigorously observed notions of right and wrong. In particular, we identify discourse ethics as a potentially useful perspective to apply to Digital Currency. First, the reduction of costs means that organisations can improve service and potentially generate more profits for shareholders and job security for employees. On the other hand, job losses are the means by which costs are cut and this has social implications for those in the firing line. The displacement of job opportunities away from face-to-face and back-office service roles to information system professionals is a common feature of the electronic banking revolution. Employment issues aside, however, there are also positive aspects of online trading for bank customers and in turn consumers. As the case study points out, access to expensive online systems is enabled by '**piggybacking'**. From an ethical point of view, this means that high quality systems are not held by an exclusive group but made available to those other than the wealthiest, hence opening up fair access.

The widespread use of FinTech has also raised concerns regarding privacy, security, consumer protection, ethical considerations, and regulatory compliance. Drawing on qualitative research, the study investigates issues such as consumer privacy, data breaches, trust, financial integrity, adoption barriers, and ethical controversies in the diffusion of FinTech. The findings highlight the importance of addressing these ethical concerns to restore digital ethics in the fintech industry and ensure principles such as fairness, transparency, accountability, and access in technology are realized.

---

33 https://www.giaba.org/media/f/1300_Money%20Laundering%20and%20Terrorist%20Financing%20through%20Corruption.pdf

The banking sector is navigating what might be its most challenging and competitive era, significantly influenced by the rapid digitalization of financial services and the emergence of novel financial players (Popescu & Popescu, 2019). This shift has not only intensified competition but also heightened the focus on data protection and privacy, alongside escalating customer expectations. The traditional core principles of finance ethics has distilled seven basic principles found in the codes of conduct of 11 financial services professional associations: integrity, objectivity, competence, fairness, confidentiality, professionalism, and diligence, as shown in Table 1.

Nº	Ethical principles in finance	Definition
1.	**Integrity**	Moral self-government, autonomy, dependability, and honesty. Consistent thinking and behaviour, a clear conscience, and responsible behaviour
2.	**Objectivity**	Client interests must be protected and advanced. Keeping trust and perceptions accurate. Keeping bias and conflicts of interest at bay
3.	**Competence**	Providing clients with competent financial services. Maintaining expertise in the workplace through ongoing education and professional experience
4.	**Fairness**	Treating customers fairly, applying the "Golden Rule" consistently, ensuring fair returns for all, balancing interests, and avoiding disparate treatment
5.	**Confidentiality**	Confidently managing client relationships, protecting and not disclosing sensitive information, and building and maintaining trust through information sharing
6.	**Professionalism**	Clients must be treated with courtesy and respect, and confidence must be established, as well as a reputation and trust must be maintained with clients and the general public.
7.	**Diligence**	Providing services promptly and thoroughly, tailoring services to customer needs with attention to detail and persistent focus and conducting a thorough review of support staff.

Table 1: A list of ethical principles in finance and their definitions Principle

The incorporation of digital technology has significantly reduced entry barriers into the financial services industry, allowing the number of new financial service providers to skyrocket in recent years (Banna & Alam, 2021)[34]. Neobanks, Fintechs, BigTechs, and cryptocurrency exchanges are all disrupting the banking industry, and traditional financial institutions are either in the process of being disrupted or have already been disrupted (Murinde et al., 2022).

[34] Ethical Fintech is a New Way of Banking by Rina Arum Prastyanti, Rezi, Istiyawati Rahayu

These developments pose challenges and opportunities for traditional financial institutions, many of which are either currently experiencing disruption or have already been affected.

Fintech lending is reshaping the financial landscape by offering accessible, convenient lending solutions for both individuals and businesses. However, innovation or digitalisation brings with it several ethical concerns:

1) **Privacy and data security:** To assess creditworthiness, fintech lending platforms collect and analyze massive amounts of personal and financial data (Raj & Upadhyay, 2020). When this data is not adequately protected or is used beyond the scope for which it was Originally intended, ethical concerns arise.

2) **Fairness and transparency:** Fintech lenders frequently make lending decisions using complex algorithms and machine learning models. The ethical challenge is to ensure that these models are fair and unbiased while not perpetuating discrimination based on race, gender, or socioeconomic status (Rovatsos et al., 2019). Transparency in algorithmic decision-making is critical because it allows borrowers to understand how decisions are made and seek recourse if they are treated unfairly.

3) **Responsible lending practices:** To prevent predatory lending, fintech lenders must adhere to responsible lending practices. While the convenience and speed of online lending can be advantageous to borrowers, there is a risk of exploiting vulnerable individuals or extending credit to those who cannot afford it.

4) **Customer support and protection:** Fintech lending platforms must prioritize customer protection by implementing robust complaint handling mechanisms and dispute resolution processes. To address borrower concerns and provide assistance throughout the loan lifecycle, adequate customer support should be in place.

5) **Financial inclusion and literacy:** Fintech lending should strive to promote financial inclusion and literacy (Moenjak et al., 2020). While these platforms have increased credit availability to underserved populations, they should also invest in educating borrowers about responsible lending, loan terms, and financial management. Efforts should also be made to include marginalized communities and to ensure that fintech lending does not exacerbate existing inequalities. Ecosystem of fintech, including companies, regulators, and investors, faces a balancing act. Stricter regulation

guarantees safer transactions for consumers but can pose barriers for new entrants, potentially stifling industry growth.

Banking compliance is filled with ethical implications, considering the very important role it plays in the integrity of financial systems and protection of various interests. Essentially, ethical conduct in banking compliance involves adherence to legal standards and moral principles that govern financial operations and transactions. It also helps build trust, ensures fairness, and protects customers by pledging for high moral values that put customers first, the economy, and society in general, and the wider economy. This review identifies that banks are still attached to ethical grounds, and their compliance structures are strong; however, they find ethical challenges in the new digital currency world.

2.2.3. Ethical Dimensions and AML Considerations in the Era of CBDCs

i. *CBDC landscape and ethical*

The ethical landscape of CBDCs extends beyond technical capability and into the area of societal impact. The layout and implementation of CBDCs bring profound moral implications, particularly concerning privacy, inclusivity, and the prevention of financial crimes. To forge CBDC systems that not simplest innovate but additionally guard, it's critical to embed ethical issues into their very architecture. Privacy and records governance emerge as number one ethical fears. CBDCs, through distinctive feature of their digital nature, may want to potentially enable remarkable surveillance abilities if no longer tempered by means of sturdy privateness safeguards. A stability needs to be struck among the want for transparency to discourage financial malfeasance and the vital to guard character privateness rights. Detailed evaluation of privacy-preserving technology, which includes zero-knowledge proofs and steady multi-celebration computation, could offer answers that permit CBDC structures to affirm transactions without exposing touchy statistics. Furthermore, the integration of AML frameworks into CBDC operations underscores the moral responsibility to thwart monetary crimes even as respecting consumer confidentiality. CBDC systems should be designed to prevent exploitation by using illicit actors, incorporating superior AML strategies without compromising the moral tenets of person privateness. This may be achieved by deploying current AML tools along with anomaly detection algorithms and device learning models that discover suspicious styles without unnecessarily invading personal privateness.

CBDCs can also allow for economic inclusion by making digital forms of currency more available and accessible to unbanked and underbanked parts of the population. But this salient aspiration has to be tugged with great caution to avoid creating new forms of exclusion or discrimination. Deep examination

is required on issues like the potential capacity limits to CBDC adoption, including virtual literacy and technological access. All of these ethical dimensions are to be in full investigation when projects of CBDC development reach out for interactions with a wide range of stakeholders, from ethicists to consumer protection corporations and financial experts. That would mean CBDCs are not only sound technologically but also attuned to broader social values and principles.

The evolution of CBDCs, therefore, needs to be informed by a thorough and nuanced appreciation of the ethical and AML-related considerations. With a range of examples and case studies, we take an in-depth look into those essential aspects so that responsible advancement of the CBDCs can serve to improve monetary systems in an ethical and secure manner.

ii. History of AML

There is no consensus on the origin of the term"money laundering". Some researchers have traced the origin of the term to the practice of washing coins in casinos to make sure they did not spoil the white gloves of the casino ladies (Unger 2013b), while, in other places, it was traced to the time of Al Capone who used to launder his criminal proceeds using launderette to avoid detection by law enforcement (Unger 2013b). There are also some who traced its origin to the Watergate scandal, when it first appeared in newspapers (Schneider & Windischbauer 2008), Abdullahi Usman Bello[35].

The idea of money laundering is simple in principle. The person who has received some form of ill-gotten gains will seek to ensure that they can use these funds without people realising that they are the result of inappropriate behaviour. To do this they will need to disguise the proceeds such that the original source of the proceeds is hidden and therefore the funds themselves appear to be legitimate. Given that it is often cash that needs to be disguised, the criminal will often seek out legitimate cash-based businesses to enable them to disguise the source of their illegitimate cash.

When you are discussing the laundering of money, there are generally two different connotations to consider. Money laundering refers both to the use of a cash business such as a launderette to facilitate the mingling of legal and illegal funds and also to the generic process of disguising the original proceeds of the funds, a process more normally referred to as layering. By mixing legitimate and illegitimate funds, the entire amount could potentially appear to be legitimate, and would therefore have been laundered, achieving the objectives of the money launderer. The funds will appear to have come from the legitimate business whereas some of the funds actually have arisen from criminal activity of some type. Indeed, coin-operated launderettes, which are generally cash-based businesses, would represent an

[35] Improving Anti-Money Laundering Compliance: Self-Protecting Theory and Money Laundering Reporting Officers - Abdullahi Usman Bello – p26

ideal opportunity to achieve this, and much early money laundering did make use of legitimate cash-based activity to disguise and transform ill-gotten gains.

It is important to recognise that there are two main styles of money laundering – professional and amateur. The professional money launderer will take advantage of any perceived weakness in the systems of control operated by a financial institution or regulatory structure. Amateur money laundering takes an opportunity and does not really cover its tracks very well, leaving obvious causes for concern which are easy to identify either by employees being diligent or through the use of modelling systems. It is normally the latter type of money laundering that is detected by law-enforcement agencies. The professional is always much harder, and therefore more expensive, to identify.

Clearly, organised criminals are able to take advantage of any number of cash-based businesses to disguise illegal proceeds. The following are just a few of the types of business which have been subject to abuse by money launderers[36]:

- ✓ Launderettes
- ✓ Newspaper sales
- ✓ Taxis
- ✓ Bars and fast food restaurants
- ✓ Casinos
- ✓ Insurance
- ✓ Asset management
- ✓ Antiques
- ✓ Property.

If we consider that this currency, which traditionally poses challenges for criminals due to the risks of physical transport, becomes entirely virtual, it opens up both new opportunities and challenges. On one hand, the elimination of physical transport could make illicit activities such as Money laundering easier to conceal. On the other hand, it presents challenge for professionals fighting against these crimes.

iii. *Terrorism Financing*

In the immediate aftermath of the attacks of 11 September 2001, the Bush Administration told the American public that it would not mount a traditional effort in its "war on terrorism". The campaign would be a protracted affair, invoking non-traditional methods, institutions, and resources, including an effort to suppress both the raising and the movement of funds that could be used to support the acts of global terrorists.

As President **George W. Bush** declared on 24 September 2001:
We will direct every resource at our command to win the war against terrorists, every means of diplomacy, every tool of intelligence, every instrument of law enforcement, every financial influence. We will starve the terrorists of funding, turn them against each other, rout them out of their safe hiding

---

- ✓ [36] **Handbook of Anti-Money Laundering,** Dennis Cox, p6

places, and bring them to justice[37].

This definition is based on the internationally accepted definition of terrorist financing as provided by the United Nations (UN) International Convention for the Suppression of Financing of Terrorism (1999) and on Recommendation II of the Financial Action Task Force (FATF) Special Recommendations on Terrorist Financing and its Interpretative Note. Article 2 of the International Convention for the Suppression of the Financing of Terrorism provides:

Any person commits an offense within the meaning of this Convention if that person by any means, directly or indirectly, unlawfully and willfully, provides or collects funds with the intention that they should be used or in the knowledge that they are to be used, in full or in part, in order to carry out:
a) *An act, which constitutes an offense within the scope of and as, defined in one of the treaties listed in the annex;* or*
b) *Any other act intended to cause death or serious bodily injury to a civilian, or to any other person not taking an active part in the hostilities in a situation of armed conflict, when the purpose of such act, by its nature or context, is to intimidate a population, or to compel a government or an international organization to do or to abstain from doing any act*[38].

Traditional ideas on money laundering do not apply to terrorist financing. The basics of criminal money laundering involve washing large amounts of dirty money. However, terrorist funding can and does operate on a shoestring. That being said, the actual funding of terrorism – generating the funds as opposed to supplying them to frontline terrorists – does involve large amounts of money. This money is generated through donations, fake charities, front companies, criminal activities and other supply mechanisms. All of this money has to be processed and hidden in the world's financial system. However, as with traditional money laundering, there is mounting evidence that this is being increasingly achieved outside the traditional Western banking system through such methods as informal exchange systems (such as hawala or hundi), diamond trading and online share trading (to name but three). A further key problem is that because the amounts involved in mounting a terrorist operation are remarkably low, it is not necessarily feasible or possible for regulated institutions or companies to identify terrorist customers by analysing their financial transactions. Or to put it in very simple terms, the frontline terrorist bank account is more likely to have very small sums of money in it and transfers to it, rather than transfers of large amounts and a high balance[39].

---

[37] Countering the Financing of Terrorism - Thomas J. Biersteker and Sue E. Eckert – p1
[38] © 2009 The International Bank for Reconstruction and Development / The World Bank – p7
[39] Dirty Dealing: The Untold Truth about Global Money Laundering, International Crime and Terrorism - Peter Lilley - Preface xv

iv. Proliferation Financing

Financing of the Proliferation of Weapons of Mass Destructions is a requirement on countries to implement targeted financial sanctions to comply with the United Nations Security Council (UNSC) resolutions on the proliferation of WMD and its financing. This requirement is similar in its approach to the targeted financial sanctions applicable in the context of the fight against terrorism and terrorism financing but has a narrower application: it addresses exclusively the freezing without delay of funds or other assets of persons or entities designated by the UNSC as being involved in illicit proliferation of WMD and domestic cooperation.

The FATF defines proliferation of weapons of mass destruction (WMD) as the transfer and export of nuclear, chemical or biological weapons, their means of delivery and related materials. The issue of proliferation received international attention for several years. A number of international conventions provide for measures to detect and prohibit proliferation, especially with regard to nuclear materials (such as the Nuclear Non-Proliferation Treaty). These treaties do not, however, consider the aspect of financing proliferation. In 2004, the UN Security Council issued Resolution 1540, requiring states to put in place a number of measures in order to prevent the proliferation of nuclear, chemical or biological weapons. Subsequently, the FATF started in 2007 to consider the threats related to proliferation financing and its interconnection with terrorism and terrorism financing.

The interconnection is since proliferation might be a means for supporting the undertaking of terrorist activities. Its disruption is therefore essential for the prevention of terrorist acts. Moreover, the practical undertaking of proliferation financing often uses the same channels as terrorist financing. Measures to be applied to disrupt proliferation financing would therefore often be similar to the measures applied to counter terrorist financing[40].

2.3. Security and Privacy Challenges in CBDC Operations

2.3.1. Fortifying Trust: Securing the Future of Finance

As a widely available and electronic means of payments, CBDC would be faced with security risks like cyber and consumer protection risks. The economics of the security risks of a CBDC and cash are different because of lower entry costs of attempting to find vulnerabilities in the system and a potentially higher reward in a national system (Kahn et al. 2020a). An approach here is to find the distribution of responsibilities between the different participants in the ecosystem that are Bank, distributors, and users

[40] https://www.coe.int/en/web/moneyval/implementation/financing-proliferation ; https://www.fatf-gafi.org/content/dam/fatf-gafi/reports/Status-report-proliferation-financing.pdf

themselves that create the incentives to manage the risks appropriately. This remains an important area of technical research[41].

At the heart of the CBDC system lies security, built on the foundational principles of confidentiality, integrity, and availability. Beyond these core elements, the system must also guarantee that the central bank maintains exclusive authority over the issuance and redemption processes. We also pay a great attribute to the none-repudiation principle. To ensure the robustness of a CBDC system, a layered defense strategy must be established, leveraging established cybersecurity techniques and processes. Given that security is a paramount attribute for a CBDC, considerations related to it may impose limitations on the characteristics and potential use cases of the selected CBDC solution.

- ***Confidentiality***

Confidentiality encompasses the protection of holdings, transactions, and identities, ultimately safeguarding privacy. In particular, any information stored in a CBDC system should adhere to the minimalism principle-retain only what is strictly necessary for operational needs. Undesired disclosure of such sensitive information considerably raises the consequences of a security breach. Compliance with KYC requirements and the regulations surrounding AML/CFT/CPF may require that personally identifiable information (PII) be stored and linked to value stores and transactions.

- ***Integrity***

Integrity concerns revolve around countering counterfeiting and double-spending across all CBDC use cases, while ensuring the accuracy and irreversibility of transactions. Unlike physical banknotes, CBDC systems face a core risk of double-spending, which refers to the ability to spend the same value multiple times. Digital signatures can effectively combat counterfeiting; however, additional protective measures are required to prevent double-spending. These measures may include the integration of tamper-resistant hardware in local store-of-value devices, the establishment of organizational authority within a central ledger, or achieving consensus within distributed ledger systems.

- ***Availability***

Within the realm of a CBDC, availability pertains to the system's capacity to withstand large-scale cyberattacks. Disruptions, such as distributed denial of service (DDoS) attacks or botnet assaults, have the potential to temporarily restrict or disrupt access to the CBDC system. Employing standard cybersecurity techniques can fortify public endpoints and interconnected systems, mitigating the impact

[41] Central Bank Digital Currency; Considerations, Projects, Outlook
Edited by Dirk Niepelt, Centre for Economic Policy Research, 33 Great Sutton Street - London, EC1V 0DX - UK

of such attacks[42].

2.3.2. Privacy and data protection issues?

There are several potential privacy and data protection issues that may arise in line with the technical design choices related to our CBDC. Recently, the ECB published a survey in which the most pressing issue for European citizens is privacy. Given the broad scope of a CBDC, the potential privacy and security implications of a CBDC project are enormous, and its successful implementation requires strong security protocols and a robust architectural framework.

Furthermore, the effectiveness of a CBDC project is heavily reliant on its policy objectives and intended use-cases. Consequently, it is imperative to integrate data protection and privacy requirements at the very core of the CBDC concept. This should be accompanied by ongoing monitoring through a data protection impact assessment to ensure that necessary measures can be promptly taken to address emerging concerns. Simultaneously, it is crucial to provide a clear specification of the policy objectives and use-cases, as well as how they may intersect with other digital policy initiatives and related aspects. This comprehensive approach is essential to ensure the successful and responsible implementation of a CBDC[43].

i. *Privacy and Data Protection Considerations in CBDC Design*

Privacy is a significant concern with regard to federal CBDC accounts, as they may provide the government with unprecedented access to personal bank transaction data, which has been a major source of disagreement throughout the development process. A government's decision to create a CBDC must strike a balance between the right of individuals to privacy and the need to curb illegal financial activities. The US Privacy Act of 1974 currently governs the government's access to personal data; however, this law was created in a different era of payment processing and, therefore, may need to be revised [M. Ashfaq, R. Hasan, J. Mercon 2023]. The design choices made in the development of a CBDC have profound implications for the preservation and management of privacy. In the context of a CBDC issued by the Central Bank of West African States (BCEAO), certain design decisions can significantly impact the assurance of privacy.

In designing a CBDC, one of the main approaches is an account-based system where verified identities

[42] Bank Of Canada: Security of a CBDC - Staff Analytical Note 2020-11 (English); Cyrus Minwalla - June 2020 https://www.bankofcanada.ca/2020/06/staff-analytical-note-2020-11/

[43] European Data Protection Supervisor: https://edps.europa.eu/data-protection/our-work/publications/techdispatch/2023-03-29-techdispatch-12023-central-bank-digital-currency_en

of every account holder are required; this is to uniquely identify an individual in the payment ecosystem. While this is indispensable in ensuring functionality, security, and compliance, there are challenges related to privacy and data protection. On the other hand, a purely token-based system is theoretically much more accessible and protects data better, but it brings its own risks, such as the potential of financial loss in case the end users fail to store their cryptographic keys properly.

Moreover, the type of technological infrastructure behind the CBDC can further worsen the current status quo regarding privacy and data protection in the digital payment environment. For example, depending on the degree of accessibility to transactional data by different stakeholders along the value chain of a payment, such data can be used more frequently for creditworthiness scoring and invasive marketing practices, facilitated by the presence of a single, persistent CBDC user identifier.

For this reason, the technological options taken during the development of a CBDC must consider privacy and data protection for all citizens in the BCEAO regions. These projects therefore involve large-scale operations on the processing of personal data with a high degree of risk to the rights and freedoms of data subjects. Hence, privacy and data protection must be embedded in the regulatory regime and at the heart of technological design choices of the project. All feature, configuration, and risk acceptance choices should be strictly justified and documented. A comprehensive data protection impact assessment is required throughout multiple phases of a CBDC project.

The process of research and development for the design of a CBDC should adopt a data protection by design and by default philosophy from the very beginning. A retrofitting effort, insofar as it would even be possible for design flaws of a CBDC, is economically costly and involves uncertainties that could undermine public and corporate acceptance of the project.

If CBDC development-and in particular, considerations of data minimization and storage limitation-is merged with distributed ledge technology, it may give rise to some difficulties because blockchain technology is per se immutable and/or ever-extending.

Furthermore, CBDC design raises some privacy and data protection issues on the crossborder payments side. Even though there is a common set of guidelines for domestic regulation, the set of international rules and implementation patterns can make interactions across borders very tough. This is likely to pose additional difficulties when designing and implementing crossborder CBDCs when it comes to issues like privacy, data protection, and compliance with AML requirements.

Addressing these potential challenges requires thoughtful design and multilateral coordination to align technical, regulatory, and supervisory frameworks. Standardization and harmonization efforts, aimed at

establishing consistent privacy and transparency standards, can ensure interoperability across jurisdictions and enduring relevance.

ii. *Enhancing Privacy in Payment Transactions*

In the existing environment, cash is being used for most form of anonymous financial transaction although subject to the limit of transaction in a structured regulated framework. As digital methods of payment will gain acceptance among all and reduce the use of physical cash, cash may continue to be edged out of more significant roles in financial transactions. Cash transactions offer a unique form of anonymity, allowing for direct peer-to-peer exchanges without the involvement of a third-party intermediary to validate the transaction. Conversely, the proliferation of private digital payment solutions in the market has led to the heightened exploitation of user data, consequently eroding the realm of anonymous payments.

The token-based CBDC solution, much like physical banknotes, has the potential to restore anonymity as a unique feature in the digital means of paying. It can offer secure, stable, and anonymous cashless transactions, which is actually a gap in the market that exists now.

Offline solutions, particularly a token-based CBDC with offline transaction capabilities, hold promise in terms of preserving privacy and data protection. These solutions necessitate minimal processing operations and enable local transaction processing without third-party validation. They also serve as a secure contingency in the event of significant internet disruptions. Such a token-based CBDC with offline transaction capabilities could effectively emulate the functionality of physical cash or endorsed checks.

It's important to acknowledge that the digital nature of a CBDC inherently increases transparency. Striking the right balance between privacy and the imperative to combat illegal activities like drug trafficking, money laundering, and terrorism financing, which rely on anonymous cash transactions or alternative remittance systems, is a complex challenge. Legislators play a pivotal role in defining this equilibrium and establishing necessary use-cases. Advanced pseudonymization techniques will be combined with other privacy enhancing technologies to arrive at this type of balance.

Lastly, there is a need to devise a suitable method for identifying and enabling access to offline digital tokens. Account-based identification systems have the potential to unveil and potentially track all end-user transactions, leading to profiling concerns. In contrast, an offline token-based CBDC system can preserve the anonymity of payments while still facilitating secure and efficient transactions, and then reveals a reliance on short-term data. The temporal scope of this research may not capture the full spectrum of variables influencing transaction efficiency over extended periods. Economic conditions are subject to fluctuation, and the resilience of CBDCs to such changes remains underexplored. Long-

term studies are necessary to truly understand the efficiency outcomes in diverse economic conditions. This calls into question whether the short-term efficiencies reported in these studies will stand the test of time and variable economic pressures. The current body of literature would greatly benefit from longitudinal research that considers a wider array of economic scenarios and the potential adaptability of CBDC systems.

iii. *Systemic Risks of Profiling and Surveillance*

Ability to monitor financial transactions of an individual results in the emergence of an extraordinarily detailed portrait that defines their life--online and offline-spending propensity, including. No other party interacts so intimately during a payment cycle as the several players operating during its operation acquire massive volumes of personal information regarding. This gives rise to a systemic risk of profiling and surveillance by players in the payment ecosystem. Under CBDCs, the potential for such risks is closely interlinked with the design choices being made.

For example, a design that prevents central banks from handling personal data, or requires robust data minimization practices may mitigate or eliminate the privacy risks compared to existing payments systems. In contrast, one that allows the central bank to track and store personally identifiable information linked with payments, or lets merchants capture and correlate payment details with individual customer records could increase these privacy risks compared with existing modes of payment.

Second, the CBDC issuance significantly increases the direct possibilities of the central bank, and, transitively, those of other public authorities to access financial data relating to citizens; this may eventually threaten systemic public surveillance. Whether this information is reused, shared with third authorities, or merely leaked out as a result of certain vulnerabilities, having such vast amounts of data recorded inherently creates risks related to mass surveillance and misuse.

To help overcome these issues, the employment of privacy-enhancing technologies, such as advanced pseudonymization techniques and zero-knowledge proofs, becomes necessary. These technologies strive to reduce the information disclosed by transaction partners to only that which is absolutely necessary for validation that a payment has indeed been satisfactorily executed.

Besides, it remains important to provide and legally establish retention periods for personal data concerning the purposes of its processing. This will minimize risks in cases of hacking or unauthorized access to the CBDC's technological infrastructure.

2.4. Potential of CBDCs to Reshape Banking Compliance and

Cybersecurity

2.4.1. Impact of CBDCs on Regulation Structures

Although governments repeat that regulations of all kinds are for our good and always to protect the citizen, the truth is that they are nothing more than the disguised use of government force against citizens to maintain control. Economic and financial regulations are created to protect the interests of big business, especially the banking and financial sector. Governments and lawmakers use the so-called revolving door to gain access to high-level, politically appointed political or civil service positions from which they legislate and regulate with the primary objective of benefiting the banking industry and controlling citizens.

Using public institutions that supposedly oversee banking, financial and competition activities. When their time of public "service" is over, most of them use the revolving doors to return to the corporate world, occupying high and wellpaid positions. CBDCs will be the perfect instrument to control and impose the restrictions they wish to impose, always to "protect us" and in strict compliance with the laws; laws that will be created or modified as necessary for this purpose. Bitcoin is a permissionless system, no permission is needed to create a wallet, send or receive Bitcoin. Bitcoin transactions are irreversible, unlike credit card transactions and bank transfers, and cannot be censored, worldwide, regardless of governments, states or borders[44].

The legal foundations for issuing CBDCs must be carefully considered. Central Banks must ensure that any actions taken align with the state constitutional monetary and financial laws and pass judicial tests. The fundamental principles of public and constitutional law, such as conferral, subsidiarity, and proportionality, impose limitations on the powers of the local institutions, which would extend to the issuance of CBDCs.

To mitigate potential regulatory impacts negatively, Central Bank to explore alternative approaches, such as improving current payment infrastructures to reduce frictions. This includes encouraging international cooperation to enhance the efficiency of cross-border fund transfers and developing digital payment instruments that offer privacy and security.

CBDCs could revolutionize the financial industry, careful consideration must be given to their impact on regulatory structures. The shift towards digitization necessitates an evolution in regulatory approaches to maintain stability, promote inclusion, and ensure privacy while harnessing the benefits of

[44] Understanding CBDC - Money and Blockchain by Martin Mendo Antunez

CBDCs. Our research results must be able contribute to understanding how central banks can navigate these new and complex environment, balancing innovation with the need for robust regulation.

2.4.2. CBDCs and AML Frameworks

In 2016, **Ben Broadbent**, a senior Bank of England official, delivered a speech titled "Central Banks and Digital Currencies" at the London School of Economics that must also be catalogued into monetary history. The speech sought to touch on the following questions:

> *What is the key innovation in private-sector digital currencies such as bitcoin? What is a 'central bank digital currency'? And what might be the economic implications of introducing one?*[45]

The speech tried to grapple with the magnitude of Bitcoin's innovation and CBDCs.

While these currencies take their first steps in gaining traction, they will interact with discrete regulatory regimes, most notably AML. Based on the arguments above, the intersection of CBDCs with AML regimes is going to be crucial. This paper particularly focuses on the CBDC to be issued by the BCEAO, regarding the required optimal ethical dimension, banking compliance, and cybersecurity features.

1) **Data: The Cornerstone of Digital Transactions**

Digitization of money is closely linked to the handling of data. Everything with digital transactions, data created and shared alone, amounts to huge volumes of personal data inputs acting as crucial ingredients of commerce. But this data-centric nature of digital transactions does pose a host of challenges to regulators and central banks: susceptibility to network effects in market concentration may favor the incumbents who have exclusive access to data, matters of privacy and governance of personally identifiable information, and going digital puts payment systems at stake for money laundering and other illegitimate activities.

2) **Triple Imperative for Central Banks**

For central banks, the pivot to CBDCs presents a 'triple imperative': fostering competition, ensuring data privacy, and maintaining payment system integrity. These imperatives become increasingly significant against the backdrop of emerging technologies like cryptocurrencies, stablecoins, and the incursion of BigTechs into payment systems. These innovations promise cost savings and convenience, but their ultimate impact hinges on the market structures and governance models they adopt. Notably, network effects associated with BigTechs may lead to market dominance, marginalizing competitors and raising concerns about data misuse.

---

[45] Layered Money: From Gold and Dollars to Bitcoin and Central Bank Digital Currencies by Nik Bhatia - 2021

3) Opportunity in CBDCs

The overriding criterion when evaluating a change to something as central as the monetary system should be whether it serves the public interest. Here, the public interest should be taken broadly to encompass not only the economic benefits flowing from a competitive market structure, but also the quality of governance arrangements and basic rights, such as the right to data privacy. It is in this context that the exploration of CBDCs provides an opportunity to review and reaffirm the public interest case for digital money as stated in the Bank for International Settlements (BIS) Annual Economic Report 2021[46]. CBDCs, whether wholesale or retail, represent a digital embodiment of central bank money, offering finality, liquidity, and integrity. They empower central banks to sustain the public good nature of money, provided they adhere to key design principles.

4) Design Principles for CBDCs

The design of CBDCs should align with a two-tier system where central banks focus on core functions such as ensuring monetary stability and security, while the private sector drives customer service innovation. CBDCs should, therefore, enable the private sector to handle user interactions, including account management and enforcement of AML/CFT/CPF regulations, thereby maintaining the central bank's limited financial system footprint akin to cash.

5) Account-Based CBDCs and Digital Identity

The BIS report advocates for an account-based CBDC model, anchored in an effective digital identity scheme. This model contrasts with a token-based design, which allows anonymous payments. An account-based CBDC, rooted in digital identity verification, enhances monitoring of illicit activities while providing privacy options: transaction data could be concealed from third parties and authorities, contingent on the payment authentication design. However, the debate on who should issue and manage digital identities persists, given the varying levels of trust in entities handling personal data.

6) Striking a Balance

Achieving equilibrium between protecting user data and maintaining system integrity is pivotal. The design must prevent data accumulation and misuse while ensuring compliance with AML/CFT/CPF regulations. An account-based CBDC, integrated with a robust digital identity framework, could offer a solution, facilitating transparent and secure transactions that comply with AML directives.

As CBDCs continue to shape the financial sector, integrating AML frameworks into their design and operation is essential. This integration ensures that CBDCs not only enhance transaction efficiency but

[46] Annual Economic June 2021 Report -p66 - https://www.bis.org/publ/arpdf/ar2021e.pdf

also uphold stringent AML standards, promoting a secure and ethically sound financial environment. The CBDC issued by the BCEAO, and other central banks embarking on similar ventures, must navigate these considerations, optimizing their digital currency offerings to align with AML regulations and foster a secure, inclusive financial ecosystem[47].

2.4.3. Cybersecurity Threats on CBDCs

The main point is that all would be blamed for the risk CBDCs bring in: inflicting more of the high centralization of the financial system. Currently, a few banks hold a dominant control in the USA over the power of finance. CBDCs can leverage this by ciphering the transaction data into a single authoritative ledger. That digital record would not only be the transaction's history but might further include cash flows that were conventionally untraced.

The effects of this centralization are far-reaching and not readily foreseeable. A combined ledger capturing all financial transactions in a country would present an unprecedented objective for cybercrime activators and, therefore, serious security risks. It could also become an instrument of the authorities in their intrusions into the financial lives of citizens. Although appropriate technical solutions could make this risk quite minimal through careful policies, they invariably involve very serious trade-offs between security, privacy, functionality, and accessibility of users.

In the ensuing discussion, we outline the roles that would be integral to a CBDC's operation, the tasks associated with these roles, and the inherent trust placed in them. A threat model tailored to CBDCs is then introduced, covering the core security needs and potential adversaries. A critical analysis follows, examining various digital currency models and their alignment with the threat model.

In live with our review advances with a comparative study that brings to light the weaknesses of CBDC design, exploring security challenges, and the examination of how different CBDC designs might navigate these complex waters. This discourse aims to inform and guide the secure implementation of CBDCs, considering the array of cybersecurity challenges they embody[48].

1) Fortifying the Digital Realm: The Four Cornerstones of CBDC Security

In this digital era, one of the determinants of success for CBDC is inseparable from cybersecurity. Full-

[47] Central Bank Digital Currency: Considerations, Projects, Outlook by Edited by Dirk Niepelt

[48] https://www.atlanticcouncil.org/in-depth-research-reports/report/missing-key/#background

fledged protection from any cyberattack is unavoidable; building government trust toward CBDC integrity is inevitable. To this respect, the adoption of proven cybersecurity frameworks will be indeed valuable, including those by **National Institute of Standards and Technology** (NIST) and **Microsoft**. The present study explores the basic security issues that must be the key contributors toward achieving success in CBDCs:

Safeguarding Access: The access to CBDC should be password enabled with credentials in secure storage. Through simple passphrase protectors, or advanced hardware tokens, these are access keys, losing them may just mean compromised accounts or loss of funds.

Privileged Users: The potential for exclusive access positions, with the power to lock away or withdraw locked funds, already exists in CBDC concepts, making many CBDC protocols similar to pre-existing financial compliance protocols. However, with such a potential, the proper risk management strategy is very important in dealing with insider threats.

Ensuring System Integrity: The environment within CBDC is threatened by 'double-spending'- that may upset the environment. The only means of reduction of that risk is strong control, and more so when the CBDC is off-line capable, therefore open to several unauthorized spendings.

Quantum Resistance: Quantum computing theoretically poses an existential threat to the cryptography on which CBDCs are based. Proactive planning and quantum-resistant cryptographic methods, in advance, are therefore a must in the future-proofing of CBDCs against such advanced computational offenses.

2) A Digital Bastion: The Intersection of Blockchain and Cybersecurity

BCEAO advances into the CBDC age with the cohesion of blockchain technology and security protocols. Blockchain, being immutably decentralized and carrying the stack of security features that inject trust into digital currencies, evokes pain and pleasure—all the more compelling arguments as to why blockchain is inseparably knitted into the fabric of CBDCs.

3) CBDCs and Cybersecurity Enhancement: A Strategic Framework

The development of CBDCs presents a remarkable cascade of change in financial systems and the emergence of new modes of security and trust in digital exchanges. For cases where the initiative for a CBDC comes from the central bank, improvements in cyber security are not only necessary but a basic prerequisite to secure the new monetary instruments. This literature review discusses how CBDCs infuse synergy between BCEAO and cybersecurity.

4) Blockchain: The Backbone of CBDCs

The central pillar of CBDCs is blockchain technology. On the top of this pillar, there is a public record of virtual money dealings that cannot be changed. The result is the transactions become tamper-proof and endurable. It actually is a series of interrelated blocks in which each is securely associated with its preceding block, containing data including transaction values, involved parties, and time records. Blockchain is dubbed transparent by design, guaranteeing that although some participant information is kept confidential, both the occurrence of transactions and their permanence in the system can be seen by the public.

5) Data Security and Management

In a digital economy where information is superior, safeguard and management of data could be considered invaluable. Yet, blockchain goes a step further than the regular machine learning algorithms, encasing identity, safety of transactions, and the communication framework, all within an open framework. Once data is entered into the blockchain, it becomes an immutable, solid, impeccable record of transactions.

6) Blockchain's Role in Cybersecurity for CBDCs

All this makes a sound base for the development of a real digital currency with the help of blockchain technology used for an upcoming CBDC by BCEAO. This can secure a safe, efficient, and transparent medium to undertake the digital transactions that are vital in holding tight to the integrity of the financial ecosystem. At a time when fraud and unauthorized access are rampant, blockchain emerges as a strong shield.

The intersection of blockchain technology and cybersecurity forms a critical component of the infrastructure for CBDCs, such as the one being developed by BCEAO. The immutable and decentralized nature of blockchain inherently enhances the security of digital currencies, safeguarding against fraud and cyber threats. As the BCEAO ventures into the digital currency domain, the strategic application of blockchain technology will be instrumental in fortifying its CBDC against the myriad of cybersecurity challenges it faces. Thus, blockchain emerges not just as a technology of choice but as a strategic imperative for the successful deployment and acceptance of CBDCs in the modern financial landscape[49].

2.5. Synthesis of Literature

[49] Transforming Cybersecurity Solutions Using Blockchain by Rashmi Agrawal, Neha Gupta - 2021

2.5.1. Identifying Gaps and Opportunities for Future Research

We have elaborated in sufficient detail on the importance that virtual currencies are taking on in today's world and detail the growth spurt that it is redrawing financial boundaries. As CBDCs go more mainstream, there's a growing need for new, efficient ways to handle this technology, especially in ways that protect ethical standards, ensure compliance, and fortify cybersecurity. The review covers the recent research and indicates areas of lacking knowledge, pointing out opportunities for innovation and exploration.

1) **Spotlight on Untapped Technological Strategies**

A significant gap has been detected in the lack of strategic approaches tailored for the management of CBDC technology. There's a scarcity of research on how to effectively harness various digital platforms for CBDC operations, indicating a pressing need for studies that can lay a solid foundation for the technological stewardship of these currencies.

2) **Overlooking Crucial Technological Aspects**

Another area where literature falls short is in addressing key technological aspects crucial for CBDC's smooth functioning. Matters such as enhancing laptop battery life, multitasking capabilities, and securing internet connections for CBDC transactions are largely unexplored. This oversight points to the necessity for in-depth research to ensure the continuous and secure operation of CBDC infrastructures.

3) **Performance Evaluation: An Uncharted Territory**

The effectiveness of new technological management methods in the CBDC landscape remains unevaluated, particularly concerning the ISO/IEC 25010:2011 system quality model's criteria. The absence of such evaluation is a roadblock to confirming the reliability and future-proofing of CBDC systems.

4) **Compliance Considerations Left in the Shadows**

Literature on the compliance of CBDCs is surprisingly scant. CBDC systems must conform to the digital regulatory framework and banking law. This aspect, however, is under-researched, opening it up to probable legal and regulatory conundrums.

5) **Security: The Missing Chapter**

Despite security being a cornerstone concern for CBDCs, the research on cybersecurity measures, data protection protocols, and threat mitigation is inadequate. Bridging this gap is fundamental to maintaining the integrity and trust of CBDC systems.

6) **Implications and Pathways Forward**

Filling the current gaps is a breakthrough in making CBDCs fit perfectly in the existing financial systems. Developing new strategies to regulate the technology, researching new areas such as battery efficiency and infocomm security, addressing the effects on ethical, regulatory, and security issues, all

work together to make overall CBDC infrastructure more robust.

7) Addressing the Regional Research Gap in CBDC Development

The assessment of the current regional trends with respect to CBDCs reveals a striking absence of involvement in research work and maybe even interest, more so in the African continent. This gap suggests that while the rest of the world is making great strides with the uptake of digital currencies to improve the socio-economic life of their people, the African continent, and in fact the rest of the economic belt, seems to be lagging. The information finds that there is a troubling shortage of queries or searches regarding CBDCs in this area over the past decade, one that hints at potential negligence or missed opportunity in the evolution of digital finance. This trend calls for a complete reassessment and increased focus towards the African continent concerning the development and implementation of CBDCs.

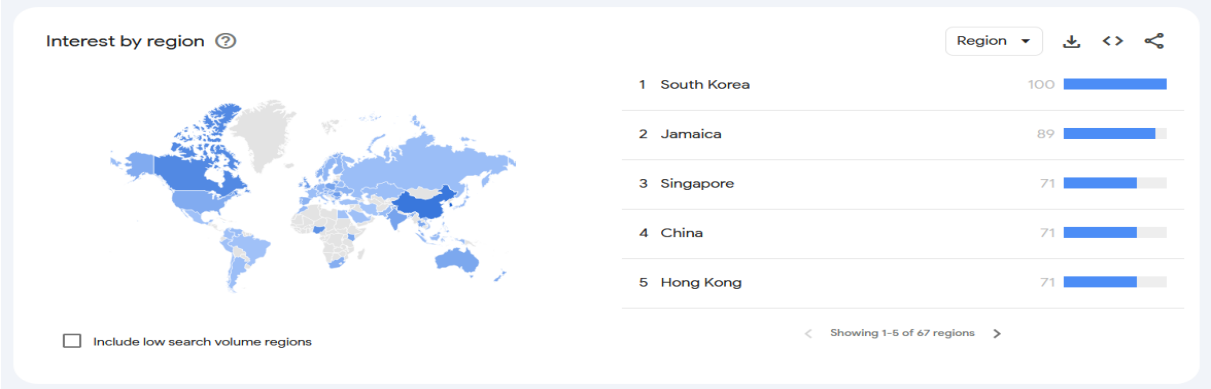


Figure 9: CBDC trend in the world

Source: https://trends.google.com/trends/explore?date=today%205-y&q=CBDC&hl=en

This trend presents a critical reassessment and increases the focus of CBDC developments and implementations with respect to the African region. It underscores the need for targeted research initiatives, policy discussions, and educational outreach to bridge this gap. All these will be an active participation in and investment within the digital currencies in the region that will or would not have been allowed to miss out in this move toward global financial systems using digitization. The general approach would indeed support the promotion of inclusive growth and equal opportunity for access to finance by using innovative solutions related to digital currencies.

2.5.2. Relevance to Thesis Objectives

Literature indicates that CBDCs will be a significant innovation for stabilizing financial systems, but there is little empirical evidence concerning effects on economies during financial crises particularly towards banking regulations, and compliance with AML/CFT/CPF requirements. In addition, the ethical role of CBDCs in such intricate settings is not adequately investigated. The key disadvantages outlined

in the last chapter (2.5.1. - Identifying Gaps and Opportunities for Future Research) demonstrate the significance of this thesis in gathering the missing pieces and answering the basic questions of CBDC development. The contribution towards stabilization in economies was settled in current literature, yet the failure was to look into a scarcity of empirical evidence in the economies where financial crisis dominated. More research must be performed to bridge this gap and establish that economic stability is everywhere present from the usage of CBDCs.

As already highlighted, the research gaps that currently exist require filling, and this thesis represents an initial effort to demystify these under-researched areas for the purpose of advocating a safe, ethical, and regulation-compliant integration of CBDCs into the world financial system. Through the filling of these research lacunae, the thesis contributes to both the discussion and technological advancement required to realize the full potential of CBDCs in revolutionizing digital and financial payments.

SECTION TWO: RESEARCH METHODOLOGY AND

FINDINGS

III. DATA AND METHODOLOGY

3.1. Introduction

Our exploration of the ethics, compliance and cybersecurity aspects of CBDC unfolds in this section. Through a methodical lens, we critically assess how these dimensions manifest today banking sector around the world and then applying our methods to the specific context of Mali within the UEMOA sphere. We outline our research methodology, elaborating the philosophical frameworks that drive our inquiry, as well as structural design that organizes it, hence guaranteeing that all the stages ranging from hypothesis formulation to conclusion are firmly rooted in a robust empirical foundation.

Working for excellence in research philosophy design, methodology, and data collection, coupled with the ambitious nature of the study, must be possible and moral at the same time. We go far beyond mundane numbers and statistics and choose a series of quality both in qualitative and quantitative data that best reflects the realities of the Malian banking landscape. The sectoral and geographical scope of the research makes possible an examination of the context surrounding, and which is surrounded by, the ethical practices of CBDCs. As such, the research is always beyond pure theory to the real impact of digital currencies in a recognizable economic and cultural context.

The research design is the minimum structure that frames our study by specifically outlining the questions that are posed. We elaborate on the methodologies employed for sampling and data collection, guaranteeing that we acquire thorough and representative data. The financial landscape of Mali is meticulously outlined with statistical data, situating it within the global and regional banking frameworks, while emphasizing its significance as a pivotal locus for analyzing digital currencies in a developing economic context. We do an all-round analysis of our sample data selection methodology: we build on statistical techniques and go on with analytical methodologies that we will describe in detail on this chapter.

3.2. Research Philosophy

Starting in the 1990s, incompatibility thesis had been rejected by many researchers advocating the pragmatic position that quantitative and qualitative research are very important and should often be judiciously mixed in single research studies (R. Burke Johnson and Larry Christensen - 2020)[50]. According to pragmatism, what is ultimately important and justified or "valid" is what solves our problems and what works in particular situations in practice and what promotes social justice. Pragmatisms focused on the ends that we value.

[50] Educational Research : Quantitative, Qualitative, and Mixed Approaches - Seventh Edition By R. Burke Johnson and Larry Christensen

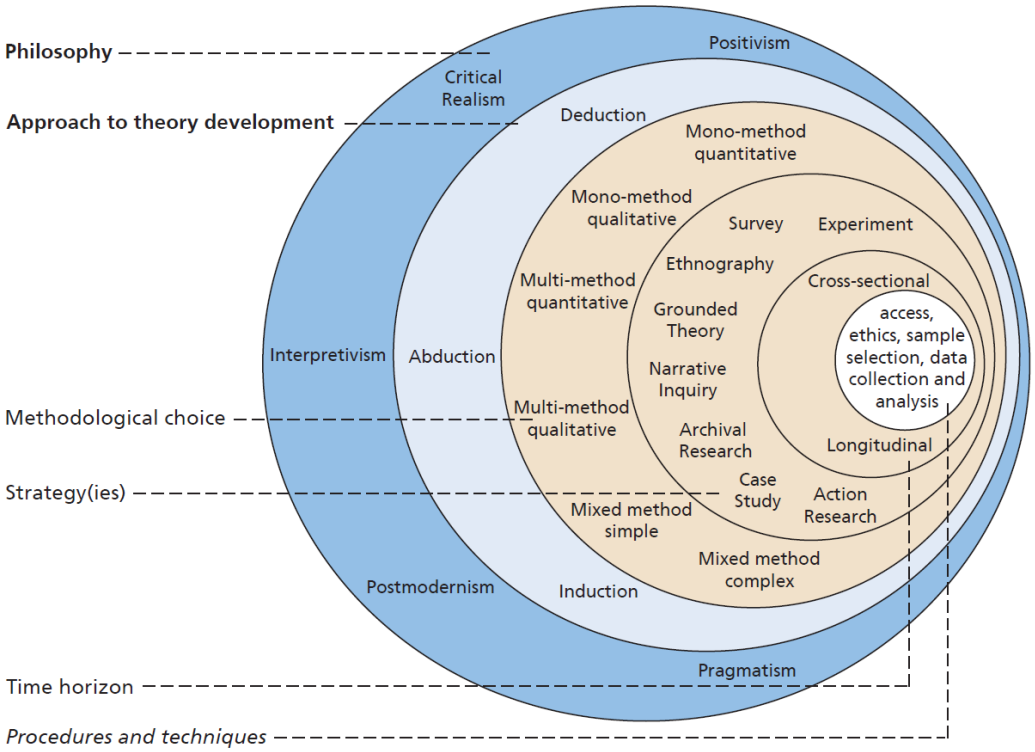


Figure 10: The 'research onion'

Source: *2022 Mark NK Saunders; developed from Saunders et al. 2019*

According to pragmatism, our research design should be planned and conducted based on what will best help to answer our research questions; the result is pragmatic knowledge. Pragmatism says that theories or programs or actions that are demonstrated to work for particular groups of people are the ones that we should view as currently being the most valid for those people. We specifically call our much-expanded version of pragmatism "**dialectical pluralism**" (Johnson, 2017)[51] because a philosophy for mixed research should carefully listen to ideas, assumptions, and approaches found in qualitative and quantitative research and in any other relevant domain. The word dialectical is intended to imply a dynamic back-and-forth listening to multiple perspectives and multiple forms of data. Although mixed methods research is still the "new kid on the block," the list of researchers identifying with this approach is increasing rapidly.

The term **research philosophy** refers to a system of beliefs and assumptions about the development of knowledge. Although this sounds rather profound, it is precisely what you are doing when embarking

[51] How to Construct a Mixed Methods Research Design ; Judith Schoonenboom · R. Burke Johnson
Published online: 5 July 2017 - https://pubmed.ncbi.nlm.nih.gov/28989188/

on research: developing knowledge in a particular field[52]. The knowledge development you are embarking upon may not be as dramatic as a new theory of human motivation, but even addressing a specific problem in a particular organization you are, nonetheless, developing new knowledge. Your research philosophy sets out the world view within which your research is conducted. As shown in the opening vignette, the assumptions of the world view within which research is undertaken are important, impacting which data are privileged and how they are interpreted.

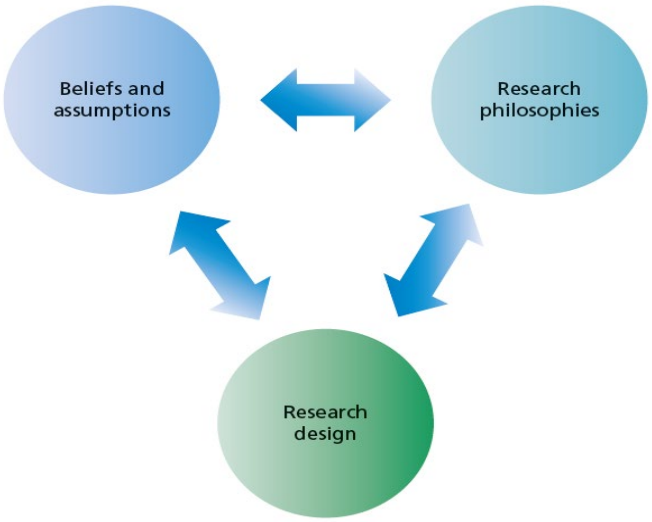


Figure 11: Developing your research philosophy: a reflexive process

Source: *Alexandra Bristow and Mark Saunders 2015*

There is continuous refinement and alignment of research decisions **to this reflexive process. Beliefs and assumptions** influence the **choice of research philosophy,** which in turn guides the **research design.** However, the process is reflexive, meaning that insights gained from research design and execution may lead the researcher to **reconsider their beliefs, assumptions, and philosophical stance.** We emphasize that developing a research philosophy is **not a linear process** but rather a **reflective and iterative one.** Researchers must critically evaluate their own assumptions, understand different philosophical paradigms, and align their research design accordingly

Crafting a high-quality thesis requires a thoughtfully formulated research philosophy, which serves as the backbone for selecting appropriate methodologies, data collection methods, and analysis techniques.

[52] **Research Methods for Business Students -** NINTH EDITION ; Pearson Education Limited
Mark N.K. Saunders, Philip Lewis and Adrian Thornhill - 2023 (Ninth Edition) -p131

Saunders, Lewis, and Thornhill (2023) describe the term of research philosophy to a system of beliefs and assumptions about the development of knowledge[53]. This foundation is crucial in ensuring that the research approach, data gathering, and analysis are all well-aligned and effective for the study's aims.

Our research on the CBDC on a relatively new subject compared to the history of the currency, but however this currency has already been launched by several central banks around the world but also in the UEMOA zone. Our objective in this research is to understand how the CBDC works and its ethical side. In addition, we wish to understand the challenges presented by this new currency in terms of Regulatory Compliance of Central Banks based on the opinions of professionals or people working in this environment, as well as the expectations of regulators and the general public. After that, we will be able to determine quite precisely the mandatory ethical aspects linked to the CBDC and its choice of mechanical design.

In addition, our study aims to determine whether the CBDC can meet the expectations of all parties in compliance with the texts and jurisdiction of the fight against financial delinquency, AML/CFT/CPF as well as the difficulties to be overcome in this application and in ultimately make proposals and suggestions. Therefore, we adopt pragmatism as a philosophical hypothesis, which combines a qualitative with a quantitative approach.

The Pragmatic Worldview

Another position about worldviews comes from the pragmatists. Pragmatism derives from the work of Peirce, James, Mead, and Dewey (Cherryholmes, 1992) [54]. ***Pragmatism*** as a worldview arises out of actions, situations, and consequences rather than antecedent conditions (as in postpositivism). There is a concern with applications what works and solutions to problems (Patton, 1990). Instead of focusing on methods, researchers emphasize the research problem and use all approaches available to understand the problem (see Rossman & Wilson, 1985). As a philosophical underpinning for mixed methods studies, Tashakkori and Teddlie (1998), Morgan (2007), and Patton (1990) convey its importance for focusing attention on the research problem in social science research and then using pluralistic approaches to derive knowledge about the problem. Based on Cherryholmes (1992) and Morgan (2007), Creswell, John W provides a philosophical basis for pragmatism research:

---

[53] Research Methods for Business Students - NINTH EDITION ; Pearson Education Limited
Mark N.K. Saunders, Philip Lewis and Adrian Thornhill - 2023 (Ninth Edition) -p131

[54] RESEARCH DESIGN - Qualitative, Quantitative, and Mixed Methods Approaches by JOHN W. CRESWELL - THIRD EDITION

- ***Flexibility in Philosophy and Reality***: Pragmatism is not tied to a single philosophy or reality, allowing researchers in mixed methods studies to draw from both quantitative and qualitative assumptions (Morgan, 2007; Cherryholmes, 1992).
- ***Freedom of Methodological Choice:*** Researchers have the liberty to select methods, techniques, and procedures that best suit their research goals.
- ***Multiple Approaches to Data Collection and Analysis:*** Unlike approaches that adhere strictly to quantitative or qualitative methods, pragmatism advocates for the use of multiple methods for a more comprehensive understanding (Patton, 1990).
- ***Practical Definition of Truth:*** In pragmatism, truth is viewed as what works at a particular time and is not confined to a single reality, either independent of or within the mind. This approach allows mixed methods researchers to use both quantitative and qualitative data for a better understanding of research problems.
- ***Focus on Research Purpose and Consequences***: Pragmatic researchers prioritize the goals and intended outcomes of their research, establishing a clear rationale for mixing quantitative and qualitative methods (Tashakkori and Teddlie, 1998; Morgan, 2007).
- ***Contextual Nature of Research***: Pragmatism acknowledges that research is influenced by its social, historical, and political context, and thus, mixed methods studies may incorporate postmodern perspectives, focusing on social justice and political objectives.
- ***Reframing Questions about Reality***: Pragmatists recognize an external world independent of the mind but prefer to move beyond traditional questions about reality and nature's laws, focusing instead on practical inquiries (Cherryholmes, 1992; Rorty, 1983).
- ***Embracing Diverse Methods and Perspectives***: Pragmatism in mixed methods research opens the door to a variety of methods, worldviews, assumptions, and data collection and analysis techniques.

Any research philosophy can be criticized; therefore, pragmatism is our research philosophy. According to our research philosophy assumption, it determines our direction to select methods, the way of data collection, and analysis.

3.3. Research Design

C.R. Kothari (2004)[55] define as follow "*A research design is the arrangement of conditions for collection and analysis of data in a manner that aims to combine relevance to the research purpose with*

[55] Research Methodology - Methods and Techniques (SECOND REVISED EDITION) By C. R. Kothari

economy in procedure". In fact, the research design is the conceptual structure within which research is conducted; it constitutes the blueprint for the collection, measurement and analysis of data. As such the design includes an outline of what the researcher will do from writing the hypothesis and its operational implications to the final analysis of data.

Research design is the action plan or blueprint of the research. It should provide a logical sequence of activities that allows the reader of your project to see the connections between the research questions that you have posed in the introductory chapter of the project, the approach that you adopt to address the questions, the assumptions underlying your approach, how you collect and analyses your data, as well as your findings and conclusions. These choices require careful deliberation (John Kuada 2012)[56].

In line with our pragmatic approach that embraces mixed methods, we proceed to the pivotal phase of sampling. As elucidated by Andrew, Pedersen, and McEvoy (2019), sampling represents the mechanism through which researchers select participants. This phase is of utmost significance in our research process (Andrew et al., 2019). The design of our methodology requires the creation of two separate sampling groups: one dedicated to qualitative research and the other to quantitative research. The sampling strategy bifurcates into probability and non-probability sampling. Probability sampling, operates on a random selection principle, offering every individual in the population an equal chance of being selected. Conversely, non-probability sampling, as Easterby-Smith ET AL. (2015)[57] highlight, aims for purposeful sample selection to heighten result accuracy. In our study, we employed non-probability sampling for the qualitative aspect and probability sampling for the quantitative data.

Aspect	Qualitative Research	Quantitative Research
Purpose	To capture an in-depth, complex picture.	To quantify variables and elucidate patterns.
Researcher's Knowledge	Begins with a broad question; specifics emerge with engagement.	Begins with a specific question/hypothesis to be tested.
Timing in Research	Ideal for initial exploratory phases.	Suited for confirmatory phases, post-exploration.
Research Design	Flexible and developing as the study progresses.	Structured and fixed from the outset.
Role of Researcher	Primary instrument for data collection; close engagement with subjects.	Utilizes tools and standardized instruments for data collection.
Data Form	Textual, visual, or physical manifestations.	Numerical, suitable for statistical analysis.
Perspective	Subjective interpretation is key; understanding participant viewpoints.	Objective measurement; focusing on statistical objectivity.
Data Richness	Deep, nuanced, and context-rich; however, more labor-intensive to collect.	Streamlined and efficient for analysis; may lack depth in context.
Researcher's Involvement	Tends to become personally involved in the subject matter.	Maintains a detached, unbiased stance towards the subject matter.

[56] Research Methodology - A Project Guide for University Students by John Kuada ; 1st e-edition 2012
[57] Management and Business Research 5th Edition – 2015 ; By Mark Easterby-Smith, Richard Thorpe, Paul R. Jackson

Aspect	Qualitative Research	Quantitative Research
Participant Numbers	Typically smaller, focused samples providing depth.	Larger samples necessary for statistical validity.
Outcome Contribution	Generates new theories or expands on existing ones.	Tests and confirms existing theories.
Research Process	Iterative, with potential back-and-forth between collecting and analyzing data.	Linear and sequential, with a clear progression from data collection to analysis.
Interpretation of Data	Open-ended, leading to multiple potential insights.	Seeks singular, definitive conclusions where possible.
Suitability	Excellent for complex social phenomena where context and depth are required.	Best for research requiring clear, definitive conclusions and numerical representation of data.
Theory Development	Contributes to the development or understanding of theories based on observed behaviours and experiences.	Contributes to theory testing and refinement through empirical data analysis.
Sample Size Generalization	Less emphasis on sample size for generalization; more on depth of information per case.	Relies on large sample sizes for broad generalizability.

Table 2: Features of Qualitative Research vs. Qualitative Research

3.4. Research Method

Once our research questions are clear and have learned about the basic foundations of research, we are ready to decide on the most appropriate research method(s) for our study.

In ***quantitative*** research, the research questions often ask about the relationships among variables that you are interested in, especially independent (causal) variables and dependent (outcome) variables.

In ***qualitative*** research, the research questions often ask about what you would find if you were to explore, describe, and explain some phenomenon in a local or particular place.

3.4.1. Qualitative Data Collection Methods

Defining what qualitative research is, as opposed to what it is not, presents a challenge, as the term is used to cover a wide range of methodological and epistemological paradigms. However, in educational research, the focus of such studies is on an in-depth probing of phenomena such as people's beliefs, assumptions, understandings, opinions, actions, interactions or other potential sources of evidence of the processes of learning or teaching.

As we have defined our top research questions on section 2.5.1. (Identifying Gaps and Opportunities for Future Research), in our research on "Optimizing the Ethical Dimensions of Banking Compliance and Cybersecurity for Digital Currency," we analysed the rationale behind the design of the CBDC operating strategy and solicited the expertise of experienced professionals.

Our selection process targeted professional networks, particularly via LinkedIn as well as our professional relationships and contacts and members of several groups sharing thoughts on money

laundering and cybersecurity. This allowed us not only to expand the scope of our information sources, but also to increase the quality of the information collected. We have therefore respected the qualitative collection process as indicated in the image.

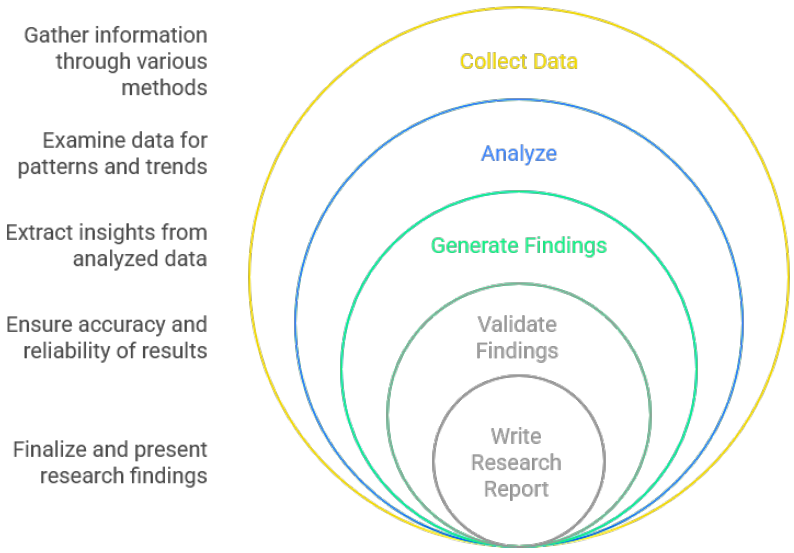


Figure 12: Qualitative research process

We started by developing an online survey using Goodle-Form. Google Forms, part of Google's free Google Docs Editors suite, is a versatile survey creation tool. It offers several benefits, including real-time data collection and analysis, wide accessibility and reach, and effective data visualization and reporting, all at no cost. Then find the contact details of a group of 120 financial and technology professionals and share this form with them. This included people working in banks, central banks, AML and financial crime units, digital currency companies and other professionals working in the field of AML/CFT/CPF.

N°	Interviewee	Role	Position
1.	**Dr. Ismail Sissoko**	Doctor, Teacher, Researcher in IT field	Doctor Researcher
2.	**Dr. Adama Togola**	Director of IT Department, Bank of Africa Mali	Director
3.	**Dr. Ibrahima Sogoba**	IT and Law Specialist	Entrepreneur
4.	**Dr. Julian Rowel**	Chief of GRC (Governance, Risk, and Compliance)	United Nations
5.	**Mr. Moussa Konate**	Professor of Finance and Accounting	Professor
6.	**Mr. Souleymane Tieman Kane**	IT Expert, Former Worker at MINUSMA	Entrepreneur
7.	**Mr. Ousmane Sow**	IT Specialist	Employee
8.	**Mr. Youssouf Dembélé**	IT Engineer, Cybersecurity Specialist	IT Manager

Table 3: Interviewee participants

We have prioritized professionals, those who have very in-depth knowledge of our research subject in order to obtain qualitative results. Of all the people we contacted, nine responses stood out. These

responses led us to meet people working in the field of digital currency operations, well-known experts in the field who had agreed to discuss with us about the ethical aspect of this new technology. The topics of discussion or questions focused on the aspect of money laundering using CBDC, the possibilities that this currency can offer for criminals wishing to use it to finance terrorist groups and finally the cybersecurity risks. linked to this currency.

3.4.2. Quantitative Data Collection Methods

A quantitative approach means using measurements and numbers to help formulate and test ideas[58] Elaine Wilson[2017]. It usually involves summarizing numerical data and/or using them to look for differences and associations between sets of numbers. Quantitative method is justified because the philosophical worldview of the researcher and the paradigm orientation of this study (positivism/positivist) aligns with and corresponds to a quantitative method (Creswell, 2009). Moreover, it enables the application of relevant statistical methods for analyzing data, yielding results from larger, population-representative sample sizes. The study also utilized numerical data and measured variables, testing hypotheses grounded in theoretical principles to enhance both the reliability and validity of the data and the study's outcomes. Quantitative researchers tend to seek explanations and predictions that, in most cases, will generalize to other persons and places. The intent is often to identify relationships among two or more variables and then, based on the results, to confirm or modify existing theories or practices. Researchers typically identify only a few variables to study and then collect data specifically related to those variables. Methods of assessing each variable are identified, developed, and standardized, with considerable attention given to the validity and reliability of specific instruments and other assessment strategies (more about such qualities later in the chapter). Data are often collected from a large sample that is presumed to represent a particular population so that generalizations can be made about the population [P. D. Leedy, J. E. Ormrod, L. R. Johnson][59].

Furthermore, it gives researchers the flexibility to select specific variables for investigation and to employ closed-ended questionnaires. This approach typically produces results that are more objective and have higher reliability and validity compared to qualitative and mixed methods. Additionally, it is more cost-effective and time-efficient in terms of data collection and analysis than qualitative and mixed-method approaches. Besides, it guarantees a high level of standardization, validity and reliability, and it makes it much easier to compare the findings obtained and generalize to a larger population (Healey, 2009). This will consist of a single quantitative data collection and analysis technique through

[58] School-based Research - A Guide for Education Students, 3rd Edition by Elaine Wilson - Elaine Wilson, 2017.
[59] Practical Research: Planning and Design, 12th Edition ; Authors: Paul D. Leedy, Jeanne Ellis Ormrod, Laura Ruth Johnson

the survey questionnaire which will be administered using an online channel. This technique has been chosen since it can support this study, essentially by addressing the research questions in order to achieve the objectives of this research.

Therefore, a quantitative method was selected to explore another dimension of the study. This approach was utilized to examine the causal relationships between CBDC technologies and adherence to banking laws. In applying the quantitative method, the researcher formulated predefined expectations or hypotheses about the study's outcomes. This process involved adopting a deductive approach and a scientific methodology to analyze the cause-and-effect dynamics within the scope of the research. Therefore, we use probability sampling for the survey and questionnaires to enable gather numerical data on the awareness, attitudes, and practices related to ethical dimensions, compliance, and cybersecurity among professionals in the banking sector and other stakeholders. Analyze quantitative data to identify patterns, correlations, or trends in attitudes and practices regarding CBDCs.

For This second research method, Google Form helps again, allowing people to answer they surveys conveniently. We use a kind of random sampling method from different working regions, which are not only from the finance field. Furthermore, using snowball sampling, we sent the link to friends and colleagues who are from different working regions; all of them replied to us and helped us to spread our survey on their social media platform like LinkedIn, Facebook and WhatsApp. It is unable to count the respondents who have not completed and quit the system in advance; that is our limitation of survey. We predict that apart from the three respondents who are in direct contact with us, there may be other respondents who withdraw from the questionnaire in advance because they do not know about our topic. We received **196 valid surveys from people** in different fields, teachers, students, finance, AML/CFT/CPF, technology, Bank professionals, Digital Currency professionals.

3.4.3. Mixed Data Collection methods

Mixed methods research combines strengths of quantitative and qualitative research; it often both explores and generates new knowledge and tests relationships we think exist (e.g., hypothesis testing). It is a key idea in research that “Research methods are subservient to and follow the research questions”. The goal is to determine the best way(s) to answer our research questions[60].

The integration of both qualitative and quantitative methodologies within a single study, known as the mixed methods approach, has been gaining traction in recent years, as noted by Creswell (2003) a

[60] Educational Research : Quantitative, Qualitative, and Mixed Approaches - Seventh Edition By R. Burke Johnson and Larry Christensen

prominent figure in the field of research methodology. Easterby-Smith et al. Easterby-Smith et al. (2015) found that the use of mixed methods enhances the validity and reliability of research. Furthermore, it provides a robust foundation for theoretical development and encourages the examination of issues from diverse perspectives to generate effective solutions for research and social challenges.

However, it's important to acknowledge, as Onwuegbuzie, Johnson, and Collins (2009) point out, that mixed methods research can be demanding in terms of time and resources, requiring significant input from both qualitative and quantitative aspects for thorough analysis. For our study, this approach is particularly advantageous. It allows for a comprehensive data collection, encompassing insights from professionals through qualitative research and broader public opinions through quantitative methods, aligning well with our research objectives and questions. Consequently, it necessitates more questions than a qualitative survey but typically fewer questions than a quantitative study

Easterby-Smith et al. (2015) identify two crucial design choices in mixed methods research: sequencing and dominance. Even though in the current study we have gathered qualitative and quantitative data at the same time, aiming at a comprehensive analysis, our study is sharply tilted towards qualitative domination. This tilt arises from our research framework, which appreciates broader insights and increased levels of nuanced understanding that become accessible through qualitative research from wide perspectives, divergent from the rather public-centric focus that characterizes quantitative research. However, although the focus is on qualitative research, focusing on taking the overall approach, we believe as well in the eminent importance of data in both forms, qualitative and quantitative.

We have opted for a mixed-methods approach, integrating qualitative insights from financial experts on CBDCs and quantitative data from financial service users to ensure a comprehensive analysis aligned with our research objectives.

3.5. Sampling and Data Collection Methods

This study's data collection involved three distinct sources:

Firstly, we carried out online interviews among the important stakeholders, covering both industry and firm-level information. The interviews were therefore carried out with greater priority placed on professionals from the banks and electronic money institutions in the UEMOA region and beyond the region. Other appropriate respondents from the general public comprised IT experts, professors from universities, and CBDC users. Both primary and secondary data were collected at the same time, where the use of primary data was sought directly from the banks in Mali. This was done online because it is adaptable and convenient enough for professional respondents. The field work for primary data started on Monday, November 13th, 2023, and should close on Thursday, October 31st, 2024. This timeline was purposely picked to allow an effective judgment of the financial system while it is relatively stable.

Our secondary data included a comprehensive questionnaire developed online for the purpose of conducting an online survey. Consisting of 17 questions, the employees could take this survey at their convenience, offering in-depth insights into the information security readiness and resilience at the individual and organizational levels. Analyzing this data gives detailed information. The overall results were further elaborated with a detailed discussion focusing on the potential scientific directions sensitized and critical research paths. Respective, the study discussed an extensive list of AML legislation and cybersecurity measures by underscoring the associated struggles alongside the necessary benchmarks to progress within the technology of CBDCs.

The third source of data was literature studies. Regarding literature studies, we based our approach on the method described by Webster and Watson[61] which involved an in-depth review of primary documents and on-site interviews, guided by the methodology.. In this approach, we sourced literature from reputable journals and expanded our research through backward and forward tracing of cited and citing papers, including recent conference papers.

The literature review of this study undertook three distinct functions. First, it served as a sturdy base and foundation for the case study being undertaken, in that it presented important background information. Second, it was a means of data collection in regard to our case of interest. Thirdly, it provided an international perspective on our research question and helped us understand within a global frame.

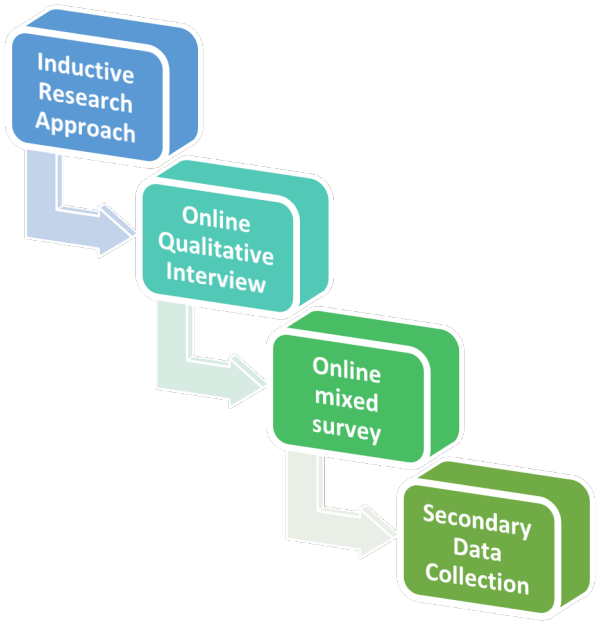


Figure 13: Sampling and Data Collection Methods

[61] Physical and Digital Security Mechanisms: Properties, Combinations and Trade-offs by Author: André van Cleeff Type: PhD Thesis - University of Twente - Publication Date: June 3, 2015

3.5.1. Inductive Research Approach

In the current research, an inductive methodology has been selected where ethical concerns, banking compliance, and cybersecurity considerations of deploying CBDCs form objects of comprehensive research investigation. An inductive method is typically used in developing theories from data that have been collected based on participants' experience or point of view in place of testing pre-existing hypotheses. As such, it starts with broad research questions meant to explore different dimensions of CBDCs without assuming anything beforehand. We focus, to highlight experienced lived by practitioners in the field, maybe to find patterns, threads, and meaning or insight emerging from their stories. The research questions to be answered in this study are:

- *What ethical concerns do professionals perceive in the implementation of CBDCs?*
- *How do professionals navigate the compliance challenges associated with CBDCs?*
- *What are the critical cybersecurity threats encountered in the context of CBDCs, and how are they addressed?*

Subsequently, we devise a methodology that employs in-depth interviews and open-ended survey inquiries to collect comprehensive, descriptive information. This approach facilitates a profound understanding of participants' viewpoints and also offers the adaptability to investigate unforeseen subjects that may emerge throughout the data collection process.

We will conduct expert interviews as part of conducting qualitative research among a diversified group that includes banking, cybersecurity, and CBDC compliance experts. It will go to great lengths to extract personal experiences from the experiences of the participants, and detailed elaboration will be obtained regarding their work or engagement with CBDCs. Key topics explored include:

- **Personal Experiences with CBDCs:** Participants share their direct involvement with CBDC projects, highlighting the challenges and opportunities they encountered.
- **Perceptions of Ethical Concerns:** Participants share how ethically different they feel CBDCs are compared to traditional forms of a central bank regarding their experiences.
- **Navigating Compliance Challenges:** Respondents give examples of specific compliance challenges they have encountered and what they did to deal with them.
- **Impact of Emerging Technologies:** Respondents comment on how emerging technologies, particularly blockchain, have influenced their professions in the context of CBDCs, categorizing these influences into those that have been facilitating and those that have been complicating.

- **Experiencing Cybersecurity Threats:** Participants recount instances of cybersecurity threats or breaches related to CBDCs and how these were managed.
- **Adapting Regulatory Strategies:** Participants offer insights into how regulatory bodies should adapt to effectively govern CBDCs based on their experiences.
- **Balancing Privacy and Compliance:** Participants discuss instances where they had to balance privacy concerns with compliance requirements in CBDC operations.
- **Enhancing AML/CFT/CPF Protocols**: Participants discuss their opinions about how CBDCs influence AML/CFT/CPF protocols in their industries.
- **Future Outlook on CBDCs:** Participants consider future trends and innovations in CBDCs and how these might affect banking compliance and cybersecurity.

The inductive approach would be used as a research strategy to develop new theories and insights from the actual experience of professionals dealing with CBDCs. The output will discuss ethical considerations, challenges in terms of regulatory compliance, and related cybersecurity risks for CBDCs. Such knowledge would be of great benefit to regulators, financial institutions, and developers of technology with regard to CBDC operationalization so that it is secure, compliant, and ethically responsible. The method should permit detailed analysis to be done in regard to the perspectives of people and their reaches in how the new phenomenon will work in real life, thus enabling the formulation of new theories and insights that will follow cryptocurrencies. In that sense, the research is derived from realities of practice with actionable insights and recommendations for the future of digital currency in the banking industry.

3.5.2. Online Qualitative Interview

According to John W. Creswell [2013][62], there are five interrelated steps in the process of qualitative data collection. These steps should not be seen as linear approaches, but often one step in the process does follow another:

1. **Identify participants and sites:** selecting the individuals and locations that will best help in understanding the central phenomenon and research questions.
2. **Gain access to these individuals:** having permissions to interact with participants and visit sites or by phone contact.

[62] Qualitative inquiry and research design : choosing among five approaches By John W. Creswell. 3rd ed.

3. **Types of information:** deciding on the kind of data that will effectively answer the research questions.
4. **Design protocols or instruments:** creating tools for collecting and recording the necessary information.
5. **Data collection:** conducting the actual data gathering while being mindful of potential ethical issues.

Creswell emphasizes the distinction between quantitative and qualitative methodologies in collecting data as described earlier. Our sampling method favored those who had hands-on experience and knowledge experts in CBDCs and related areas. We applied expert sampling in our purposive strategy to include experts who were very experienced in bank compliance, cybersecurity, and digital currencies. After having chosen our participants, we created a semi-structured interview schedule for eight participants and performed the interviews online through Ms Teams or over the telephone. Semi-structured interviews, being guided but not restricted in what they address (Easterby-Smith et al., 2015), allow participants to answer freely with their opinions. Background information such as industry alignment was collected in the initial section of the interview. Second-stage questions then probed their knowledge regarding currency, digital currency, and CBDCs in particular. In the second section, where the topics discussed the AML/CFT/CPF and cybersecurity area, open-ended questions were used to gain a detailed understanding of the nature and design aspects of CBDCs.

The interview process was divided into two stages:

1. **Stage 1:** Gathering background information, such as industry affiliation and professional experience.
2. **Stage 2:** Exploring participants' understanding of currency, digital currency, and specifically CBDCs, with a focus on areas like AML/CFT/CPF and cybersecurity. Open-ended questions were used to obtain detailed information about the characteristics and design choices of CBDCs.

Key Topics Explored:

In-depth interviews were conducted with key stakeholders to gain qualitative insights into:

1. **Money Laundering Offense:** Exploring the practical challenges and potential solutions offered by CBDCs in combating money laundering.
2. **Terrorism Financing:** Understanding the mechanisms of terrorism financing and how CBDCs can mitigate these risks.
3. **Financing of Weapons of Mass Destruction:** Investigating the potential of CBDCs to enhance monitoring and enforcement mechanisms to prevent WMD financing.

4. **Customer Due Diligence:** Examining how CBDCs can improve the processes involved in customer identification, verification, and risk assessment.
5. **Politically Exposed Persons:** Analyzing the challenges in managing PEP risks and the role of CBDCs in enhancing monitoring and reporting mechanisms.
6. **Record Keeping:** Discussing the benefits of CBDCs in improving record-keeping practices through secure and immutable transaction records.
7. **Reporting Requirements:** Assessing how CBDCs can streamline and enhance the reporting process for suspicious activities and large transactions.

At the initial contact with the respondents, we explained the purpose of the study, described the research design, and guaranteed that personal data would not be disclosed, but rather used only for research purposes. They were further informed that the interview would take approximately 30 minutes and would be recorded; this was upon getting their consent. A total of nine respondents agreed to the interview. Informed consent was obtained from participants by repetition at the time of interviews, with emphasis repeated on the recording of sessions. They confirmed they had understood this consent. We interviewed questions relating to our objectives of research, and their recorded responses were played back to them, as reported in an archived manner. Since the participants were French-speaking, the recordings are documented in French. Key points are translated to English for the purposes of analysis.

After collecting all the interview data, we used a **color-coded brick coding** technique to analyze the information. As described by Miles & Huberman (1994, p. 56), "Codes are tags or labels for assigning units of meaning to the descriptive or inferential information compiled during a study".[63] These codes can apply to various text segments, such as words, phrases, sentences, or entire paragraphs. We interpreted and analyzed the interviewees' experiences to identify patterns and draw conclusions. Additionally, we focused on identifying keywords to further analyze the data and derive our conclusions.

By following this structured approach, we ensured a thorough and ethical data collection process that provided deep insights into the ethical dimensions, banking compliance, and cybersecurity related to CBDCs.

3.5.3. Online mixed survey

It is on this premise that the online mixed survey in this study has combined both quantitative and qualitative approaches for comprehensive data from professional and expert boundaries of banking

[63] Qualitative Data Analysis: An Expanded Sourcebook / Matthew B. Miles, A. Michael Huberman. 2nd ed.

compliance, cybersecurity, and CBCDs. This will, in turn, deeply explore participants' opinions, life experiences, and meaning attached by participants to the experiences for a fine-grained understanding of ethical dimensions, challenges of compliance, and cybersecurity threats related to CBDCs.

The survey objectives are to identify and confirm challenges that affect some aspects of banking compliance and cybersecurity, and to assess benefits accruing from the implementation of ethical dimensions in the CBDC frameworks as ways of responding to these challenges.

Survey Objective: The survey identifies and confirms the challenges that affect some aspects of banking compliance and cybersecurity and evaluates benefits accruing from the implementation of ethical dimensions in the CBDC frameworks as ways to respond to these challenges.

Key Areas Explored:

1) **Personal Experiences with CBDCs:** Understand participants in direct contact with CBDCs and how they encountered challenges and opportunities.
2) **Perceptions of Ethical Concerns:** Discuss how ethical concerns about CBDCs are perceived by participants in comparison with traditional systems of banking.
3) **Navigating Compliance Challenges:** Specify situations where the participants felt that compliance challenges pertaining to CBDCs were overcome and how these challenges were overcome.
4) **Impact of Emerging Technologies:** Explore how the use of emerging technologies, such as blockchain, has influenced participants working with CBDCs.
5) **Experiencing Cybersecurity Threats:** Gather information from participants about the experience regarding cybersecurity threats or breaches relating to CBDCs and how the cases were dealt with.
6) **Adapting Regulatory Strategies:** Understand how the participants believe that regulatory bodies will have to shift strategies to better supervise CBDCs effectively.
7) **Balancing Privacy and Compliance:** Present how participants have to trade off privacy against compliance issues in their operations of the CBDC.
8) **Regional Variations in CBDC Adoption:** Examining how regional differences affect the adoption and implementation of CBDCs and the manifestations of these differences in participants' work.
9) **Enhancing AML/CFT/CPF Protocols:** Understanding the impact of CBDC implementation on AML/CFT/CPF protocols within participants' organizations.
10) **Future Outlook on CBDCs:** Gathering participants' views on the future of CBDCs in banking compliance and cybersecurity, including anticipated trends and innovations.

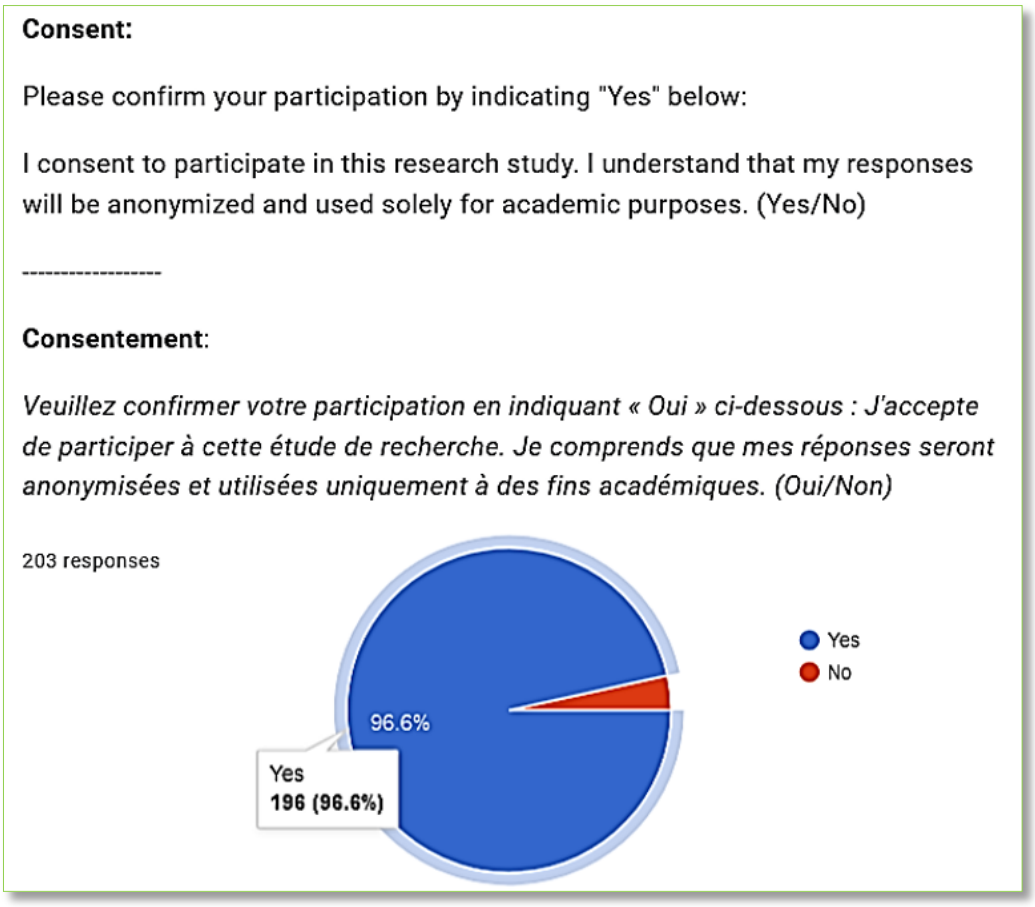


Figure 14: Consent to participate in the survey

Participants:

- Number of targeted participants: 220
- Number of participants: 203
- Number of responses: 196 (96,55%)
- Number of reluctant: 7 (3,45%)
- Time Required to Complete the Survey: Approximately 20 minutes.

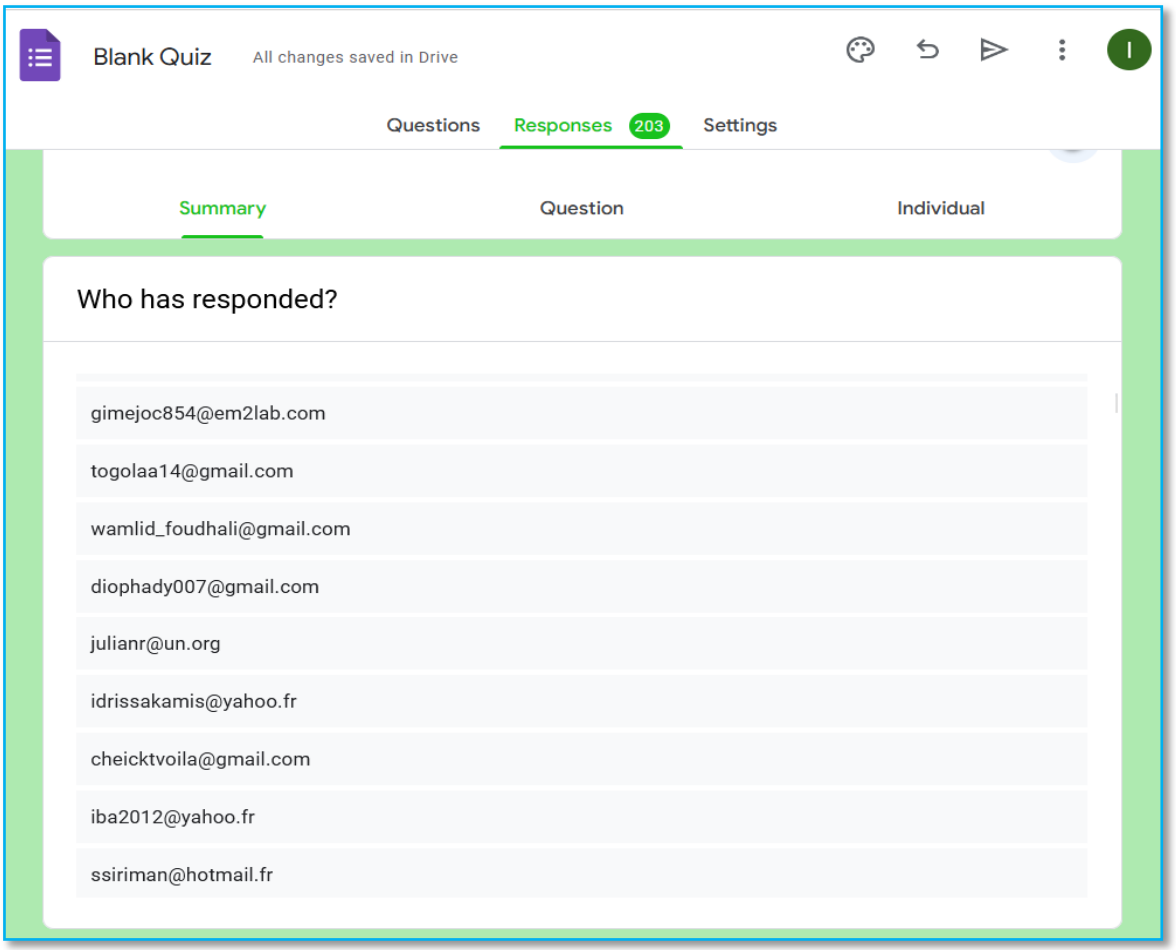


Figure 15: Survey participation

Confidentiality and Ethics: The survey ensures confidentiality, with all personal information kept private and destroyed after the research is completed. Participation is voluntary, and the project has been approved by the **SELINUS UNIVERSITY** Research Ethics Committee.

3.5.4. Secondary Data Collection

Secondary data collection involves gathering and analysing existing data that was originally collected for other purposes. This approach provides valuable context and background information, supporting and informing the primary research findings.

i. Secondary Data Classification

Secondary data are classified as either internal or external based on their source:

Internal Secondary Data: Information acquired within the organization where the research is conducted.

External Secondary Data: Information obtained from sources outside the organization.

The two major advantages of using secondary data in research are time and cost savings. During the interview process, many interviewees referred to secondary data to support their claims and hypotheses. This literature list is detailed at the end of the document, on **literature and Academic Journals**.

ii. Sources of Secondary Data

The secondary data used in this study comes from a variety of reputable sources, including:

Academic Journals: Peer-reviewed articles providing insights into the ethical dimensions, compliance standards, and cybersecurity issues related to CBDCs.

Industry Reports: Publications from financial institutions, consultancy firms, and industry analysts offering data on current trends, challenges, and best practices in digital currencies and banking compliance.

BCEAO: Instructions and directives from BCEAO.

Government and Regulatory Publications: Documents from central banks, financial regulatory bodies, and international organizations such as the IMF and the World Bank discussing policies, regulations, and the broader economic impact of CBDCs.

Online Databases: Resources from Uniselinus University Library, Google Scholar, and repositories of financial data and statistics, including reports from Bloomberg, Reuters, and other financial news services.

Just as we trust the primary data collected, we also trust the secondary data reviewed in this study. Given that CBDCs are a new topic, our secondary materials primarily come from official institutions and academic articles related to it.

Secondary data collection is a crucial component of this study, providing a foundation of existing knowledge and context that supports and enhances the primary research findings. By integrating data from a variety of credible sources, we can develop a more comprehensive understanding of the ethical, compliance, and cybersecurity challenges and opportunities associated with CBDCs.

3.6. Study Area

Identifying the geographical scope of any study has critical implications that set the environmental, contextual, and research background. This section looks into the geographical scale in which our study is positioned and discusses why it is important to investigate ethical, regulatory, and cybersecurity implications of CBDCs within this region.

3.6.1. Area, Context and Population

i. *Geographical Boundary:*

Our focus, therefore, has been on the West African sub-continent, and countries include Mali, Burkina Faso, Nigeria.

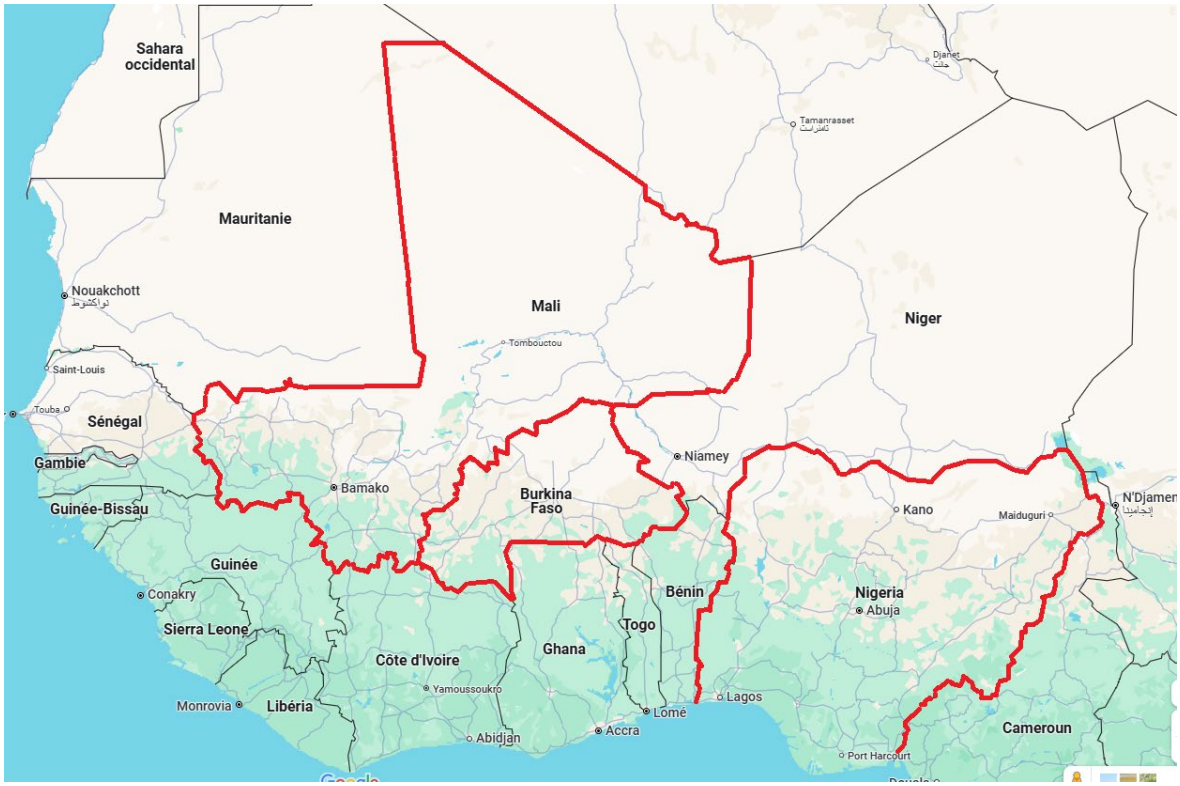


Figure 16: Geographical Boundary

Source: https://www.google.com/

The study will, therefore, be based more specifically on the first two countries and less based on Nigeria which will be used to provide a benchmark or comparison. The environment for studying the introduction and impact of CBDCs within this region is rather fascinating and complex. All the countries within this area have attained different levels in adopting digital financial technologies; some are early innovators, while others are catching up. We have chosen this region due to the rapidity of technological changes, different regulatory environments, and the challenges and opportunities that exist uniquely for the adoption of CBDCs.

ii. *Contextual Scope:*

1. ***Economic Landscape:*** West Africa is characterized by a mixed bag of emerging and developing economies, with its population largely dependent on unofficial financial systems. Because of that, the region presents one of the suitable case studies to

understand how a CBDC is designed to operate in conjunction with pre-existing local financial architectures to advance goals of financial inclusion.

2. ***Regulatory Environment:*** Regulatory frameworks for CBDCs differ from one country to another in the region. For instance, different approaches of the Central Bank of Nigeria, the Bank of Ghana, and BCEAO in the regulation of digital currency in Nigeria, Ghana, and within the UEMOA bloc, respectively, present a useful relative comparison that will further our understanding of how policy contributes to CBDC adoption, best practices determination, and likely missteps.
3. **Technological Adoption:** Technological progress is very uneven across West Africa; some countries enjoy advanced digital infrastructures, while others are still in the building process. This offers a window for comparative work on how CBDCs function under different levels of technological readiness and brings about different sets of challenges and benefits.
4. **Cultural and Social Factors:** CBDCs' success depends on social and cultural vectors like faith in financial institutions, levels of digital literacy, and overall socioeconomic conditions. It is such dynamics that nuanced understandings can be derived regarding how a variety of different communities in West Africa might be variously impacted by implementations of CBDCs.

iii. *Study Population:*

The study targets a broad range of stakeholders, including:

- **Banking Professionals:** Individuals working in compliance, cybersecurity, and digital currency divisions within banks and financial institutions.
- **Technology Experts:** Professionals specializing in blockchain, cybersecurity, and other technologies relevant to CBDCs.
- **Academics and Researchers:** Scholars and researchers specializing in finance, economics, and technology fields that offer both theoretical and empirical evidence.
- **General Public:** Consumers and, more so, the end-users of financial services who can contribute to issues dealing with usability and trustworthiness of CBDCs.

iv. *Data Collection Methods:*

Mixed methods research may use quantitative research and qualitative research equally or unequally (Creswell and Plano Clark 2017), one methodology having a dominant role and the other a supporting role. This prioritisation reflects the research purpose, researcher preferences and the expectations of

those who commission the research (such as your project tutor or the managers in an organisation) [64]. We have adopted a mixed-method approach for data collection with a greater emphasis or weighting on quantitative data in the following ways:

- **Surveys:** We issued questionnaires to professionals in banking, regulators, and technology experts to quantify experiences and perceptions about CBDCs.
- **Interviews:** In-depth interviews with key stakeholders were conducted to obtain qualitative insights into the challenges, benefits, and ethical considerations associated with CBDCs.
- **Literature Review:** The study placed our findings into context, drawing from existing research and publications, and provided a theoretical framework for our study.

West Africa's dynamic environment is perfect for studying CBDCs. We aim to find useful insights for the region and the world. Our research focuses on real-world issues to be practical and helpful.

3.6.2. General Statistics of the Study Area

We begin with a general statistic outlook for the West African zone, which would give us firm ground on which to present ethical, compliance, and cybersecurity considerations associated with CBDCs. The overview contains some key statistics relating to UEMOA nations like Mali and Burkina Faso, added to Nigeria. This brings such a profound understanding of the region's economic, demographic, and technological outlook that will go a long way in helping us further our understanding of potential outcomes and issues relating to the introduction of CBDCs.

i. Population and Demographics:

- **Mali:**The current population of Mali is 24,063,304 as of Tuesday, July 30, 2024, based on Worldometer elaboration of the most recent available United Nations estimates. The population in 2023 was approximately 23,293,698 at mid-year. Mali's population represents 0.29% of the world's population and is ranked 58th among countries and dependencies by population. The density of the population of Mali is 19 persons per square kilometer, 49 persons per square mile, and its total area is 1,220,190 square kilometers, 471,118 square miles. In 2023, 43.9% of the population (10,232,281 people) resided in urban centers. The median age in Mali is 15.3 years.[65].

[64] Research Methods for Business Students NINTH EDITION - Mark N.K. Saunders, Philip Lewis and Adrian Thornhill 2023 - P189

[65] https://www.worldometers.info/population/africa/western-africa/

- **Burkina Faso:** The population of Burkina Faso as of Tuesday, July 30, 2024, is 23,880,727. The 2023 population was estimated at 23,251,485 at mid-year. The population of Burkina Faso represents 0.29% of the total world population and is ranked 59th among countries and dependencies by population. Burkina Faso's population density is 85 per square kilometer (220 per square mile) and has a total area of 273,600 square kilometers (105,638 square miles). 31.8% of the population (7,388,364 people) resided in urban agglomerations in 2023. The median age in Burkina Faso is 16.9 years.
- **Nigeria:** Nigeria's population was 229,523,873 as of Tuesday, July 30, 2024. The population in 2023 was estimated at 223,804,632 at mid-year. Nigeria accounts for 2.78% of the total world population and ranks number sixth in countries and dependencies by population. Nigeria has a population density of 246 persons per square kilometer or 636 persons per square mile, having a total land area of 910,770 square kilometers or 351,650 square miles. In 2023, 53.9% of the population, or 120,696,717 persons resided in urban areas. The median age of the population in Nigeria is 17.2 years.

ii. Economic Indicators:

It presents a comparative review of the key economic indicators of Mali, Burkina Faso and Nigeria. It highlights differences in exchange rates, unemployment and inflation, etc. Nigeria notably has a much larger GDP but also faces higher inflation and unemployment issues than Mali and Burkina Faso. The data also reflects differences in internet and mobile connectivity levels, with Nigeria leading the way in digital access.

Parameter	*Mali*	*Burkina Faso*	*Nigeria*
Currency	West African CFA franc (XOF)	West African CFA franc (XOF)	Naira (NGN)
Unemployment rate	7.4% (2017 est.)	6.4% (2018 est.)	33.3% (2020 est.)
Inflation rate	1.3% (2021 est.)	1.9% (2018 est.)	16.5% (2021 est.)
Cost of Living (USA = 100%)	35	34	30
Commercial taxes	35.2% of GDP	33.6% of GDP	32.3% of GDP
Average income	$800 (2021 est.)	$700 (2021 est.)	$2,400 (2021 est.)
Central government debt	37.7% of GDP (2021 est.)	45.7% of GDP (2021 est.)	28.6% of GDP (2021 est.)
Corruption index	129 (2021 est.)	86 (2021 est.)	149 (2021 est.)
Gross domestic product	$18.9 billion (2021 est.)	$14.27 billion (2021 est.)	$514.05 billion (2021 est.)
Gross national product	$17.1 billion (2021 est.)	$13.8 billion (2021 est.)	$487.69 billion (2021 est.)
Exported goods	Cotton, gold, livestock	Cotton, gold	Petroleum, cocoa, rubber
Imported goods	Petroleum, machinery, food products	Machinery, food products, fuel	Machinery, chemicals, food products
International dialing	223	226	234
Internet domain	.ml	.bf	.ng

Landlines	0.23 per 100 people (2020 est.)	0.28 per 100 people (2020 est.)	0.13 per 100 people (2020 est.)
Mobile cellulars	105 per 100 people (2020 est.)	83 per 100 people (2020 est.)	94 per 100 people (2020 est.)
Internet users	11% of population (2020 est.)	18% of population (2020 est.)	36% of population (2020 est.)
Broadband Internet	0.1 per 100 people (2020 est.)	0.2 per 100 people (2020 est.)	0.6 per 100 people (2020 est.)
Roadways	22,474 km (2021 est.)	15,272 km (2021 est.)	195,000 km (2021 est.)
Railways	729 km (2021 est.)	622 km (2021 est.)	3,505 km (2021 est.)
Passenger airports	8 (2021 est.)	2 (2021 est.)	54 (2021 est.)

Table 4: Economic Indicators

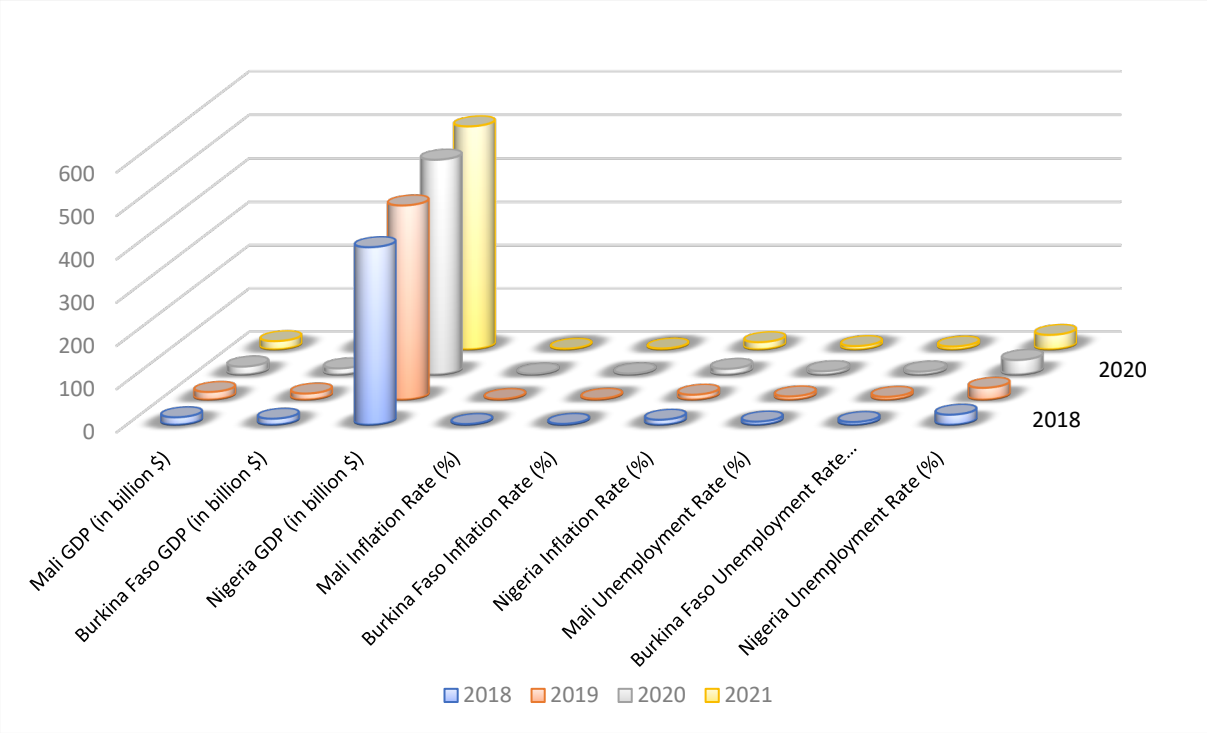
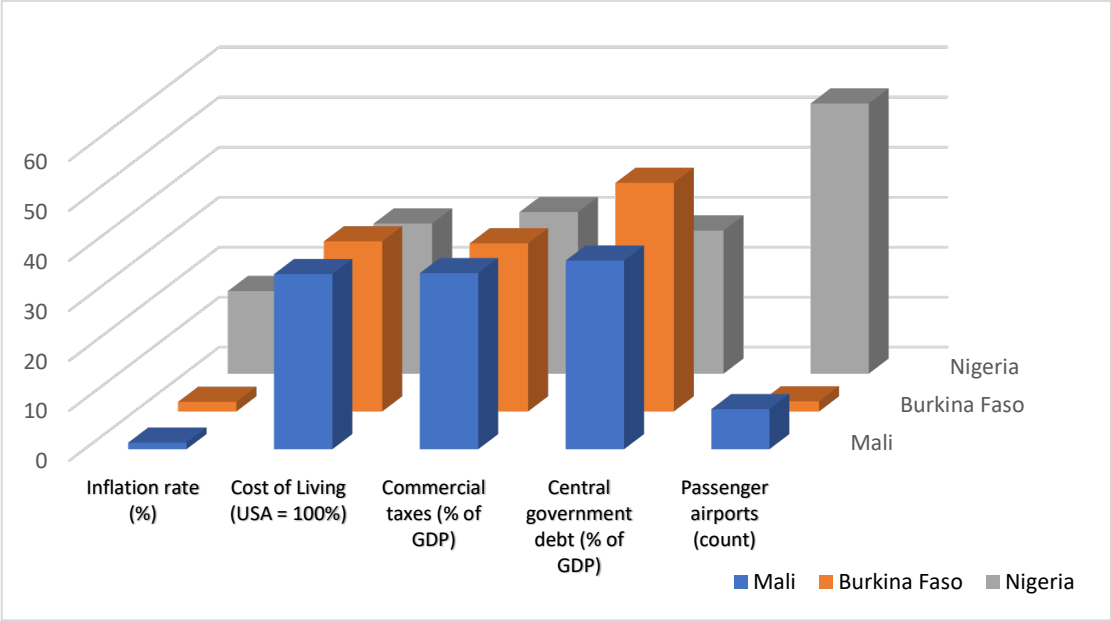


Figure 17: Economic Indicators



Graphic 9: Key Indicators for CBDC

source: https://www.cia.gov; https://www.worlddata.info[66]

iii. *Demographic characteristics*

The demographic results show the breakdown of respondents per Education Level category, Job Category, Years of Experience, Use of Digital Payments and Familiarity with CBDCs. The results are shown in Table 5.

Educational Level		Familiarity with CBDCs	Count of Use digital payment methods	Years of experience	
Master's Degree (Bac + 5) and above	61	Not familiar	**16**	Between 1 and 3 years (Entre 1 et 3 ans)	12
		Somewhat familiar	**26**	Between 3 and 10 years (Entre 3 et 10 ans)	16
		Very familiar	**19**	Less than a year (Moins d'un an)	21
				More than 10 years (Plus de 10 ans)	12
Doctorate Degree (Bac + 8) and above	54	Not familiar	**14**	Between 1 and 3 years (Entre 1 et 3 ans)	16
		Somewhat familiar	**19**	Between 3 and 10 years (Entre 3 et 10 ans)	8
		Very familiar	**21**	Less than a year (Moins d'un an)	17

[66] https://www.worlddata.info/country-comparison.php?country1=BFA&country2=MLI; https://www.worlddata.info/country-comparison.php?country1=MLI&country2=NGA ; https://www.cia.gov/the-world-factbook/countries/Nigeria/#economy

Educational Level		Familiarity with CBDCs	Count of Use digital payment methods	Years of experience	
				More than 10 years (Plus de 10 ans)	13
Bachelor's Degree (Bac + 3) and above	30	Not familiar	**12**	Between 1 and 3 years (Entre 1 et 3 ans)	12
		Somewhat familiar	**9**	Between 3 and 10 years (Entre 3 et 10 ans)	6
		Very familiar	**9**	Less than a year (Moins d'un an)	11
				More than 10 years (Plus de 10 ans)	1
Associate Degree (Bac + 2) and above	27	Not familiar	**12**	Between 1 and 3 years (Entre 1 et 3 ans)	12
		Somewhat familiar	**9**	Between 3 and 10 years (Entre 3 et 10 ans)	3
		Very familiar	**6**	Less than a year (Moins d'un an)	10
				More than 10 years (Plus de 10 ans)	2
High School Diploma (Bac) or below	24	Not familiar	**13**	Between 1 and 3 years (Entre 1 et 3 ans)	6
		Somewhat familiar	**8**	Between 3 and 10 years (Entre 3 et 10 ans)	3
		Very familiar	**3**	Less than a year (Moins d'un an)	15

Table 5: Demographic characteristics

	OCCUPATION	COUNT	TOTAL
OCCUPATION	Banking Professionals (General)	**7**	**196**
	Compliance Professionals	**4**	
	Doctor/ Healthcare Professional	**4**	
	Educators/ Researchers	**8**	
	Financial Analysts and Managers	**41**	
	IT and Cybersecurity Specialists	**29**	
	Others	**31**	
	Senior Managers/ Consultants	**4**	
	Students	**51**	
	Unemployed	**12**	
	Sales / marketing	**5**	

Table 6: Respondents occupations

- ***Key Insights***
- ***Digital Payment Usage:***
  - 92.1% of respondents use digital payment methods.

- Only 7.3% do not use digital payment methods.

- ***Familiarity with CBDCs (Central Bank Digital Currencies):***
  - Very familiar: 34.8% of respondents.
  - Somewhat familiar: 41.5% of respondents.
  - Not familiar: 37.8% of respondents.
- ***Years of Experience:***
  - The majority of respondents fall under:
    - Less than a year: 35.9%.
    - 1 to 3 years: 32.3%.
    - 3 to 10 years: 21.3%.
    - More than 10 years: 16.4%.

- ***Relationships with Banking/Finance/Cybersecurity:***
  - We saw a wide array of relationships that spanned from financial operations, compliance, and client relationships to specialist work in banking or cybersecurity fields.
  - Some gave general descriptions of what they did, for instance, back-office operations involved in mobile banking or Orange Money services.

iv. Financial and Regulatory Environment:

48% of the population in Africa are currently served by banking services, according to the African Digital Banking Transformation Report 2023. All countries have a central bank to oversee monetary policy and financial regulation (e.g., Central Bank of Nigeria, Central Bank of West African States for Burkina Faso and Mali). Regulatory frameworks may be at different levels of development and implementation, and the active improvement of regulation to adapt to digital currencies and fintech[67].

v. Banking Penetration

1- Mali:

- [67] World Bank Global Findex Database: https://globalfindex.worldbank.org/
- International Monetary Fund (IMF) Financial Access Survey: https://data.imf.org/?sk=E5DCAB7E-A5CA-4892-A6EA-598B5463A34C
- Central Bank of Nigeria (CBN): https://www.cbn.gov.ng/
- Consultative Group to Assist the Poor (CGAP): https://www.cgap.org/
- Alliance for Financial Inclusion (AFI): https://www.afi-global.org/
- International Telecommunication Union (ITU): https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx
- World Bank Doing Business Report: https://www.doingbusiness.org/

- **Banking Penetration:** Statistics show that even now, as of the latest statistics[50], only 18% of adults in Mali use formal financial services. This means that though much has been left undone to deal with some real challenges on its journey to becoming financially inclusive. Most of Mali's adults, therefore, were excluded from formal banking and therefore had restricted capabilities to use credit, savings, and other ancillary services.
- **Mobile Money Adoption:** Mobile money services have expanded swiftly in Mali, and 25% of adults are presently utilizing mobile money services. Mobile money has also become a valuable tool to increase financial inclusion, particularly in rural areas where banking infrastructure is typically poor. The simplicity and low costs have popularized the use of mobile money services among unbanked masses.
- **Digital Infrastructure:** The present status of digital infrastructure in Mali stands at about 35% penetration. These, while an improvement, still leave very important gaps that need to be filled if digital financial services are ever to be more implementable on a wider scale. Expansion of digital infrastructure is essential to facilitating broader access to financial services and economic growth.

2- Burkina Faso:

- **Banking Penetration Rate:** Banking penetration stands at approximately 20% of adults, which signifies coverage by formal banking. Though slightly more than Mali's, this constitutes a low extent of the spread of traditional bank services. The comparatively low banking penetration rate implies that a considerable percentage of the population has access to no bank account whatsoever or is using unofficial financial channels, which could suppress their economic prospects.
- **Mobile Money Adoption:** Burkina Faso has an adoption rate of mobile money services at 30%. This high adoption rate says much about the increasing significance of mobile financial services in extending access to banking services to underserved communities. Mobile money services are now an important constituent of the financial system, delivering an accessible option to conventional banking services.
- **Digital Infrastructure:** 40% of the adult population in Nigeria has access to formal financial services. Of course, this relatively high rate of penetration, compared to Mali and Burkina Faso, does testify to the fact that better availability of banking infrastructures prevails, but a huge bulk of the populace remains unbanked or underbanked, for which continuous effort toward financial inclusions is needed.

3- Nigeria:

- **Banking Penetration:** 40% of the adult population in Nigeria has access to formal financial services. Of course, this relatively high rate of penetration, compared to Mali and Burkina Faso,

does testify to the fact that better availability of banking infrastructures prevails, but a huge bulk of the populace remains unbanked or underbanked, for which continuous effort toward financial inclusions is needed.

- **Mobile Money Adoption:** Nigeria leads in the adoption of mobile money, with 50% of its adults using the services. Popularity of mobile money speaks to significance in increasing financial inclusions and increasing access to bank services at un-served communities. Mobile money has become an integral part of the financial ecosystem in Nigeria, offering various services such as money transfers, bill payments and savings.
- **Digital Infrastructure:** Nigeria has a digital infrastructure penetration rate of 55%, the highest among the three countries. This robust digital infrastructure supports the extensive use of digital financial services and mobile banking. Nigeria's strong digital foundation enables the delivery of innovative financial products and services, contributing to the overall development of the financial sector.

vi. National Regulators

Each country has its own regulators that enforce financial regulation, consumer protection together with systemic stability. A few examples of national regulators include:

- **Mali:** BCEAO regulates the Malian banking system with a view to aligning with regional and international standards. The AMRT - Autorité Malienne de Régulation des Télécommunications, des Technologies de l'Information et de la Communication et des Postes - is the regulator of telecommunication, ICT and postal services; guarantees equal treatment of operators in these sectors; and is impartial. APDP is the Authority for the Protection of Personal Data.
- Burkina Faso: The banking sector of Burkina Faso is regulated by the BCEAO, thus maintaining an integrated regulatory framework of the UEMOA countries. In general, ARCEP is responsible for regulation of electronic communications networks and services in Burkina Faso, and the CIL Personal Data Protection Authority.
- **Nigeria:** The Central Bank of Nigeria is the chief regulator of banks in Nigeria and tasked with the enforcement of the Financial Regulation Acts as well as maintaining financial stability. Other regulators include the Nigerian Securities and Exchange Commission and the National Insurance Commission.

These indicators fully explain the opportunities and challenges that will face CBDCs in the region particularly and thereby guide our research on banking compliance, cybersecurity, and ethics.

3.6.3. Finance Sector in the World

A background on the world financial industry will put our discussion into context regarding the ethical aspects, banking supervision, and cybersecurity of CBDCs. To that effect, it will aid in the appreciation of the larger landscape of the financial industry and the extent to which CBDCs bring with them a number of challenges with opportunities on a global scale.

i. Global Financial Landscape:

Global Financial System refers to a set of connected, elaborate, and dynamic institutions, markets, and instruments which mobilize and transfer credit and capital across borders worldwide. A number of major players in the global financial system not by way of limitation are:

- **Financial Institutions:** The core of the global financial system, in terms of their fundamental services, deposit-taking, and lending, consists of central banks, commercial banks, investment banks, and retail banks.
- **Financial Markets:**
  - **Foreign Exchange Markets:** They provide the foreign exchange required for trade and investment.

ii. Technological Advancements:

Technologies have completely revolutionized the whole face of the world finance sector. Some of the technologies are critical to the:

- **Digital Banking:** Also known as online or mobile banking, it has changed the way customers visit banks for financial services.
- **Blockchain Technology:** Blockchain, as observed, is the technology behind cryptocurrencies. It offers a decentralized ledger system that offers higher transparency and security in financial transactions.
- **Artificial Intelligence (AI) and Machine Learning (ML):** AI and ML are being used for fraud detection, risk management, and offering personalized financial services.

iii. Regulatory Environment:

Regulation has been central in fostering stability and integrity in the international financial system and in helping countries in their fight against financial crimes through robust AML/CFT regimes. We therefore strive to give substance to these claims by pointing out the many international institutions, national regulators, and important regulatory frameworks.

iv. International Organizations

International institutions provide guidance and support in the pursuit of stability and integrity in the international financial system. Examples of such institutions include:

- **International Monetary Fund (IMF):** It lends to the member nations with policy guidance to stabilize economies and promote sustainable growth. Besides, it also helps in building regulatory frameworks for financial system strengthening.
- **World Bank:** The World Bank offers financial and technical assistance to developing countries for various development activities aimed at poverty reduction with a maximum level of economic growth. Besides, it helps establish better regulatory mechanisms in the financial sector.
- **Bank for International Settlements (BIS):** An international settlement bank providing banking facilities to central banks. Promotional work in the interests of international monetary and financial co-operation, with related policy analysis and research to underpin banking regulations.

v. Financial Action Task Force (FATF)

FATF is an intergovernmental body that formulates international standards to fight money laundering and terrorist financing. FATF recommendations set a general framework for nations to use effective anti-financial crime controls. Nations are periodically reviewed by FATF or FATF-style regional organizations to see if they are living up to these standards [68].

Key Areas of Regulatory Focus:

- **AML/CFT/CPF Compliance:** AML/CFT/CPF regulations are enforced by national authorities to fight money laundering, terrorist financing and counter the financing of proliferation. AML/CFT/CPF regulations oblige financial institutions to implement customer due diligence (CDD) practices, report suspicious transactions, and possess effective internal controls.
- **Consumer Protection:** Supervisory authorities protect consumers by ensuring that financial institutions carry out their operations in a transparent and honest manner. This involves imposing disclosure requirements, resolving consumer complaints, and prohibiting unfair practices, protecting their privacy.
- **Financial Stability:** Regulators evaluate the financial health of financial institutions in order to avoid systemic risks. These activities include stress testing, imposing capital adequacy ratios, and monitoring risk management policies.

[68] Financial Action Task Force (FATF): https://www.fatf-gafi.org/

- **Digital Financial Services:** Increased use of digital banking and mobile financial services are altering regulatory systems to accommodate new risks and opportunities in the realms of cybersecurity, financial inclusion, and regulation of fintech companies.

vi. Global Challenges:

- **Complexity of Financial Crimes:** Most financial crimes, such as AML/CFT/CFP, are usually highly organized in transnational networks. The sophistication presents serious challenges for detection and enforcement in any one country. Offenders continue to change their modus operandi with the use of increasingly sophisticated techniques and technologies. The need for constant vigilance and innovation is necessary in keeping pace with these evolving tactics.
- **Regulatory Discrepancies:** There is a difference in the stringency and enforcement of regulations across different countries. Mostly, such differences present options for criminals to take advantage of, transferring illicit money across borders where such regulations are lax. Transborder harmonization of regulations mostly faces obstacles due to differences in legal frameworks, economic interests, and political will. An effective AML/CFT/CPF program presupposes coordination via a variety of national and transnational organizations. Ensuring that they communicate easily and effectively and exchange information freely with each other can be problematic.
- **Technological Challenges:** The new challenges brought by the advent of cryptocurrencies and other virtual assets to AML, combating financing of terrorism, and combating the proliferation of weapons activities. This technology makes for anonymity in transactions, hence illegal activities cannot be traced. Furthermore, financial institutions are highly prone to cybersecurity risks that can be utilized for financial malfeasance. Effective cybersecurity measures are called for but challenging.
- **Resource Constraints:** AML/CFT/CPF compliance is an expensive affair for financial institutions, especially the smaller ones that lack the requisite resources.
- **Data and Information Sharing:** Striking a balance between information sharing and data protection laws and privacy rights is a major challenge. Laws such as GDPR in Europe make it difficult to share financial intelligence across borders. The insights drawn from this broader perspective will lead us to devise best practices and strategies on how best to implement CBDCs in the West African subregion and beyond.

We are certain beyond doubt that these challenges facing the world of finance are the same that confront the implementation and/or adoption of virtual currencies.

3.6.4. Special Banking Sector in UEMOA and Mali

UEMOA comprises eight countries: Benin, Burkina Faso, Côte d'Ivoire, Guinea-Bissau, Mali, Niger, Burkina Faso, and Togo. These countries share a common currency, the CFA franc of XOF, which is regulated by BCEAO.

The CFA franc ensures monetary stability and facilitates trade between member countries. It is pegged to the euro, which guarantees exchange rate stability. WAEMU aims to achieve economic integration by harmonizing economic policies, promoting trade, and fostering the development of the financial sector in member states. BCEAO sets monetary policy and regulates the banking sector within WAEMU. It ensures uniform banking regulations and standards across member countries.

Globaly Banking penetration in the union is relatively low by global standards. Efforts are underway to increase access to banking services, particularly in rural areas. Mobile money services have significantly improved financial inclusion, allowing more people to access financial services without having a traditional bank account. This inclusion rate is due to its easy access to a large number of people. However, the sector of Bank faces challenges such as limited infrastructure, low financial literacy, and regulatory compliance issues. In addition, political instability in some member countries affects the stability of the banking sector.

As a member of UEMOA, Mali shares many characteristics with the broader regional banking sector. However, it also has unique features and challenges but various initiatives are underway to develop Mali's banking sector, such as improving infrastructure, enhancing regulatory frameworks, and promoting financial literacy[69].

With the opening of a new bank in February 2019, there are now 14 commercial banks operating in Mali. The sector is only moderately concentrated, with the top three banks controlling 48 percent of deposits and 40 percent of loans. The Banque Nationale de Developpement Agricole (BNDA), was an agricultural development bank and still has a focus in that area, but now operates as a general commercial bank. In addition, there are three small non-bank credit institutions, a leasing company and two guarantee funds, one for mortgages and the other for the private sector, notably for SMEs.

In private sector, Guarantee Fund started operations in late 2014 only. These 17 financial institutions are subject to WAMU regional regulations and supervised by the WAMU Banking Commission.

[69] MALI THE BANKING SYSTEM AND CREDIT TO THE ECONOMY: https://documents1.worldbank.org/curated/en/894621467999119269/pdf/105294-FSAP-P153363-PUBLIC-Mali-FSAPDM-TN-Banking-Public.pdf

Existing mobile banking services need to be broadened from basic mobile payment services to a more comprehensive menu of remittance, savings, credit, and insurance products. At present, mobile money is used primarily for person-to-person transfers and cash-in, cash-out transactions, though bill payments and other services are available. Further work is needed to expand the agent network, acceptance points and usage.

Regulatory Framework:

Regarding the regulatory framework of the banking sector in Mali, several supervisory authorities are involved in regulating this sensitive activity, in particular:

- **The Council of Ministers of the West African Monetary Union (UMOA),** which sets the legal and regulatory framework applicable to credit activities;
- **The Central Bank of West African States (BCEAO),** the issuing institution of UMOA, which notably develops prudential and accounting regulations and also performs a supervisory mission for the banking system on its own behalf;
- **The Banking Commission of UMOA,** the body responsible for overseeing the organization and control of banks and financial institutions.

Over time, with the development and increasing complexity of banking and financial operations, the regulation and supervision system of credit institutions has continuously evolved and adapted to an ever-changing field. Consequently, it is not always easy for the leaders of credit institutions, whose roles are particularly demanding, to stay perfectly and constantly informed of the evolution and status of banking legislation and prudential rules. However, they are responsible for ensuring that all these legislative and regulatory texts are rigorously respected by the bank or financial institution they manage.

3.6.5. Justification for Conducting the Study in Mali

Carrying out this study in Mali is of great importance for a number of compelling reasons, especially considering the residence and working experience of the student in the nation. The reasons why Mali is selected as a suitable and sensible place for researching the ethical, banking compliance, and cybersecurity aspects of CBDCs (CBDC) are discussed below:

i. Local Expertise and Contextual Understanding

The student's residence and work in Mali offer unique exposure to first-hand information and a close understanding of the local context. This closeness will, therefore, provide the needed profound insight into the opportunity that CBDCs represent for Mali, the challenges it may present, and inform the research with real experiences and local insights.

ii. Financial Inclusion Challenges

This means that, as shown above, Mali still has much work to do regarding achieving financial inclusion, as most of its population is beyond the reach of conventional bank products. Access to formal financial services is still available to only about 18% of the adult population. Despite growing mobile money uptake, there is still plenty of room for expansion. Studying CBDCs in this regard can offer ethically insights on how digital currencies can close the financial inclusion gap and make financial services more accessible to underserved populations.

iii. Mobile Money Growth

Mali has also seen rapid mobile money expansion, with a very significant effect on financial inclusion as well as laying the foundation for digital financial services. Understanding how CBDCs can complement and be layered on top of existing mobile money ecosystems can yield valuable lessons for other emerging economies struggling with similar conditions.

iv. Economic and Political Context

Mali's economic landscape is ruled by a formal and informal economy, with the majority of citizens relying on informal finance systems. The country is also faced with political instability and security concerns that compromise economic stability. It is critical to understand how CBDCs can work within this environment in order to formulate strong and agile digital currency solutions that are able to survive economic and political volatility.

v. Regulatory Environment

Mali being a member of UEMOA, which has a unique regulatory environment with a shared currency and central regulator (BCEAO), allows us to test the dynamics between regional regulation and national implementation plans, offering insights into how CBDCs can be harmonized across borders. The selection also allows the assessment of advanced financial solutions for an emerging economy. This study can identify how CBDCs will effectively be utilized to bring more efficient, secure, and accessible financial services, which will meet the specific needs of the people in Mali.

vi. Technological Adoption

The country is moving toward the adoption of technology, but it still lags behind other developed countries in terms of digital infrastructure. A study of CBDC usage in Mali will provide an understanding of the characteristics of technological needs and their challenges in successful digital currency implementation in similar environments; it shall go a long way toward informing the means of circumventing infrastructure limitations.

vii. Contribution to Academic and Policy Discourse

The nation will make a contribution towards the policy and academic literature on CBDCs through empirical findings and a perspective from the developing economy. This will complement the present research gap and give a broader picture of the effects of CBDCs on banking compliance, cybersecurity, and ethical issues in developing economies.

viii. *Innovative Financial Solutions*

The single financial profile of Mali provides a unique opportunity for consideration in pioneering innovative financial solutions and their suitability to address the needs of an emerging economy. This work will tend to ascertain, through CBDCs, efficient, safe, and accessible channels that mean the facilitation of financial services to the exact needs of the population in Mali.

ix. *International Perspective*

The CBDCs, considering the geopolitical position of Mali in West Africa, can act to add a cross-border trade and sub-regional economic integration aspect to the study. Of course, the realization of such potentials by CBDCs in furthering trade and economic cooperation would have regional economic strategies and plans for development become interested.

With awareness of the global impact of digital currencies, our study adopts a general international perspective. We focus on key financial hubs and their central banks that have launched CBDCs or are at advanced phases of pilot projects or studies. But we prioritize the African narrative, i.e., in the UEMOA zone. For analytical completeness, we will also examine key markets like Nigeria, US, EU, and China and highlight relevant developments in emerging economies. This strategy gives one a proper grasp of the regional and international dynamics.

With the focus being on Mali, the objective is to offer insightful findings and practical recommendations that can not only benefit Mali but also other emerging economies planning to introduce CBDCs.

3.7. Populations and Sample Selection

During the selection process, we prioritize stakeholders that are vital to the ethical considerations, banking compliance, and cybersecurity of CBDCs. These populations provide varied opinions and valuable input on the use and implications of CBDCs.

3.7.1. Stakeholders' groups

1) Banking Professionals:

The working group consists of the practitioners of compliance, cybersecurity, and digital currency from banks and other financial institutions, who have extensive and primary experience in the functioning of banks and regulatory requirements to understand exactly the challenges and advantages of CBDCs.

Among them, important members are: Compliance Officer, Cybersecurity Expert, Digital Banking Manager, and Financial Analyst.

2) Technology Experts:

Technical experts in virtual money, block-chain, and other technologies relating to CBDCs avail valuable technical guidance on the development and security of digital currencies. Their technological expertise is important in problem-solving and innovations. The main targets are Blockchain Developers and FinTech Innovators.

3) Academics and Researchers:

Financial and economic scholars, along with technical scholars, introduce theoretical contexts along with empirical research to the study. The scholarly questions position the study in relation to current knowledge and serve as a grounding for analysis of emerging data. Some of those individuals are professors at universities, economic researchers, and financial technology academics.

4) General Public:

Consumers and final users of financial services offer feedback on the usability, trust, and social implications of CBDCs. They play a vital role in deciding the public acceptance of digital currencies and their real impacts in the real world.

3.7.2. Respondent Selection:

Respondents are selected on the basis of their knowledge, understanding, and familiarity with the research subject. The selected respondents have a financial background and high exposure to the subject. They have professional experience in Enterprise Risk Management and business strategic initiatives within corporations. The participants were drawn from financial services and other institutions active in Mali and almost throughout the globe. The diverse groups that are targeted ensure wide understanding of the different aspects of CBDCs. Herein, an attempt is made to give an inclusive vision of the ethical, compliance, and cybersecurity challenges that come with CBDCs and that need to be addressed-from the banking professionals to the general public. This grounds our study in multiplicity of perceptions and thus more substantial and actionable results regarding the implementation of CBDC in Mali, and contexts with similar socio-economic parameters.

3.8. Data Analysis Techniques

Data analysis is also an integral part of insight discovery, decision informing, hypothesis testing, quality assurance, relationship understanding, and the prediction of outcomes. Here, the research approach provides depth to ensure that the information unearthed from the stakeholders will expose revealing information about the ethical considerations, banking compliance, and cybersecurity issues in CBDCs.

3.8.1. Data Collection and Analysis

Data is collected through in-depth, open-ended questionnaire questions and lengthy interviews with the key stakeholders. Both are utilized to obtain rich, qualitative data that will get at the nuanced opinions and experiences of the participants. The application of a mixed-methods approach offers an exhaustive understanding of the complicated matters in relation to CBDCs. Among the most conventional approaches to analyzing qualitative data is what is commonly referred to as thematic analysis. Thematic analysis is a concept pertaining to the examination of qualitative data, that is, by definition, the identification and extraction of primary themes in the dataset. It is a rather diffuse approach and there are few generally agreed principles for defining core themes in data (Bell, Bryman & Harley 2019)[70]. After transcribing and translating the empirical data, we categorized it to identify patterns, similarities, or differences, following Bell, Bryman & Harley (2019).

According to Vanessa (2023), thematic analysis involves making sense of data by focusing on key themes[71]. This is crucial in comprehending the principal issues that are arising from the data. There is no particular manner in which thematic analysis is to be conducted, but there are shared methods regarding how it is conducted. This allows researchers utilizing thematic analysis to be flexible regarding how it is conducted. Coding of data can be done inductively, where the content itself directs the analytical focus, or deductively, based on a priori theoretical frameworks. We found this approach appropriate to the aims and research questions of our study and opted to perform an inductive thematic analysis with a constant alternation between established theoretical ideas and the empirical data gathered. This analysis process entails a series of steps that must be followed: transcription, coding, categorization, and interpretation. Analysis was made easier through the use of electronic data processing via current software programs like Google Forms, Google Sheets, and Microsoft Excel. During the analysis of data, advanced artificial intelligence tools such as ChatGPT and Google Gemini were also utilized. These tools enable deep functionality in analyzing big quantities of data and provide extended insights, thus enabling the processing of bigger datasets with more efficiency.

3.8.2. Steps in Thematic Analysis:

Braun and Clarke (2006) have given a six-phase guide, which is quite useful in conducting this type of analysis[72].

---

[70] BUSINESS RESEARCH METHODS ; Fifth Edition 2015, BY Emma Bell, Alan Bryman, Bill Harley
[71] Research methodologies for business management, By Ratten, Vanessa, author, p18
[72] Doing a Thematic Analysis: A Practical, Step-by-Step Guide for Learning and Teaching Scholars ; Article by Moira Maguire & Brid Delahunt - Dundalk Institute of Technology

1- **Become familiar with the data:** Reading and re-reading the data a number of times to gain an impression from the material. This is quite important in terms of beginning the overall sense of perspective and experience of participants.
2- **Generate initial codes:** Systematically organize interesting aspects throughout the entire data. This would involve highlighting what is important according to the research questions.
3- **Search for Themes:** Group the codes into theme possibilities and then bring all data together relevant to each possible theme. It is in this stage when the data will be organized so as to indicate key ideas and trends.
4- **Review Themes:** The reviewer checks that the themes are representative of the coded extracts and the whole dataset, thus developing a thematic map. The step is important because it checks that the themes indeed reflect the data accurately and are coherent.
5- **Define and Name Themes:** Ongoing analysis to refine the specificity of each theme, the overall story that comes out of the analysis, and the development of clear names and definitions for each theme. Naming and defining are completed in this step so themes are clearly described.
6- **Produce the Report:** The last chance for analysis, choosing rich, interesting extract examples, final analysis of chosen extracts, linking back to the research question and literature, and generating a scholarly report. In this step, the findings are assembled into a consistent and complete report that responds to the research questions.

3.8.3. Enhancing Rigor and Validity:

The methodologies mentioned below will be utilized in an attempt to maximize the validity and rigor of the thematic analysis:

1- **Triangulation:** Triangulation will involve combining several sources of information, such as surveys, interviews, and review of literature, in an attempt to verify the findings and produce a thorough analysis.
2- **Member Checking:** Participants will review and validate the findings for accuracy and genuineness.

We utilize thematic analysis in a careful examination of collected information from alternative sources and approaches. Through this, we identify common trends and trends, and out of them, develop a concise and in-depth picture of CBDCs' ethical, compliance, and cybersecurity concerns. What we learn through such an analysis is significant in guiding CBDCs' implementation and regulation in Mali and similar locations. Well-planned and careful approaches enable our findings to be strong, dependable, and applicable in real-life scenarios.

3.9. Ethical Considerations in Data Collection

Ethical aspects form an integral part of protecting the integrity, respect and dignity of the study participants. In compliance with the ethical standards approved by the SELINUS UNIVERSITY Research Ethics Committee, several controls have been implemented to maintain the rights and confidentiality of all involved persons.

1) **Participant Information:**
   - **Informed Consent:** All participants are thoroughly informed about the objectives, methodologies, potential danger, and benefits of the study, before participating in it.
   - **Voluntary Participation:** Study participation is purely voluntary. Participants have a right to withdraw at any point in time, and no repercussions will follow such a move.
2) **Confidentiality and Anonymity:**
   - **Data Protection:** Stringent laws regarding information protection have been adhered to in information management and information storage. Information access is restricted to only approved persons involved in studying it.
3) **Privacy:**
   - **Confidential Responses:** Participants have been assured that their answers will not be disclosed publicly. Only aggregated information will be shared, and individual answers cannot in any case be traced to individual participants.
   - **Secure Storage:** Information is kept safe through the use of secure electronic systems, and printed documents kept in locked files.
4) **Right to Withdraw:**
   - **Autonomy to Withdraw:** Participants have constant reminders about their right to withdraw at any point in time, with no justification being a necessity for such an act. Withdrawal will not have any detrimental impact on their affiliation with both the research group and institution.
   - **No Consequence:** There is no penalty or any negative effect on respondents withdrawing from participating in the research.
5) **Ethical Approval:**
   - **Research Ethics Committee:** The research was critically reviewed and approved by the SELINUS UNIVERSITY Research Ethics Committee for its adherence to all ethical considerations in the process of conducting the study.

6) **Ensuring Transparency and Accountability:**
   - **Effective Communication:** We maintain transparent channels of communication with participants, offering them constant updates about the development of the research and resolving any queries or concerns that arise.

- **Participant Feedback System:** Participants can submit feedback regarding their experiences during the study, and it helps in sharpening our methodologies for future studies and in providing them with comfort and happiness.

7) **Enhancing Participant Trust:**
   - **Transparency:** Transparency in the conduct of the research is assured through explaining the objectives, methodologies, and implications of the study to the participants. Participants have an option for getting a copy and even accessing the final report.
   - **Ethical Training:** Ethical training needs to be provided to every member of the research team so that they may understand the codes and values perfectly.
   - **Support Resources:** This also includes that participants are also informed about resources such as facing some kind of distress and discomfort during the experiment.

Such actions protect the rights, dignity, and welfare of all concerned and therefore build trust and confidence in the conduct of the study. Besides, adherence to ethical conduct in our studies not only safeguards the rights of participants but also increases our output and its credibility and dependability.

3.10. Quality of the study

3.10.1. Quality of data collection method

The study utilizes a mixed-methods research approach combining quantitative data to assess compliance levels with qualitative information for investigating ethical concerns. Central to the study is an examination of enhancing ethical frameworks in banking compliance in relation to CBDC development and management. An explanatory sequential design is adopted in the study, starting with collecting quantitative information about current compliance standards, then collecting qualitative information through expert cybersecurity professionals' interviews. With such an approach, a thorough analysis of quantitative information and a deeper examination of causality can be conducted.

The two hypotheses or research questions underpinning the study include:

- ***H1: Optimum ethical framework in banking compliance maximizes CBDC security.***
- ***H2: Present cybersecurity controls in electronic banking fall short in dealing with ethical aspects involved in CBDC rollout.***

Data collection involved a range of techniques, including survey, interviews, and documentation review. Information collected through such methodologies identifies a need for increased harmonization in compliance ethics approaches and a critical role in assuring information collected is of high quality.

3.10.2. Alternative criteria for evaluating qualitative research

Other scholars, in contrast, believe qualitative research require evaluation in terms of specific criteria not applicable in quantitative studies. Reliability and validity are the concern of the conventional position. However, there is some disquiet about their adequacy to encapsulate the range of issues raised by a concern for quality (Seale 1999)[73]. Guided by an interpretive paradigm that we intercepted in the writings of Dr. C. Daymon and Dr. I. Holloway (2002), it relies on the work of Lincoln and Guba (1985) and Guba and Lincoln (1989, 1998), and is promoted by Erlandson et al. (1993) among others.

According to this stance, the goodness of research is characterized by trustworthiness and authenticity which are central to the whole research process. Trustworthiness and authenticity are shown by researchers' careful documentation of the process of research and the decisions made along the way.

Authenticity

A study is authentic when the strategies you have used are appropriate for the 'true' reporting of participants' ideas, when the study is fair, and when it helps participants and similar groups to understand their world and improve it.

Trustworthiness

The criteria for evaluating trustworthiness are credibility, transferability, dependability and confirmability.

Trustworthiness consists of four parts, each equivalent to a criterion in quantitative studies:

- **Credibility,** which parallels internal validity;
- **Transferability,** which parallels external validity;
- **Dependability,** which parallels reliability;
- **Confirmability,** which parallels objectivity,

Credibility

According to Dr. C. Daymon and Dr. I. Holloway (2002), Lincoln and Guba (1985) suggest that you should aim for 'credibility', rather than internal validity. Your study is credible if the people in it recognize the truth of the findings in their own social context. At the proposal stage, you can indicate in two ways how you will endeavour to make your study credible. First,

set out the various research methods you intend to use and how each method will complement the others. Second, indicate how you will undertake a 'member check' (section 3.8.3. Enhancing Rigor, we set out details on triangulation and member checks).

Transferability

✓ [73] Qualitative Research Methods in Public Relations and Marketing Communications by Daymon, Christine, & Holloway, Immy. (2002) - – p92

Transferability replaces the notion of external validity, and is close to the idea of theory-based generalizability. Many qualitative studies involve very small samples or single case studies and it is your role to help the reader transfer the specific knowledge gained from the research findings of one study to other settings. For instance, if we intend to explore techniques of integrated marketing communications carried out by a multinational organization, our findings would be specific to that particular setting. You would need to consider how any principles or models which might emerge from your study could be applied to similar settings elsewhere. The beginning of this process of transferability is at the proposal stage where you outline the characteristics of your focal setting, or company, and indicate how you will select your sample. When you are able to discuss how your investigation is positioned within the realm of pertinent industry or scholarly issues or concerns, the salience of your work is demonstrated. This helps you, later, to show how your findings relate – or are transferable – to other settings in the same industry. Findings from your narrower study of one aspect of the practice should be related to other studies which articulate ideas about the overall functioning of integrated marketing communications.

Dependability

Credibility and dependability are closely linked, the latter replacing the notion of reliability. If the findings of your study are to be dependable, they must be consistent and accurate. This means that readers will be able to evaluate the adequacy of the analysis through following your decision-making processes. The context of your research must also be described in detail. One of the ways of achieving dependability is by demonstrating an audit trail, a technique which we describe later in the chapter.

Confirmability

Confirmability is more suited to qualitative research than the conventional criteria of neutrality or objectivity. Your research is judged by the way in which the findings and conclusions achieve the aim of the study and are not the result of your prior assumptions and preconceptions. Therefore, for your study to be confirmable, you need to be able to show how the data are linked to their sources so that a reader can establish that the conclusions and interpretations arise directly from them. Again, auditing or a ‘decision trail’ are pertinent because they require you to be reflective and to provide a self-critical account of how the research was done. To indicate at the proposal stage how confirmability will be demonstrated in your research, it is sufficient to outline the early intentions of your study, that is, your proposed research, your expectations, and a recognition of the need to be reflexive throughout.

IV. CONTENTS AND RESULTS

4.1. Introduction

The development of CBDCs holds significant potential for changing the financial environment. It opens an opportunity for increased productivity, reduced transaction expenses, and increased access to financial services. Nevertheless, CBDCs' rollout comes with a variety of complications. In such a scenario, in our work, we have examined several aspects of CBDCs, with a focus placed on ethical concerns, compliance with international banking standards, and cybersecurity concerns critical for effective use. In this regard, in this chapter, we present a critical analysis of our observations drawn through both primary and secondary studies conducted for this chapter.

- The primary studies include information collected through in-depth surveys and in-depth interviews with key persons in banking and financial sectors. These include compliance professionals, cybersecurity professionals, banking and financial managers, and other professionals with considerable engagements with CBDCs and relevant technology. What these professionals have to say about CBDCs brings out real-life complications and benefits of CBDCs.
- Secondary studies involve a thorough review of academic sources, government and regulative documents, and web databases. Analysis in such a manner places the work in a larger corpus of work and creates a basis for new observation interpretations. Analysis of secondary data covers current CBDCs' regulative environment, technological breakthroughs, and case studies in

several regions, including WAEMU and Nigeria.

As with quantitative and qualitative research, in mixed method the findings may be represented in any number of **formats**, including a journal article, conference presentation, monograph (book), and/or a popular form of writing such as a story or blog. **Identify the intended audience(s)** and how the format chosen allows you to reach that audience. We may create **side-by-side displays** of the qualitative and quantitative data through the use of tables, graphs, charts, or figures and then provide a mixed methods discussion (**Leavy, P. 2017**)[74].

We will, in this chapter, lay down a basis for a critical analysis of the study observations, starting with a critical review of interview observations, followed by survey results and secondary data analysis. Analysis of each will present a critical analysis of key concerns, with actionable recommendations for implementers of CBDCs involved in such work.

4.2. Current State of CBDC Regulations

The Current CBDC regulations states have demonstrated necessary evidence of rapid growth. Countries are working separately on different regulatory frameworks in purpose to secure this new form of currency. These regulatory frameworks aim to address key issues such as cybersecurity, financial inclusion and ethical considerations all related to the management and operation of CBDCs. Regarding UEMOA countries, efforts are underway to harmonize CBDC regulations between the member states of the union. The objective is to facilitate transactions between these countries but also to strengthen economic integration and this integration is now easier because these countries share the same central bank.

The primary findings of our research are organized into two subsections. The analysis of the online interviews begins with the generation of initial codes from the collected data. These codes are then analysed to highlight the main themes, which include ethical considerations, regulatory challenges, technological readiness, and finally financial inclusion efforts. We will then see in the same chapter a detailed analysis of these themes, exploring the practical implications of CBDC adoption from the perspective of various stakeholders. The results of the online survey are used to complement our findings received during the interviews. These results provide quantitative data on customer profiles, payment methods and attitudes in the use and management of digital currencies. This survey also allows to explore the specific challenges and opportunities related to CBDCs in the UEMOA region, particularly in Mali or Burkina Faso and Nigeria. The survey results allow to summarize the respondents'

[74] Research Design: Quantitative, Qualitative, Mixed Methods, Arts-Based, and Community-Based Participatory Research Approaches by Patricia Leavy, Year 2017 -P183

perspectives on the ethical aspects, compliance aspects and cybersecurity dimensions of CBDCs.

Additionally, to the primary research, we integrate a secondary data analysis. This analysis integrates an extensive review of academic journals, government and regulatory publications, and online databases. Academic journals give both theoretical and empirical insights into the study that help to contextualize the research within the broader context of existing literature. Government and regulatory publications provide insight into the evolving regulatory landscape, while online databases provide data and best practices in CBDC implementation in the use of technology and innovation.

We conclude by emphasizing consensus, disputes, and concerns by various stakeholders on the adoption of CBDCs. The results analysis underlines that CBDCs need to be taken forward with comprehensive strategies on ethics compliance, cybersecurity, and inclusive financial policy. Results have highlighted implications for a comprehensive strategy in implementing CBDC. Similarly, policymakers can work on enhancing the benefits arising out of the CBDC with minimal risks to regulatory and technological hurdles. It is acquired from the insight elicited from the study that their valued guidance against the development of the CBDCs in Mali and other developing contexts is critical in making finance more inclusive, secure, or inclusive and safer.

4.3. Interview Analysis

The interview analysis played a critical role in this study. To start, discovering and developing initial codes was the beginning of analysis. These codes represented shared ideas and themes between various interviews or between responses in an online survey. For instance, numerous mentions of CBDCs being difficult to integrate with present financial infrastructure, concerns regarding ethics and privacy of data, and increased cybersecurity requirements were present. Next, these themes were organized in an orderly manner to enable a deeper examination of them. Once these initial codes were developed, then key themes in the information were discovered. Out of the themes that we selected, most apparent ones included difficulty in utilizing CBDCs, particularly ensuring that the system is efficient and simple to use. Another strong, emergent theme was ethics considerations about CBDCs; specifically, the tracking of information regarding individuals had to ensure robust protection for their privacy. Inability to comply with rules or regulations majorly regarding operations of CBDCs and their alignment with domestic and international law, became an emerging theme in itself. Other emerging themes concern the effect of emergent technologies, including blockchain-a facilitator of opportunities at the same time introducing complexities in the CBDC ecosystem.

A review of these themes allows for further refinement of these themes, breaking them down into more specific sub-themes helps to better capture the different textures around the ideas and experiences of the interviewees. For example, under the theme “Compliance Challenges”, sub-themes such as “Alignment

with international AML/CFT/PF standards", "User identification challenges, KYC", "Regulatory disparities across jurisdictions" and "Integration of compliance frameworks with new technologies" were identified. These sub-themes allowed us to better understand the specific regulatory hurdles faced by different stakeholders and highlighted the need for tailor-made solutions to address the various challenges of CBDC implementation.

This analysis also allowed us to highlight different perspectives of the respondents on key issues such as the balance between privacy, compliance, security and different regional approaches in CBDC implementation. These findings provide a comprehensive overview of the current state of CBDC implementation, and one can easily perceive the areas that require further attention and development. The analysis of the interviews revealed the multifaceted nature of CBDC technical implementation, highlighting the need for a balanced approach that addresses ethical and regulatory challenges while leveraging emerging technologies to enhance and secure the overall system against cybersecurity threats.

4.3.1. Highlights the main Themes

The analysis of interviewee responses uncovered a range of important themes critical for successful execution and governance of CBDCs. These themes point out the obstacles and complications for professionals in this new field.

i. Ethical Concerns

The most debated ethical issues, in general, deal with the anonymity of users, confidentiality, and integrity of security information. CBDCs allow an unprecedented level of transparency, hence giving a chance to track each and every transaction-a feature not available in conventional banking systems. Interviewers voiced concerns about abuse of powers; governments and possibly other powers could use CBDCs for tracking financial activity in a manner not explicitly approved by citizens.

Key points noted:

- **Data Protection:** Methods for encryption, terms for dissemination of information about users, and processes for anonymization.
- **Surveillance Risks:** Government spying, tracking of transactional histories, and general information collection.
- **User Consent:** Permission requirement, opting out/in, transparency in the consent document.

ii. Compliance and Regulatory Challenges

One of the big challenges is how CBDCs will fit into existing frameworks, notably AML/CFT/CPF. Interview respondents mentioned difficulty in balancing CBDCs with both international standards and

national legislation. In addition, virtuality added complexity to KYC processes. Efficient in a virtual environment, identification can become a problem when poorly performed, and can contribute to an increased level of money laundering activity. In this regard, unambiguous and valid compliances must be devised to dispel such apprehensions.

Key points noted:

- **Regulatory Alignment:** Gaps in legislation, harmonization of approaches, integration of international standards.
- **Framework Adaptation:** Framework development and adaptation for integration of CBDCs.
- **Cross-Border Regulation:** Territorial conflicts, supervision of cross-border transactions, and tax requirements.

iii. Technological Impact and Cybersecurity

The CBDCs are made possible, enabled, by blockchain technologies that are emerging. It offers transparency, security, but some of the significant technical challenges relate to the integration stage with current financial systems. While conducive for security, immutable blockchain nature makes compliance efforts hard in particular when errors or legal issues require transactions to be reversed.

The issue of data breach is another potential problem, as CBDCs operate in the digital environment and are highly vulnerable to cyber-attacks. This vulnerability makes it crucial to put in place robust data protection measures. These measures include both technology and clear policies to protect users' privacy rights. Continuous monitoring, rapid response protocols and collaboration with cybersecurity experts are essential to protect CBDC infrastructure.

Key points noted:

- **Blockchain Adoption:** Security Protocols, smart contract implementation and interoperability issues.
- **Innovation Opportunities:** Fintech collaborations, development, and enhancements of user experiences.
- **Cybersecurity Threats:** Vulnerability Assessment, Response of Cyber-Attack, Encryption Standards.

These themes and granular codes are a well-specified approach that interview content might be understood to analyze categorizations and, importantly, probe deeper into some very specific areas related to CBDCs.

4.3.2. Review and define themes

We started analysing the interview data by developing preliminary themes that would be reviewed and narrowed down for the purpose of capturing the exact details and background in which they were brought up. Narrowing down was done by dividing the general themes into more precise sub-themes that gave a greater insight into various challenges and possibilities in the utilisation of CBDCs.

i. Ethical Concerns

One dominating theme that came from these interviews was " **Ethical concerns".** When broad and broken down in detail, this theme was subdivided into a number of principal sub-themes, namely, **Data privacy** and **surveillance risks**.

- **Data Privacy**: One issue which bothered the users most was how the user data are dealt with in the CBDC system. Whereas conventional banking schemes rely on codified protocols that guarantee privacy in data handling, the advent of CBDCs might introduce unparalleled data accumulation and surveillance opportunities. As this respondent pointed out, there is a chance that central banks may enjoy access to transactional data granularities that can be leveraged if they are not kept in check. It also showed how important encryption of data and protection are in maintaining the security of individual financial information.
- **Surveillance Risks**: The second mentioned ethical concern is the danger that CBDCs will enhance the surveillance capacity of governments because, while CBDCs are now capable of enhancing transparency and combating illicit activities, they are also capable of facilitating another threat that is intrusive surveillance of an individual's transactions. Examples of such dilemmas given included that CBDCs would let the governments of every country keep a real-time watch on each and every transaction that happened, and that might give way to some possible abuses of power or invasion into people's liberties. This sub-theme elaborates on how an extremely fine line should be drawn in the use of CBDCs for the benefit of the public, while guaranteeing the protection of the privacy rights of citizens.

ii. Compliance and Regulatory Challenges

The second theme, "**Compliance and Regulatory Challenges**", was developed to tackle these precise areas of concern as subject matter: **Alignment with International Standards and Local Regulatory Adaptations**.

- **Alignment with international standards:** Respondents highlighted the importance of ensuring that CBDCs comply with international regulations, including in the areas of AML/CFT/CPF. We received one response explaining the challenges faced in aligning CBDC operations with strict international standards, which often require sophisticated compliance mechanisms.
- **Local regulatory adaptations**: Forum dialogue also stressed the need for local regulators to

make changes in their regulatory frameworks to fit the specific character of CBDCs because even though all the technologies evolved from the same origin, regulations vary across regions. Participants discussed how current regulations can be inadequate to deal with the challenges of digital money in general and CBDC specifically and must be amended and updated in order to regulate efficiently. We will have a chance to go back to local documents to confirm this hypothesis. This sub-theme brought out the evolutionary character of the regulatory framework and the need for constant updating to match the speed of technological evolution.

iii. Technological Impact

Technology in CBDC operations was another theme that was elaborated, and it resulted in sub-themes such as **Blockchain Advantages** and **Technological Complexities**.

- **Blockchain Advantages**: Among the points we presented was the benefits of blockchain. Blockchain would make the CBDC more secure and transparent. Blockchain's immutable ledger would provide a secure and tamper-proof record of transactions, thereby increasing trust in the system.
- **Technological Complexities:** Integration of blockchain with other emerging technologies, such as their use in Mali in telecommunication companies, raises complicated issues, more so in terms of compliance with regulatory requirements and management of these systems. The challenges will then relate to the regulatory frameworks and system governance. For example, auditing and oversight of such technological systems require some expertise in the field, which is often expensive and difficult to introduce.
- **Regulatory Readiness**: In fact, the sessions also revealed that more progressive regulatory regimes in territories were more likely to implement CBDCs. As an example, one participant highlighted how progressive legislation with regard to digital currency made one jurisdiction easier to adopt than other jurisdictions which did not have as enabling, or were older, regulatory regimes.

iv. Cybersecurity

Another category grouping for the topic "Cybersecurity" was **Threat Identification** and **Response Mechanisms**.

- **Threat Identification**: The respondents identified different forms of cybersecurity threats that CBDCs are likely to be exposed to, including data breaches and hacking. Because of this, one of the reasons for proactive identification is the detection of a possible vulnerability during testing.
- **Response Mechanisms**: Deliberations dwelt on the mechanisms through which these threats can be combated, and this includes such mechanisms as putting in place sophisticated methods

of encryption, surveillance systems working round the clock. To be sure, this was evidenced by the formation of a task force for cybersecurity that would take care of all possible breaches; an indication that proper response mechanisms are needed.

Refining and defining these themes will, therefore, provide a more focused analysis of the interview data with rich insight into the intricacies and possibilities of CBDCs.

4.3.3. Initial codes generation

An interview is a question-and-answer session. Questions are asked by the student and then the answers are noted. But frequently the discussions go beyond the topic and thus exceed the allotted time of 30 minutes with several written notes that cannot all be adequately represented in this document, so a more efficient way of the coding system is needed for further analysis. The first step in the interview analysis was to systematically generate codes, which involved identifying key themes and patterns that emerged across the various discussions. Through review of the interview responses, several recurring concepts were identified, and we weighted these responses to select the highest weights, such as **Privacy Data Protection, Surveillance Risks, Misuse of Data, Frameworks Adaptation, AML CFT Protocols, Cross Border Regulation, Regulatory Alignment, Blockchain Adoption, Compliance Challenges, Smart Contract Implementation, Data Integrity**. The overview of the initial code generation based on the interview responses is as follows:

Section/Raw Data	Preliminary Codes	Final Code	%Weight
Ethical concerns around CBDCs include issues of data privacy and the potential for increased surveillance.	Data Privacy, Surveillance Risks	Privacy Data Protection, Surveillance Risks	15%
Detailed tracking of transactions by CBDCs raises significant questions about privacy protection.	Transaction Tracking Risks	Surveillance Risks	10%
It is crucial to ensure that user data is anonymized to prevent misuse or undue surveillance by third parties.	Data Anonymization, Misuse of Data	Anonymization Techniques, Misuse of Data	10%
We implemented strict data management protocols to ensure that only necessary information was accessible to authorities while protecting user identities.	Data Protection Strategies	Privacy Data Protection	10%
The initial challenges included the need for substantial investments in upgrading our surveillance technologies and training staff to manage these new systems.	Tech Investment Challenges, Staff Training	Frameworks Adaptation, AML CFT Protocols	15%
During a collaborative project with a financial institution, we encountered significant compliance issues due to differing international regulations.	Regulatory Diversity, Compliance Challenges	CrossBorder Regulation, Regulatory Alignment	20%
To overcome these challenges, we developed a flexible compliance framework designed to adapt to various regulatory environments.	Compliance Framework Development	Frameworks Adaptation	10%

Section/Raw Data	Preliminary Codes	Final Code	%Weight
Blockchain introduced complexities in compliance, particularly regarding data management and regulatory adherence.	Blockchain Compliance Complexity	Blockchain Adoption, Compliance Challenges	10%
In implementing blockchain, we had to ensure that smart contracts adhered to the existing regulatory standards.	Smart Contract Management	Smart Contract Implementation	10%
We had to rethink our database schema to integrate blockchain, which involved new ways of storing and processing data to meet regulatory requirements.	Data Management Challenges	Data Integrity, Blockchain Adoption	10%

Table 7: Coding segmentation

These initial codes then provided a basis for further analysis, enabling the identification of key themes that would guide further exploration of CBDC issues. These codes were important in capturing a variety of perspectives and experiences from interviewees, providing a complete picture of challenges and opportunities associated with the implementation of CBDC while framing this research.

4.3.4. Respondents' perception of CBDC

Analysis of interview responses revealed that CBDCs offer both opportunities and challenges. The key opportunities include increased financial inclusion and improvement of the monetary framework as well as policies. The challenges also include more robust technological infrastructure, disruption of existing financial systems, additional requirements for data privacy and security. To a large extent, the interviews assumed that properly managed implementation would be the key factor to maximize the benefits of CBDCs and reduce the associated risks.

CBDCs could achieve **increased financial inclusion,** a notable opportunity by giving digital financial services to everyone, whether residing in unbanked or underserved areas, hence bridging the gap between underbanked populations. For instance, one of the respondents commented that CBDCs can provide easier access in countries where traditional banking is not well developed such as Mali, Burkina Faso in UEMOA zone and allow people to be connected to the financial system without a bank account.

Another great avenue that was discussed was the **enhancement of monetary framework and policies**. CBDCs could give central banks more direct control over aggregates of money and interest rates, thus setting more precise and rapid monetary policies, which would be particularly effective during times of economic crisis where traditional tools may be less effective. For instance, according to one of the respondents, in cases where the distribution of cash gets problematic, CBDC can execute direct transfers among individuals for the sake of the stabilization of the economy within more quickly.

These discussions also emphasized different concerns related to CBDC. First and foremost, **robust**

technological infrastructure was considered necessary. Any issuance of a CBDC implies secure, reliable, and scalable digital infrastructure that can sustain a higher volume of transactions involved while maintaining integrity. Poor digital infrastructure could significantly delay or limit the implementation of CBDC; without the needed technological backbone, the risks of system breakdowns or security breaches might dent people's confidence in the new currency.

Another challenge identified was the potential **disruption to existing financial systems.** Their introduction could significantly alter the role of commercial banks, probably shifting their intermediary function and reducing profitability. This might lead to opposition from the banking industry itself and may require a balancing act of sensitivity to ensure that any benefits of CBDC do not come at a cost to financial stability. Interviews were given as a case in point about the concerns that high diffusion of CBDC could lead to disintermediation, where customers would shift funds from commercial banks into digital currencies that are held directly with central banks, reducing the liquidity available in traditional banks.

Furthermore, many of the concerns were related to the guarantee of **privacy and data security**. As CBDCs operate in the digital realm, they hold the same cyber threats any other computer-based system would have such as data breaches, and unauthorized access to sensitive financial information. It was highlighted that there should be strong encryption methods, access controls and continuous monitoring that would help protect user data and build trust in the system itself. Deploying advanced security protocols and regular audits may be necessary to address cybersecurity threats.

At the end, while CBDCs present a number of opportunities for improved financial inclusion and the pursuit of sound monetary policy, their eventual deployment is conditioned on how technological infrastructure challenges, potential disruption to existing financial systems, and privacy and security protection of data are overcome. Interviews underscored the need for a careful, gradual approach to ensure the capture of the benefits of CBDC while keeping at bay risks involved.

4.3.5. From CBDC to Digital Currency Electronic Payment

While CBDC is issued directly by a central bank, Digital Currency Electronic Payment (DCEP), a broader term encompassing various digital currencies issued by different entities such as governments, central banks, financial institutions, private companies, etc. DCEP, particularly with respect to CBDCs, were recurring topic in the interviews. Even though DCEP systems will develop efficiency and transparency of transactions to a new level, they will come with inflated costs in cybersecurity improvements and data protection protocols. In addition, the embedding of DCEP into traditional banking brings another series of issues, in particular with regards to maintaining interoperability and

compliance across different regulatory environments.

When DCEP is particularly implemented through CBDCs, represents a transformative approach to modernizing financial systems. The potential of DCEP systems in improving the efficiency of transactions with a higher level of transparency was a point in question during interviews. It might cut down costs and time of a financial transaction through the possibility of making instant and direct transactions between the transacting parties without the involvement of traditional financial intermediaries, which would result in more economic activities and financial inclusion.

Some respondents gave an example where through DCEP, the cross-border payment was done. The process usually has delays and high charges since there are so many financial institutions and clearinghouses involved. But in this case, near-immediate settlement was facilitated using DCEP. It not only increased the efficiency but also provided more transparency into the process of the transaction since by real-time, both parties could trace the movement of their funds. These discussions, however, also brought to the fore **cybersecurity challenges** to DCEP systems from a cybersecurity perspective. Security Challenges of DCEP Systems. Since DCEP is an entirely digital setup, it remains amenable to threats of cyber-attack and many other crimes related to information security. Indeed, quite a number of the contributors were concerned that the current level of cybersecurity would not be able to protect such risks. For example, we noted an instance in which a pilot DCEP was undergoing a focused cyberattack that could potentially result in an infringement of the personal information of the users. The incident was a stark reminder of the need for robust cybersecurity protocols, which must encompass, among others, advanced encryption mechanisms, multi-factor authentication, and real-time monitoring systems for early threat discovery and mitigation of ensuing damage potential in view of threats that can cause grave losses.

In addition to cybersecurity, **data protection** emerged as a critical area of concern. Finally, since digitalized currency and payment systems involve the collection and storage of massive volumes of personal and financial data, it becomes very critical that stringent measures of data protection are in place. Lack of appropriate safeguards of the DCEP systems might expose users to privacy violation and unauthorized access to data, as participants warned. A representative example shared during the interviews that the privacy-enhancing technologies (PETs) in the DCEP framework added its ability to make transaction data anonymous but still enforce regulatory requirements on transparency and reporting of the data. It should also be noted that this PET is currently not available in CBDC operations in our study region.

Another significant theme was the challenge of **integrating DCEP with traditional banking systems**. However, in general terms, participants explained that although DCEP has many advantages,

complications arise when it comes to integrating DCEP and its capabilities into the legacy banking infrastructure. The critical issue here is to maintain interoperability between DCEP and the existing financial system. Interoperability will be crucial in making DCEP transactions completely seamless with traditional ways of payment and making sure that all these activities are done within preset regulatory frameworks. The research accurately outlined the complexities of integrating the DCEP within the current framework of SWIFT foreign exchange transactions, and he says that this involves more than just making the technical changes, in his work, he had to use the process of negotiating new standards of compliance, which covers the special nature of the digital currency.

Compliance with regulatory standards was another challenge highlighted in the interviews. It was added that ensuring DCEP systems operate within local and international regulatory requirements especially by AML/CFT/CPF is challenging. With respect to digital currencies, their global nature locates their regulatory compliance not in a single jurisdiction but under a myriad of legal frameworks. One example provided by a respondent related to geo-fencing technology that had to be put in place on a DCEP system in order to block transactions which could have been a violation of international sanctions or any other type of regulatory restrictions.

In brief, while DCEP systems represent a promising advancement in digital finance, their successful implementation requires addressing a series of challenges related to cybersecurity, data protection, interoperability and regulatory compliance. The interviews indicated very clearly that to realize its full potential, DCEP would need a deep investment in technological infrastructure and sustained collaboration with regulatory bodies. Proactively solving these challenges will let DCEP not only further develop a new generation of payment systems but also unlock the path toward a more secure and inclusive financial future.

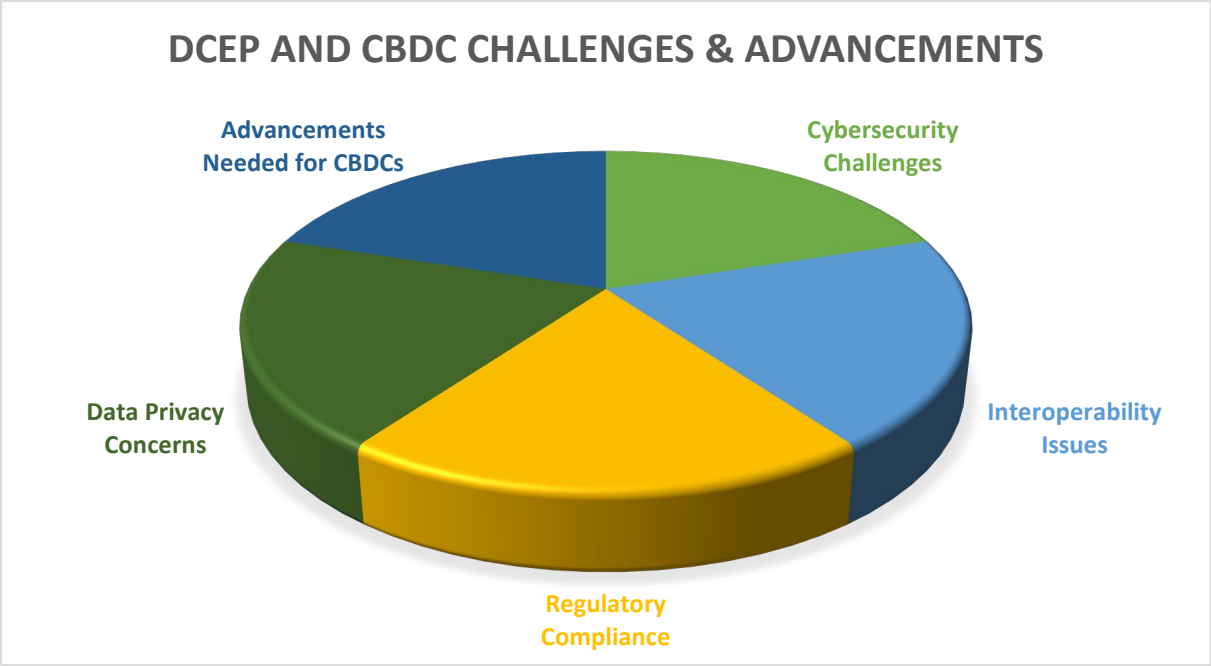


Figure 18: DCEP and CBDC Challenges & Advancements

Interoperability challenges of DCEP

The interoperability issue for the DCEP system occurs in comparison with the legacy financial infrastructures and other electronic money. Such a difference in operation frameworks is caused by a difference in technological and operational frameworks in matters of standards, regulation requirements, and technologies.

1- **Technological Standards:** Most traditional banking systems are based on established and legacy technologies that are, in their practicalities, somewhat incompatible with the new blockchain-based infrastructure of DCEP. This can lead to difficulties in achieving seamless transactions between digital and traditional financial systems. For example, problems may occur in data exchange, speeds of transaction processing, and account reconciliation between systems.

2- **Regulatory Compliance:** Most DCEP systems claim to adhere to local and international regulatory requirements, especially those involving AML/CFT/CPF. DCEP must transact between these systemic entities and comply with their definitions on AML, CFT, CPF but these requirements vary widely from jurisdiction to jurisdiction. That poses a challenge to ensure that DCEP transactions meet all necessary requirements for compliance at interaction points with the rest of the traditional banking system. Often, this results in increased costs, delays, and potential legal exposure for the financial institution.

3- **Operational Frameworks:** Basically, the operational processes that currently guide the systems of the traditional banking are often rigid, controlled, and high-structured, to the extent

that it will be hard to fit the more dynamic and decentralized processes expected of DCEP. For example, traditional banks would demand centralized control and surveillance over transactions, whereas DCEP systems will work with distributed ledgers that blur the traditional definitions of control and ownership.

4- **Cross-Border Transactions**: Interoperability in cross-border transactions is a challenging task due to the engagement of many different countries with their own developed currencies, regulatory environments, and financial systems. This is more or less the case of transactions with both host and visiting parties, thus ensuring DCEP works seamlessly across the globe by harmonizing standards and protocols a process in itself involving and complicated.

5- **Legacy Systems and Transition Costs:** Most of the financial institutions have already invested in their present infrastructure, which was based on traditional forms of currencies and payment systems. Therefore, going to DCEP-compatible systems would mean heavy investments in new technologies and training. This provides the cause for resistance to change and results in financial risks.

Addressing these interoperability challenges is crucial for the widespread adoption of DCEP through CBDC. This has to be done through continuous collaboration among technology developers, financial service providers, and regulatory bodies to ensure realization of a seamless and effective financial ecosystem that will accommodate the needs of both digital and traditional currency systems.

Based on the experiences with DCEP, what advancements are needed for CBDC?

What is missing in CBDCs? Here are the main areas of development that need to be realized for CBDC systems to reach their full potential:

1- **Enhanced Cybersecurity Measures:** As CBDCs will be digital in nature, stringent cybersecurity measures will have to be adapted to defend against hacking, fraud, and data breaches. This would involve developing advanced techniques of encryption, secure authentication processes, and real-time monitoring systems.

2- **Scalability solutions:** As CBDC systems grow in functionality, they should process a high volume of transactions without affecting speed and security. This demands scalable blockchain solutions or other distributed ledger technologies to process a large number of transactions.

3- **Interoperability Standards:** The establishment of standardized protocols for interoperability is crucial to facilitate the smooth integration of existing financial systems and various digital currencies. This process encompasses the alignment of data formats, transaction protocols, and compliance mandates across diverse platforms.

4- **Regulatory Frameworks:** There is a need for lucid and consistent regulatory guidelines to govern the use of CBDCs both domestically and internationally. This concerns specifically areas such as personal privacy, AML, CFT, CPF.
5- **User-Friendly Interfaces:** For a wide acceptance of CBDC systems, designs should have user-friendly interfaces that would attract both the technologically sophisticated users and those who are not as familiar with digital money. This includes easy mobile applications and available customer support services.
6- **Offline Capabilities:** This means developing mechanisms through which CBDC can be accessed and used when there is low or poor connectivity. This may become possible with the help of physical cards, secure offline wallets, or any new innovative devices.
7- **Facilitating cross-border transactions:** CBDCs need to be empowered for efficient processing of cross-border transactions, which requires improvement in international settlement systems and currency conversion and regulatory compliance across various jurisdictions.
8- **Public Awareness and Education:** For wide acceptance, CBDCs require far-reaching campaigns for public awareness and educational activities to let users understand the benefits, risks, and functionalities of digital currencies.
9- **Environmental Sustainability:** With the growing CBDC systems, there has to be consideration for the environment in terms of energy use, for example, driven by blockchain networks. Improvements in energy-efficient technologies will be key to minimalizing the carbon footprint of digital currencies.

Such improvements can achieve the threefold needs of security, efficiency, and inclusion in CBDC systems, leading ultimately to their successful integration into the global financial landscape.

How were data privacy concerns arrested in CBDCs?

Different issues associated with data privacy in the framework of CBDCs were addressed by some fundamental strategies, such as:

1- **Strict Access Controls:** Setting up role-based access controls on who may view or change sensitive data. Only the authorized personnel are allowed to look at the information, hence reducing the possible risks of leakage of data.
2- **Robust Encryption Protocols**: Strong encryption algorithms provide superior standards for data encryption processes across every position to make interception in transit or when data is in storage extremely improbable to crack in the case of an attack.

3- **Compliance with Privacy Regulations:** Bringing the operations of CBDCs into alignment with the existing local and international data protection regimes, like APDP law, GDPR or CCPA, aiming at legal compliance and protection of users' rights.
4- **User consent mechanisms:** Transparent user consent mechanisms that guarantee that users are aware of how, when, where, and why their personal data is being used, stored, and shared, and have the ability to either consent or reject certain data collection practices.
5- **Regular Audits and Monitoring:** Regular periodic audits, continuous monitoring of the flow of data and processes against any vulnerability or breach, will enable immediate responses in case of any violation of privacy.

These measures engender the confidence that, in the development and deployment of CBDC systems, data privacy concerns are well taken care of so as to create trust among users and regulators.

4.3.6. Summary: Consensus, Disputes, and Concerns

In summary, what came out of the interviews was one consensus: potentials of CBDCs to enhancing the financial system in terms of **transparency and efficiency.** However, there were disputes regarding the best approach to address ethical concerns and regulatory challenges. Some recommended **robust privacy protections,** while others suggested the development of comprehensive frameworks that regulated it. There were also concerns as to the long-term sustainability of the CBDC systems, especially in areas where digital infrastructure is less developed.

Interviews conducted for this study revealed an overall high consensus in this regard: CBDCs can actually turn into a real game changer, changing the landscape of finance. Among the main advantages, the surveyed pointed to CBDCs increasing transparency, easing financial transactions, and bringing efficiency to the financial system as a whole. It was generally envisaged that CBDCs could help improve most of the shortcomings of current financial systems related to slow transaction times and high costs of cross-border payments if they put up digital technologies.

The interviews also exposed some key differences over how best to address ethical concerns and regulatory challenges raised by CBDCs. Perhaps the most contentious issue was the balance to be struck between privacy and regulatory oversight. Some interviewees forcefully made the case for robust privacy protections that would ensure protecting user data and preventing government overreach. This, in the absence of good privacy measures, will contribute to increased surveillance of transactions, thus causing erosion of freedom and privacy rights at the individual level. One of the respondents reflected that CBDCs could be used to trace and control spending behaviours with consequences in relation to civil liberties.

On the other hand, participants have pointed out the need for appropriate and holistic regulatory frameworks to ensure CBDCs are not used to launder money, to finance terrorists or to increase proliferation of weapons of mass destruction. In their own view, they believe that robust regulatory oversight is key to maintaining financial markets and systems, and thus securing that no criminal uses of CBDC occur. Of these participants, the ones who endorsed the use of KYC and AML even at some personal sacrifice to privacy. This gap reflects how policymakers are already moving into a very complex ethical environment in the design of CBDCs.

Apart from the privacy and regulatory debates, concerns were also aired over the long-term sustainability of CBDC systems, particularly in territories that are less developed digitally. According to a number of interviewees, while CBDCs hold a range of important potential benefits, all of these come with the precondition that robust technological infrastructure should be available. Implementation of the CBDCs in areas that lack digital infrastructure can become highly problematic due to limited access to technologies and a digital divide between urban and rural areas. For example, in some developing countries where access to the internet is not very widespread and people lack relevant digital skills, the wide application of CBDCs may be complicated. Instead, it can be provocative of financial exclusion, rather than a solution to the problem.

Second, there was the likelihood of disrupting current systems that the use of CBDCs might bring. For example, the fear that once CBDCs were issued, this would undermine the role played by traditional banks in financial systems. Traditional banks might consequently suffer destabilization and bring about unintended consequences on the economy. Of special concern in the area are possible changes that CBDCs might bring about in monetary policy and financial intermediation, ushering in new risks regulators and policy authorities ought to take up. We believe that if this currency were managed under the responsibility of these banks, this could help resolve the difficulties associated with it.

That is, this set of interviews has disclosed profound disagreements and concerns related to privacy, regulation, and sustainability. The issues raised highlight the importance of thoughtful, balanced design of CBDCs that will enable them to fulfill their potential without giving rise to new risks or further amplifying existing inequalities within the financial system.

4.3.7. Interview Findings

The findings from these interviews bring out the complexity in the implementation and operating of CBDCs. While both may agree on the array of important benefits that CBDCs take, mostly on improving financial inclusion and transparency of transactions, there is important challenges come due to this; some of them would include regulatory compliance and ethical concerns on privacy, technological

demands for a fully integrated CBDC system. The results have indicated that, in the successful deployment of CBDCs, an important implementation approach would be gradual, controlled, and constantly adjusting using real-time feedback.

It provides an overview of major themes and issues relating to the implementation, operation, and management of CBDCs that came up from the interviewees. As a result, the interviews brought out a comprehensive discussion with respect to the challenges and opportunities connected with the utilization of CBDCs. Although consensus on the beneficial sides of the CBDC was unanimous, a number of disputes and concerns have been indicated in the course of interviews, which have to be taken into account for successful implementation.

i. Consensus on the Benefits of CBDCs

In general, the interviews showed a general agreement about CBDCs' potential for innovation in the financial system. Common mentioned benefits include CBDCs' potential to promote financial inclusion. In areas characterized by poor access to traditional banking, CBDCs represent a feasible digital alternative for unbanked and underbanked communities to access financial services. In addition, CBDCs have the potential to bridge the divide between the formal financial system and groups traditionally locked out of its system through access to financial services in a digital form. More so, apart from listing the above in our agenda, we could, rightly or wrongly, attach our own initiative, which cashed on the spontaneity of CBDCs and virtual currencies, to the framework of our global operations, and hence transaction times reduced meaningfully and hence it increased efficiency manifold.

It was also indicated that another advantage of CBDC is that it would probably promote transparency in transactions. All transactions with digital currency-based CBDCs are completely traceable. This could lead to a reduction in fraud, money laundering, and other illicit financial activities. This characteristic was considered useful in countries where corruption and mismanagement of money have become normal practice since it would enhance confidence in the financial system.

ii. Disputes and Challenges

Notwithstanding this agreement around the benefits that CBDC would bring, the interviews revealed crucially disagreement upon how to overcome challenges linked with its implementation.

1- Regulatory Compliance:

Another point which came out to be particularly thorny was how to ensure the compliance of different regulatory frameworks operating in different areas. CBDCs add new dimensions to the already complex regulation authorities in that they are digital and decentralized. Indeed, different countries have varying maturity levels in their regulations, making inconsistencies within CBDCs, in terms of both their

implementation and governance, quite possible. Some interviewees stressed the need for greater centralization through the adoption of international standards in order to guarantee homogeneity across borders. Local regulations are crucial and would never apply an approach in a cookie-cutter way. For example, if it is a region with less-developed regulatory frameworks, then maybe a more tailored approach would be needed to ensure that CBDCs are not inadvertently creating new risks.

2- Ethical Concerns and Privacy:

Another issue of contention was on how to deal with the ethical issues surrounding privacy. Those interviews were conflicting as per opinions on their definition of what kind of privacy should be extended to CBDC users. While some interviewees want maximum protection of privacy against government reach for individual freedom, others said a fair volume of transparency is required to fight financial crime.

One of the persons interviewed highlighted that CBDCs can become a means for mass surveillance by governments, especially in countries with an authoritarian regime. A few interviewees suggested that strong encryption and anonymization techniques could be used for this purpose which is not currently used in UEMOA. The suggestion was, however, not unanimously agreed upon because some noted that too much anonymity would not help to prevent financial crimes such as money laundering and financing terrorism or even prevent the proliferation of weapons of mass destruction.

3- Technological and Infrastructure Demands:

The other major area of concern was the technology itself that would be required in implementing a fully integrated CBDC system. Many interviewees pointed to the challenges necessitated by the requirement for strong technological infrastructure, particularly in regions with underdeveloped digital infrastructural development like in Mali and in Burkina Faso.

For example, one of the respondents described struggles they are having with a pilot project in a rural setting dogged by poor internet connections and limited access to digital devices, hence impeding the CBDC adoption process. In response, the respondents made some suggestions toward individual efforts to be taken in improving digital infrastructures, such as widening access to the internet and the use of affordable digital devices.

Moreover, interoperability with existing financial systems stands out as an interesting challenge. Ensuring that this interoperability is achieved to provide users with a seamless experience without fragmentation calls for coordination among many players, from the central banks to commercial banks and technology providers.

iii. *Concerns Regarding Sustainability*

Another major concern raised in the interviews was related to the sustainability of the CBDC system, mainly in areas with underdeveloped digital infrastructure, like the region of the study, Mali, Burkina Faso, Nigeria. While bringing in new technologies and innovations could be intended to bridge the existing gaps, there is the likelihood that the introduction of CBDCs may foster the existing inequalities in the absence of equal access to the required technology. Ensuring that CBDCs have access to all members of the population, including those in rural and underserved areas, is important to avoid the digital divide.

Several interviewees noted the importance of a phased and carefully monitored approach. Staggering CBDC deployments to ensure that an ample volume of real-time feedback is obtained during the execution of deployments can enable policymakers to adjust to any issues that may arise in the course of implementation and to realize all benefits without the introduction of new risks.

In sum, the findings from the interviews accentuate the CBDC complexity of deployment and management. While there is widespread agreement on the benefits they can deliver, chiefly regarding financial inclusivity and transaction transparency, there are also substantial obstacles. Notably, these concern regulatory adherence to the numerous current regulatory frameworks that would need to be incorporated; ethical concerns over privacy; and technical needs for a fully integrated CBDC infrastructure. These findings point towards the desirable design and implementation of them in a gradual manner, with due caution and under close observation and feedback for adjustment over time. It also gives a view of the major themes and issues imparted to the implementation and management of CBDCs, providing direction towards identifying challenges and maximizing benefits in emerging financial technology.

4.4. Online Survey

The "**Online Survey**" elaborates in great detail the way in which the survey was designed and administered. It explicitly indicates that these sections were carefully designed with a view to obtaining useful information about CBDCs. It initially describes the kinds of questions used. These questions were designed to explore broad themes like trust in digital currencies, privacy issues, and general sentiments about CBDCs. It also provides a breakdown of the demographics of the participants. It highlights the variation in their professional background, years of experience, familiarity with CBDC, and geographical location. This serves to guarantee a diversified view of the issues talked about.

The platforms that were used to send out the survey shall also be mentioned during the discussion. This will indicate how online tools are strategically utilized to get the maximum as well as responsive audience. From here, major findings emerging from the survey are then analyzed, pointing out the most

important emergent themes. While, for example, privacy concerns are universally recognized, there is notable variance in the levels of trust depending on familiarity with digital technologies and financial systems.

It also puts these results of the survey into perspective with the results from the earlier interviews, showing points both of agreement and disagreement. Such comparison makes clear that although both data underlined privacy as a key issue in trust regarding digital currencies, for example, survey respondents showed a wider spread than expert consensus. Lastly, the session wraps up with broad implications derived from the survey results, with suggestions that these shall be indispensable in setting up the future course of research and policy responses in this fast-developing CBDCs field.

4.4.1. Participants Profile and Demography

These surveys represent a cross-section of various professions, most of them in banking, finance, and cybersecurity. The survey questionnaires provided **196 responses** among participants with differing roles and quite varying lengths of time spent in their respective fields.

i. Educational Background

The majority of the people participating in this survey demonstrated a very high level of education; most have received at least a bachelor's degree. Many of them have master's or Ph.D. degrees as well. This manner of academic excellence reveals the professionalism of the respondents, most of whom are highly involved in banking, finance, and cybersecurity fields.

The responding samples varied widely in their level of educational attainment. The majority, **31.12%**, had a master's degree (Bachelor's + 5 years or higher), which showed highly educated participation by the respondents. The next is **27.55%** of the participants had PhDs (Bachelor's + 8 years or higher), the very best respondents indicating further that many of the respondents were well academically qualified. Of these, the participants who had attended college at a bac + 3 and bac + 2 level (Bachelor's + 3 years or Bachelor's + 2 years) constituted **15.31%** and **13.78%** of the participants, respectively. In addition, **12.24%** of the respondents had completed secondary education or lower (below Bachelor's + 2). This latter category also includes those who had no formal education or who did not specify or preferred to refrain from providing this information.

Educational Level	Count	Percentage
Master's Degree (Bac + 5) and above	61	**31.12%**
Doctorate Degree (Bac + 8) and above	54	**27.55%**
Bachelor's Degree (Bac + 3) and above	30	**15.31%**
Associate Degree (Bac + 2) and above	27	**13.78%**
High School Diploma (Bac) or below	24	**12.24%**

Grand Total	**196**	**100.00%**

Table 8: Educational Background

From this segmentation, it can be appreciated that the participants were largely well educated, which is important in order to understand their insights into complex topics such as Central CBDCs.

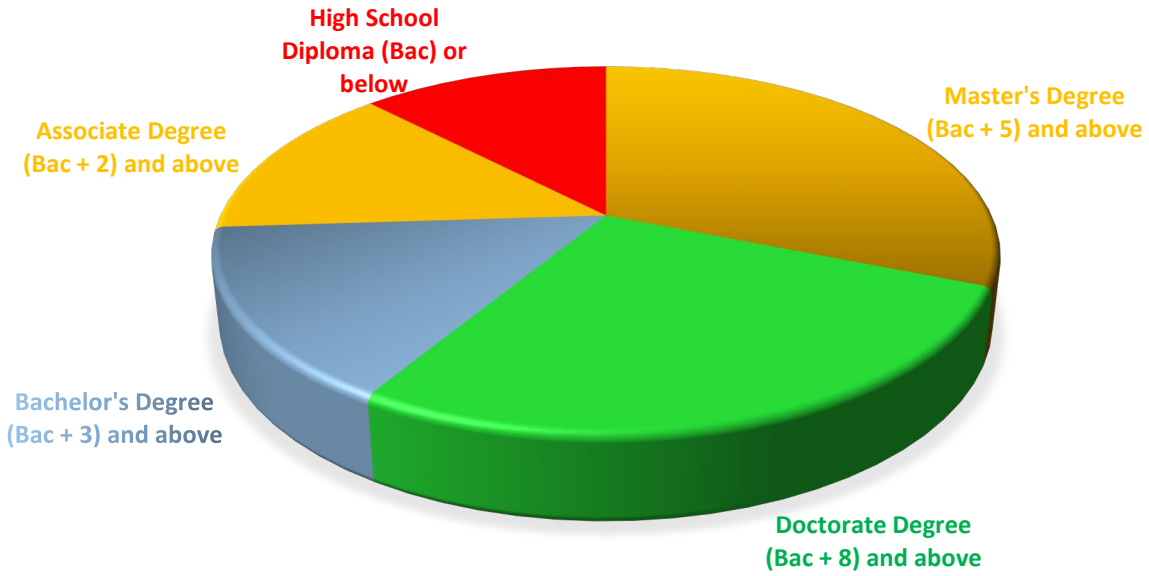


Figure 19: Participants educational background

ii. *Professional Roles and Experience*

This is confirmed in the range of the professional roles and experiences of the survey participants, which illustrated the variety of expertise needed for the CBDC context and the larger financial ecosystem. The majority of surveyed delegates lay within compliance, cybersecurity, financial analysis, and traditional banking roles, confirming the multidisciplinarity with which the implementation and, conversely, the development of the CBDC need engagement in this sector.

CBDC and IT Professionals: Most of the participants, **20.92%**, work in areas such as financial analysis, compliance, IT, and general banking operations. These activities are a testament to the multifaceted nature of expertise required by CBDC projects, which involve critical aspects including cybersecurity, financial strategy, and regulatory compliance. Of these, **14.80%** of participants engage in activities related to IT and Cybersecurity, therefore underlining the key role played in protecting digital assets and securing financial transactions. IT professionals design and provide maintenance for the infrastructure on which CBDC systems normally operate; this most often includes the integration of advanced technologies like blockchain and distributed ledger systems. Meanwhile, financial analysts and advisors constitute **20.92%,** who are very instrumental in the assessment of the economic impact of CBDC implementations, guide strategic investments, and provide substantial insights for effective decision-making. Banking professionals stand at **3.57%,** showing that traditional expertise in banking still has a

place in the context of digital innovation. They bridge the gap between the legacy financial systems and the emerging digital landscape so that the essence of traditional banking is not lost in the transition. All these put together show that CBDC projects have to be rightly mixed with technical, analytical, and operational skills for success.

Students: Students: A majority of the respondents are students, **26.02%**, which is an indication of interest in the next generation of professionals in fields related to CBDC.

Freshness of views, curiosity, and the ability to engage with emerging trends that students bring in are a part of the ecosystem that is priceless. Many of these students will likely be studying in streams of finance, computer science, or law-all highly relevant subjects concerning the development and implementation of CBDCs. The fact that such a broad section of them have participated in this survey itself shows that perhaps academic institutions have begun to recognize the importance of digital currency-related courses in their curriculum. In this way, students will be prepared for important roles in the future of digital finance by fostering knowledge and skills in this area.

Unemployed: Another prominent **6.12%** represents the category of unemployed candidates that would show, therefore, how attractive the sector in CBDC-related topics might be even among people that belong to less associated labor market categories, searching for inclusion and professional advancement within this niche; though most of such a category already passed some selection steps, especially unemployed ones having passed a technical evaluation. Needless to say, but the existence of unemployed members will also lead directly to the establishment of up-skilling and training courses.

Sales/Marketing Professionals: **2.55%** Sales and marketing are important in ensuring that CBDC solutions will always meet the needs of a very diverse customer base. Many times, they act as the first point of contact with the client, gathering feedback and adapting digital currency services to their needs, which ensures a better user experience and access. In such a case, their expertise will be very important in bridging the gap between technical innovation and user adoption-so that CBDCs are not just functional but also friendly.

Educators/Researchers: Representing **4.08%**, educators and researchers contribute significantly to the theoretical and practical understanding of CBDCs. Their work involves exploring the ethical, economic, and technological dimensions of digital currencies, providing a foundation for informed decision-making and innovation. These professionals play a key role in disseminating knowledge and fostering interdisciplinary collaboration, which is critical for addressing the complex challenges associated with CBDC implementation.

Compliance Professionals: A small but important cluster, **2.04%** of the total, consists of compliance officers and other professionals who work toward the development of CBDC systems in a way that adheres to regulatory requirements, thereby keeping financial risks minimal. Their tasks will relate to policy drafting, auditing, and transaction tracking to avoid situations like money laundering and fraud.

This group's competencies are needed to ensure confidence and integrity within the digital financial system.

Practitioner/Healthcare Professional: While a smaller subset at **2.04%**, health professionals show the wider appeal and interdisciplinary interest in CBDCs. Though their direct involvement might be very limited, it serves to bring out a diverse range of perspectives that can contribute to an understanding of the shaping of the digital currency landscape.

Senior Managers/Consultants: **2.04%** This category consists of those professionals who provide strategic guidance and specialized advice on CBDC projects. They ensure the initiatives are aligned with the best practices of the trade and regulatory requirements; hence, it reflects insight into how to balance innovation with compliance.

Others: A healthy percentage, **15.82%,** is what the "Others" category constitutes, which is bound to include administrative, support, self-employed, mechanical engineers, human resources specialists, or other categories of contributions to the general CBDC ecosystem. Accordingly, all of these functions may not touch on the core areas of technical and financial with respect to CBDCs but are integral to the seamless flow and accomplishment of such programs.

From this distribution, one could underline interdisciplinary CBDC development and implementation. Every single group brings something unique and is a witness, taken together, that some kind of cooperation has to be in place across professional domains. Diversity enriches insights collected, and the presence of those mentioned ensures an integral approach toward the problems and opportunities given by digital currencies.

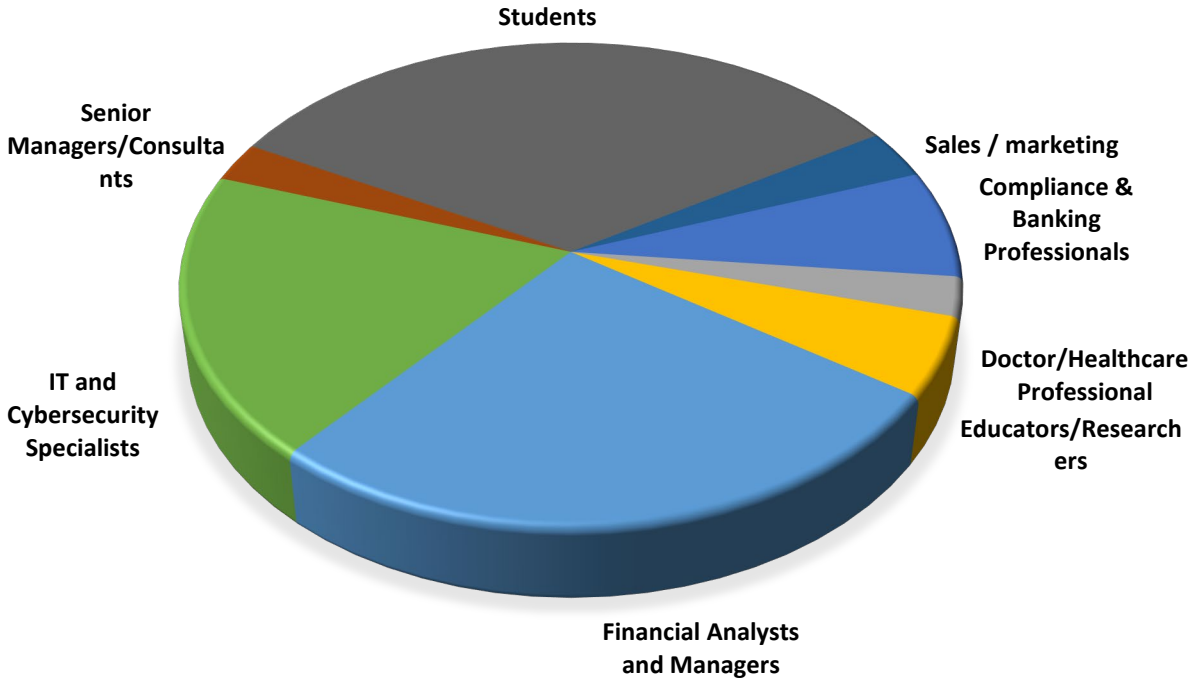


Figure 20: Survey participants fields of occupation

The multidisciplinary view about the successful implementation and management of CBDCs is therefore underscored. From this distribution, one could underline interdisciplinary CBDC development and implementation. Every single group brings something unique and is a witness, taken together, that some kind of cooperation has to be in place across professional domains. Diversity enriches insights collected, and the presence of those mentioned ensures an integral approach toward the problems and opportunities given by digital currencies.

iii. Geographical Distribution

Despite, the root of this study is Africa, with 33 participants (17.37%), the international dimension of the research is significant. This is also evident in the varied representation from all across the globe. Europe leads the way with 40.53% respondents, then Asia with 25.26%. participants, then North America with 10.00% participants, and South America with 3.68% participants. Small but significant representations are that of the United Kingdom with 1.58% participants, Australia/Oceania with 1.05% participants, and the UAE with 0.53% participant.

This wide geographical representation underpins the global relevance of the study for a wide set of insights emanating from various regions that are very active, both in innovations relating to banking and digital currency. While focusing on core inputs from Africa, participation across the world indicates interests in these globally important varied regional perspectives for better understanding and addressing challenges and opportunities associated with CBDCs in the fast-changing landscape.

iv. Professional Experience and Familiarity

Based on our survay, the respondents included a number of professions with some years of work experience and the use of the digital currency.

- ***Years of Experience:***

15.43% of total respondents mentioned experience of more than 10 years in their related industries. This is indicative of a very seasoned group of professionals with an in-depth knowledge base and experience in their particular fields.

20.00% of the respondents relate to the category of 3-10 years of experience. This categorically states the mid-level group must be very informed in regard to both old practices and trending ones within the industry.

30.29% have between 1-3 years of working experience, hence it represents the new sets but relatively growing experts of the industry.

Lastly, 34.28% have less than a year of experience, which again shows the inclusion of individuals in the very first phases of their careers.

- ***Digital Currency Familiarity:***

32% of the respondents answered that they are very familiar with the concept and functioning of CBDCs, which indicates a fairly substantial knowledge base among one-third of the participants.

40% indicated that they are generally familiar with CBDCs. This would suggest general awareness; however, much is yet to be learned.

28% of the participants reported not knowing what a CBDC is, which could be the group that perhaps needs further enlightenment on the use of this new technology.

Results from the survey show that the concept, use, and operations of CBDCs are known differently among the respondents:

- **Not Familiar:** There is a large group, 34.18% of the total respondents, who reported not knowing about CBDCs. This observation creates a need to increase educational programs and awareness-raising programs in improving an understanding of digital currencies and its potential implications.
- **Somewhat Familiar:** The largest, 36.22% share, report their level of knowledge as general or just above general about CBDCs. Probably they may hold a basic sense about the subject but lack insights to understand fully the mechanism behind CBDC and its benefits.
- **Very Familiar:** An impressive 29.59% of respondents report a high level of familiarity with CBDCs. This group probably consists of professionals, researchers, and/or interested parties with direct contact and/or high level of interest in the field of digital currencies.

The distribution reflects variable awareness and level of information about CBDCs, and therefore, a

demand for focused programs for closing gaps in information, particularly for respondents not yet aware of such innovations. Overall, 65.82% of respondents have at least a minimum level of familiarity with CBDCs, between basic and thorough level of awareness. This observation reflects a growing awareness and curiosity about digital currencies, particularly amongst respondents with a general and high level of awareness about the concept.

The findings reiterate the imperative for focused efforts in closing gaps in information for 34.18% of respondents not knowing about CBDCs, and at the same time, enhancing current awareness for the larger group. These observations reiterate a demand for collaboration between multidisciplinary groups and for educational programs for creating a larger and deeper level of awareness about CBDCs amongst a variety of interested groups.

- ***Usage of Digital Means of Payment:***

Significantly, **93.37%** of respondents in the survey showed use of mobile wallets, electronic banking, or prepaid cards for payment transactions. That reflects that respondents have high familiarity with electronic payment tools. On the other hand, about 6.63% of respondents have no use of electronic payment channels, and that could mean restricted access to, or preference for, traditional payment channels.

These previews of the participants' level of experience and familiarity with digital currencies give a well-rounded view concerning the state of the industry at the present time and also point out areas where further education or exposure to CBDCs may be useful. This comprehensive participant profile analysis highlights the diversity of perspectives and expertise involved in the survey, offering valuable insights into the critical considerations for CBDC adoption.

4.4.2. Key Findings and Insights

Analysis of survey data of CBDCs reflects an important insight from the stakeholders with respect to the associated ethical, regulatory, and cybersecurity issues related to the assets.

First, one main observation is the strong intercorrelation across multiple **ethical considerations**, **including privacy**, **fairness**, and **transparency**. Those respondents who rated one ethical consideration highly were very likely to hold others in high regard, which further suggests CBDC development should take into account all, or at least most, ethical dimensions as intertwined and integral for making the technology work.

Another key finding is the predictability of the perceptions regarding the effectiveness of the

cybersecurity strategies. For instance, the perception for the effectiveness of one cybersecurity strategy, say encryption, has tended to closely relate to the way people rate other cybersecurity strategies. Therefore, this indicates a range of focused and comprehensive cybersecurity strategies that need to be adapted in order to ensure that CBDCs are founded on sound security frameworks.

Strong interrelations among perceived cybersecurity risks, such as data breaches, hacking, and unauthorized access, are also eminent in the analysis. All these risks will be perceived as interlinked; therefore, the urgency of elaboration of the cybersecurity frameworks which can face a broad range of threats simultaneously is underlined.

Most of the respondents consider that significant difficulties can be seen in trying to align CBDCs into the present regulatory framework. This is very closely associated with the need for updates in regulations rather urgently to meet the peculiar challenges that CBDCs are causing, for their safe and effective deployment. The views on the impact of CBDCs on traditional banking were divergent. Some of the respondents argued that the CBDC may drive a positive impact in the economy, whereas some think it will disrupt it negatively, reflecting the continued uncertainty over the broader economic implications of digital currencies.

Ethical issues on CBDC cybersecurity have always cropped up, and strong security balanced with user privacy and openness should be ensured. This flags the ethical complications that surround the CBDCs and how those issues should be watched out for with care.

The analysis can also suggest distinct groups of stakeholders with varying priorities. Some of the respondents are more concerned with privacy and supportive of encryption, while others are concerned more with fairness and access. This diversity needs to be taken into consideration when implementing CBDC.

Finally, the analysis underlines the fact that fitting the CBDC processes in line with international financial legislation is a complex and urgent matter, where global effort coordination is required. Secondly, as described by correspondent AML and related rules, effectiveness in applying existing CBDC systems is deemed quite sufficient to have large improvement potential.

These insights provide the comprehensive understanding of various interrelated issues involved in development, usage, and regulation related to CBDCs. Issues of ethics and regulations deployed, including cybersecurity concerns, form a vital part of deploying digital currencies successfully in a safe but efficient way.

4.4.3. Perceptions of CBDCs: General Trends

- ***Ethical Issues:***

The majority of the respondents identified the aspects of privacy, equity, and transparency as being essential ethical issues that must be considered in all the stages of crafting and launching CBDCs. Most of the participants considered these ethical aspects to be interconnected and mentioned that it is of importance to ensure that CBDCs are crafted in accordance with these values.

- ***Cybersecurity Concerns:***

Compliance issues relating to accommodating CBDCs in existing regulation were the major concern of the majority of the respondents. There was a widespread feeling that existing regulations were desperately in need of reform to accommodate the specific compliance issues that CBDCs pose.

- ***Regulatory Challenges:***

Compliance issues relating to accommodating CBDCs in existing regulation were the major concern of the majority of the respondents. There was a widespread feeling that existing regulations were desperately in need of reform to accommodate the specific compliance issues that CBDCs pose.

- ***Economic Impact:***

Perceptions regarding potential effects of CBDCs on the conventional banking business were varied, but there was greater concern for disruption rather than positive impact. This completes our journey through beliefs held by participants about the ecosystem as such. On to ethical matters in cybersecurity. Aside from that, an aspect that struck us was the ethical aspects of the large-scale security measures themselves. A balance between tight security policies and openness and user privacy has been identified as necessary; a rather complex ethical landscape around CBDCs, to say the least.

- ***Myriad Stakeholder Perspectives:***

It implies that various stakeholder groups with varying priorities are reacting. So, for instance, there are individuals with a high appreciation for privacy and thus support for encryption, while others have an interest in equity and usability and thus differing perspectives on what will be best in the future regarding CBDC implementations.

- ***Global Regulatory Alignment:***

Most of the participants viewed the alignment of operations for CBDC with international regulations of finance as the big challenge, and many thus recognized that implementation efforts had to be coordinated at the global level.

- ***Effectiveness in AML-CFT-CFP Compliance:***

Although the bar continues to move, the overall effectiveness of the existing CBDC systems in AML, combating the financing of terrorism, and combating the financing of proliferation was rated as moderate, indicating areas for further work.

These trends generally signal the level of complexity of perceptions about CBDCs, with strong emphasis on ethical considerations, cybersecurity concerns, regulatory challenges, and potential economic consequences. In this regard, stakeholders believe that a balanced and inclusive approach is key to full deployment in a secure manner.

4.4.4. Improving the adoption of CBDCs in UEMOA

Some specific ways in which CBDCs can be ethically implemented in the UEMOA and its adoption has a host of challenges and opportunities present themselves as taken from survey data by regional stakeholders. The analysis consolidates the pertinent findings into the themes of privacy, financial inclusion, issues of regulation, cybersecurity, and the greater economic implications brought about by CBDCs.

- ***Privacy and Data Protection:***

These answers mark it as one of the key variables that deserve extra heed being paid during their development and implementation phases for the CBDC. It will therefore, involve cybersecurity that is unbreakable using encryption and will implement strict policy related to handling personal data aimed at the creation of trust within the public masses as well as at preserving integrity of the CBDC system upheld.

- ***Financial Inclusion and Accessibility:***

This meant that CBDCs needed to be rolled out as far as possible to each and every citizen, especially in the most underdeveloped towns or areas. The structures for CBDC, according to the respondents, need to be all-inclusive and usable on all devices down to simple mobile phones. Digital literacy training was also proposed along with access to such technologies at an affordable cost in order not to widen financial inequalities.

- ***Regulatory and Governance Challenges:***

One of the major challenges of recent times involves CBDC inlay into a regulatory system, say within UEMOA. This necessitates an urgent need to further evolve and harmonize regulations in accordance with some of the features of digital currencies. In addition, CBDC governance transparency and accountability were seen as a requirement to attain public trust, and an answer to the call necessitates open communication on each step being undertaken, with greater public involvement in decision-making.

- ***Cybersecurity Concerns:***

The results showed high concern for data breaches and unauthorized access as part of the greatest CBDC cybersecurity concerns. Again, the respondents insisted on the overall security framework, including

frequent security audits, sophisticated encryption technologies, and privacy-enhancing strategies to mitigate risks.

- ***Economic Impact and Implementation Challenges:***

Economic Impact and Challenges in Implementation: Views were divided on the economic impact of CBDCs on conventionally set-up banks, with some hopeful it would bring in salutary effects while others were afraid it would cause disruption. There was an indication that the functioning of CBDCs will have to be so aligned as also to meet international norms on financial regulation and total compatibility with the existing systems-each of these being challenges when it comes to planning and implementation.

- ***Ethical Issues***

One of the key issues that cropped up with ethical overtones was the misuse of CBDCs, both by people and authorities. The panel felt a strong governance structure would be highly necessary for reduction in ethical risks and to have a CBDC system that was nondiscriminatory and transparent; equity-enhancing and exclusion-preventing policies would be needed.

- ***User Experience and Support:***

It was also concluded that ease-of-use interfaces held the secret to mass utilization of CBDCs. In the design of a CBDC system, it should be intuitive, accessible for all people with every level of digital literacy. Complementing that very importantly would be full customer service and support for end-users, which shall help them shift toward the usage of CBDCs and deal with obstacles or issues arising thereby.

The CBDC introduction in the UEMOA region will surely be driven by solid attention to privacy, security, inclusiveness, and transparency. The attention of these priorities through well-crafted regulatory frameworks, robust cybersecurity measures, and widespread education programs would go a long way to have the CBDCs positively contributing toward financial inclusions and economic stability across the region.

4.4.5. Regional Variations in Survey Responses

The responses contain expert opinions, some from UEMOA and some from outside UEMOA. This will be of great value in comparing the data from the different regions easily. The comparison is done strictly to reflect factually what was obtained from the survey data, without speculative expressions:

- ***Protection of Personal Data***

- **UEMOA:** For the participants in the UEMOA region, privacy and data protection should be at the heart of the development and implementation of CBDC. The cybersecurity to be deployed to safeguard users' data is rigid, thus commanding trust in the CBDC ecosystem with the use of

encryption technologies and robust mechanisms of authentication.

- **Outside UEMOA:** In more developed regions, also, survey data places privacy amongst the top concerns, with a number of the responses referring to comply with stringent data protection legislation. But in UEMOA, no doubt, the reasons for privacy measures are identified more with establishing preliminary levels of trust as the general levels of digital literacy and levels of trust in the digital financial system are lower.

- *Financial Inclusion and Accessibility*

- **UEMOA:** From the responses obtained in the survey, financial inclusion is a significant issue in the region of UEMOA. In this respect, responses have been emphasized to ensure that CBDCs become accessible to all citizens, particularly underserved or rural areas. In fact, one finds a strong appeal toward the operability and accessibility of the CBDC platforms on modest, lower-technology devices.
- **Outside UEMOA:** In comparison, responses from the rest of the world, such as Southeast Asia, indicate that though financial inclusion is relevant, there is more concern about the integration of CBDCs with the existing mobile money platforms already in use for financial inclusion. For UEMOA respondents, however, there should be a conquest of the digital divide through literacy programs and affordable access to technology.

- *Regulatory and Governance Challenges*

- **UEMOA:** For UEMOA, the main challenge reported in most of the responding countries was how to fit the CBDCs into the existing regulatory regimes. Concretely, developing regulations is necessary to account for the unique characteristics of digital currencies and to harmonize these across the member states.
- **Outside UEMOA:** In other regions, the survey data indicates that regulatory challenges are similarly significant, but the focus is slightly different. For instance, in Europe and North America, the challenges faced have to do with aligning CBDCs with complex and well-established financial regulatory systems, while UEMOA respondents point to foundational development that is needed at the level of regulation.

- *Regulatory and Governance Challenges*

- **UEMOA:** In the UEMOA region, significant cybersecurity threats were pointed out by respondents. These risks include data breach and unauthorized access. According to the results of this survey, this has become a critical priority for establishing a full cybersecurity framework that encompasses regular security audits and advanced encryption technologies.
- **Outside UEMOA:** Beyond this region, those mature in digital infrastructure consider cybersecurity a significant concern but are more focused on sustaining a high level of standards within an already established cybersecurity environment. However, UEMOA members mark this

to be more urgent in nature as it pertains to developing those capabilities in the first place.

- ***Economic Impact and Adoption Challenges***

- **UEMOA:** In the UEMOA region, the majority of surveyed respondents had mixed feelings about the probable CBDC consequence on the level of the economy as a whole. While others were optimistic, there were those who speculated that disruption would be caused to the conventional banking fraternity. There is a high level of concern about how CBDC operations are aligned with international financial regulations.
- **Outside UEMOA:** In more advanced economies, the economic concerns regarding CBDCs typically involve bank disintermediation and monetary policy effectiveness. UEMOA respondents are more concerned with how CBDCs could be designed in a manner that does not exacerbate the fragility of the financial sector.

- ***Public Confidence and Ethics***

- **UEMOA:** The answers that come from the UEMOA region highlight trust in the CBDC system. In their opinion, trustworthy governance needs to be transparent, whereas ethical frameworks must be sound enough to prevent misuse of the system. Fairness and prevention of ex-post exclusion are among other main ethical issues highlighted by the UEMOA country respondents.
- **Outside UEMOA:** Other regions seem to face similar trust issues; these issues may be somewhat different in origin, however-sourced more strongly in varying levels of trust in governmental institutions or concerns about surveillance, for example. Transparency and moral governance are basic building blocks of trust in UEMOA.

While some challenges at CBDC adoption-such as issues on privacy and cybersecurity-are shared across regions, survey data illustrates particular challenges the UEMOA region faces in areas of financial inclusion, regulatory integration, and public trust. Solutions to these challenges will require approaches that are unique and tailored to the needs and concerns of UEMOA stakeholders.

4.4.6. Survey Findings

We have used Microsoft Excel to analyze the survey data as Excel equips us to understand our data by using natural language queries without writing complicated formulas. Besides, it provides high-level visual summaries, trends, and patterns. The data is very precious and of high quality since it was received from professionals and experts: 65% had a master's or Ph.D. degree, and 45% of the respondents were professionals or played related roles in the realm of CBDC. We analyzed through questionnaires the respondents' attitude, view, and cognition towards CBDC and deduced the demand for CBDC from the

public;

The results indicate a strong consensus among participants that ethical dimensions across privacy, fairness, and transparency should be considered while developing and implementing the functioning of CBDCs.

i. Ethical and Social Considerations

- Key Ethical Considerations

User Privacy and Data Protection: Has emerged as the most important ethical concern for **73.47%** of the total respondents.

Fair and Equitable Access: This translates to **62.24%** of participants regarding Fair and Equitable Access to be an essential requirement, highlighting that CBDC systems should be inclusive.

Transparency and Accountability: The percentages of respondents who believe that transparency and accountability are crucial elements in governance is **65.31%**. This implies the construction of confidence and oversight.

Minimizing Potential for Misuse: Another key consideration is the need to reduce potential misuse as **45.41%** of the respondent's express concern regarding the strong guards against illegal activities.

Priority	*Score*	*%*	*Key Insight*
User Privacy and Data Protection	144	73.47%	Ensuring the protection of personal data and privacy is essential.
Fair and Equitable Access for All Citizens	122	62.24%	Ensuring everyone has access to CBDCs without exclusion.
Transparency and Accountability in CBDC Governance	128	65.31%	Clear and accountable management of CBDCs is crucial.
Minimizing Potential for Misuse by Individuals or Authorities	89	45.41%	Mechanisms to prevent misuse of CBDCs are important.

Table 9: Key Ethical Considerations

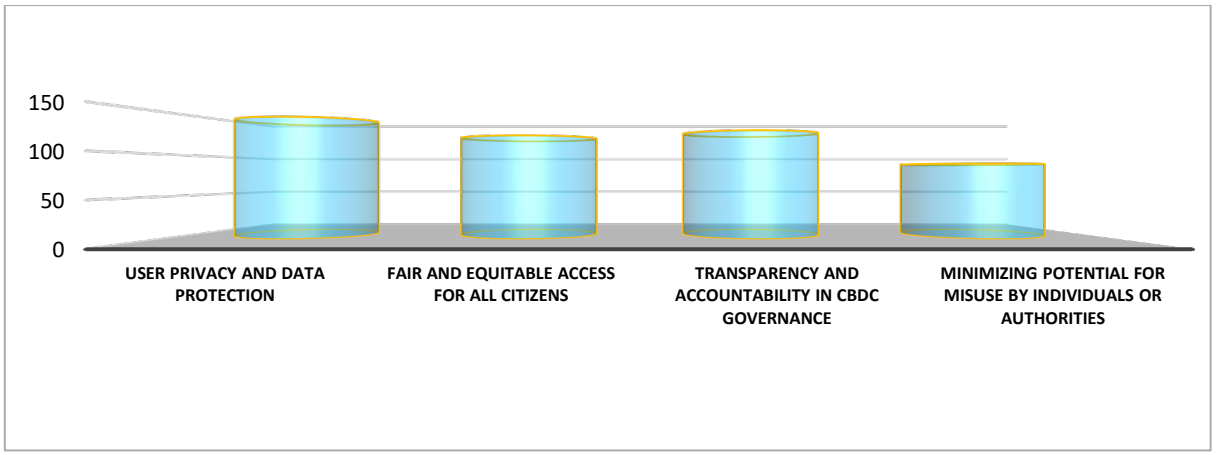


Figure 21: Ethical Considerations

- ***Opinions on the Ethical Implementation of CBDCs***

The majority proportion, **62.37%,** viewed that CBDC can be introduced in an ethical manner; 7.22% commented that it would not be possible for CBDC implementation to be carried out ethically.

Level of Agreement	%
Agree	*40.21%*
Strongly Agree	*22.16%*
Neutral	*30.41%*
Disagree	*5.16%*
Strongly Disagree	*2.06%*

Table 10: Opinions on the Ethical Implementation of CBDCs

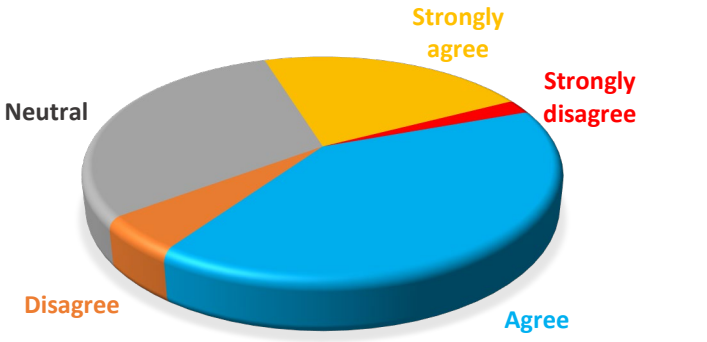


Figure 22: Opinions on the Ethical Implementation of CBDCs

- ***Effectiveness of Strategies to Mitigate Inequality and the Digital Divide***

45.36% believe this would be moderately effective in not allowing the CBDCs to widen the financial inequality or a digital divide if free or subsidized internet access was provided.

Strategy Effectiveness	% Respondents
Not Effective	***8.76%***
Somewhat Effective	***14.43%***
Moderately Effective	***31.44%***
Effective	***31.96%***
Highly Effective	***13.40%***

Table 11: Effectiveness of Strategies to Mitigate Inequality and the Digital Divide

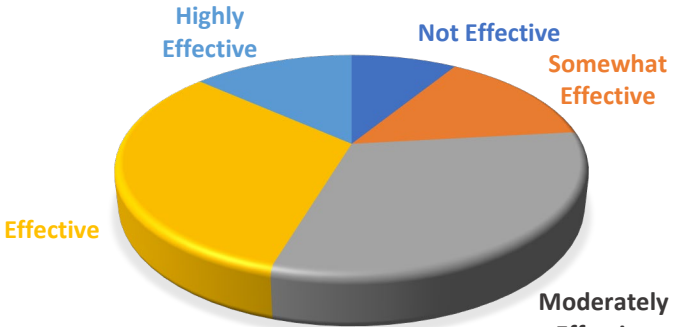


Figure 23: Effectiveness of Strategies to Mitigate Inequality and the Digital Divide

A participant contributed some important details be

To ensure that CBDCs do not exacerbate financial inequality or the digital divide, banks should (translation from French):

1) **Facilitate access:** Offer accessible CBDC accounts to the unbanked and solutions to those without stable internet access.
2) **Educate:** Offer programs to familiarize all customers with CBDCs, with a particular focus on vulnerable groups.
3) **Ensure accessibility:** Make CBDC platforms easy to use for a diverse population, including older adults and people with disabilities.
4) **Collaborate:** Work with diverse partners to expand access and adoption of CBDCs.
5) **Develop offline solutions:** Allow CBDCs to be used without internet to include users in remote areas.

6) **Listen and adapt:** Collect user feedback to continually improve CBDC offerings in an inclusive manner.

These actions can help minimize the potential negative impact of CBDCs on financial inequality and the digital divide.

- ***Digital Literacy Programs for CBDC Adaptation***

47.43% of the respondents consider that the digital literacy programs are effective and highly effective, which thus helps customers better adapt to CBDC technology, while 34.54% find the solution Moderately Effective.

Strategy Effectiveness	*%*
Not Effective	2.06%
Somewhat Effective	15.98%
Moderately Effective	34.54%
Effective	29.90%
Highly Effective	17.53%

Table 12: Digital Literacy Programs for CBDC Adaptation

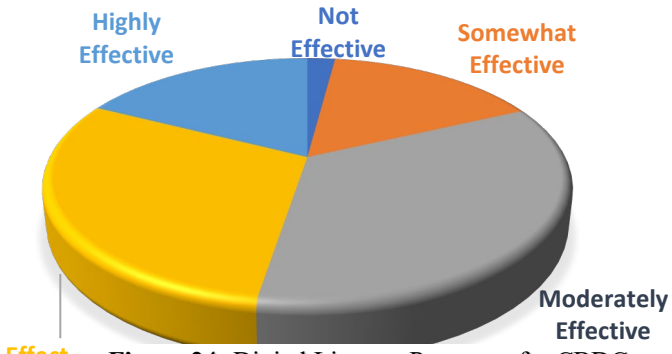


Figure 24: Digital Literacy Programs for CBDC Adaptation

ii. *Accessibility, Usability, and Privacy*

- ***Tiered Access to CBDC Services***

The majority of the respondents, 53%, considered tiered access to the services of CBDCs effective and highly effective in ensuring equal access.

Strategy Effectiveness	*%*
Not Effective	3.08%
Somewhat Effective	11.79%
Moderately Effective	35.90%
Effective	38.46%
Highly Effective	10.26%

Table 13: Accessibility, Usability, and Privacy

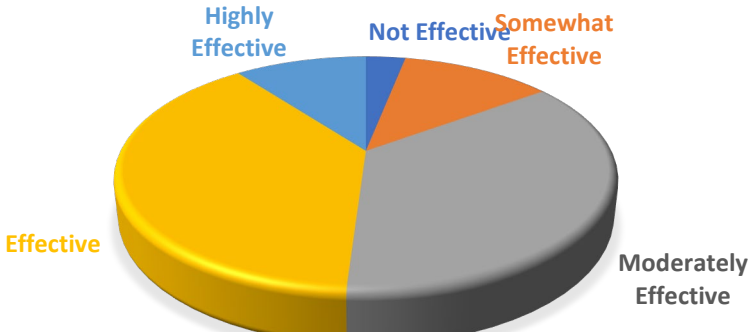
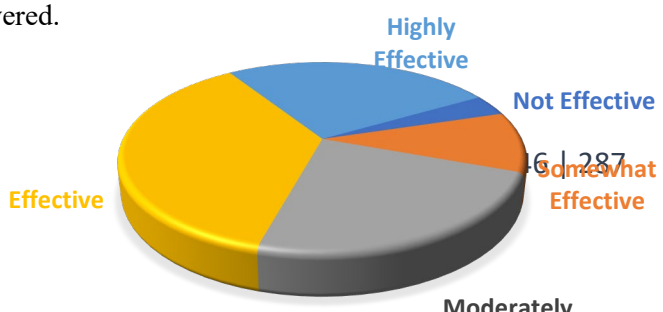


Figure 25: Accessibility, Usability, and Privacy

- ***Accessible Customer Support for CBDCs***

65% consider widely available and accessible customer support services as an effective or very effective means of having questions about CBDCs answered.



Strategy Effectiveness	%
Not Effective	3.59%
Somewhat Effective	10.26%
Moderately Effective	23.59%
Effective	36.41%
Highly Effective	25.64%

Table 14: Accessible Customer Support for CBDCs

Figure 26: Accessible Customer Support for CBDCs

- ***User-Friendly Interfaces***

59.28% of the total respondents find making easy-to-use and accessible interfaces to be very or effective.

Strategy Effectiveness	%
Not Effective	4.12%
Somewhat Effective	8.76%
Moderately Effective	27.84%
Effective	31.44%
Highly Effective	27.84%

Table 15: User-Friendly Interfaces

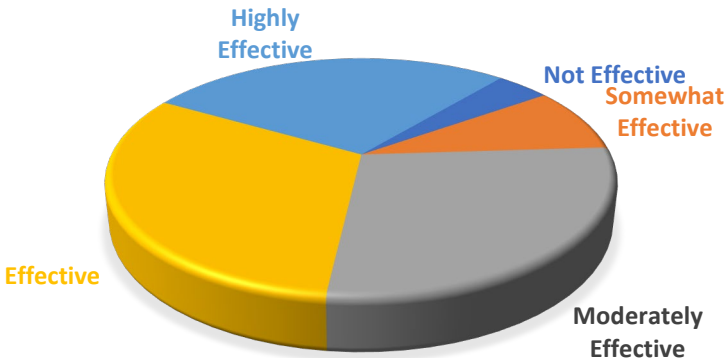


Figure 27: User-Friendly Interfaces

- ***Importance of Privacy, Financial Inclusivity, and Fraud Prevention in CBDCs***

User Privacy and Data Protection

- **Key observation:** An astonishing fact is that the majority of them, 61.86%, view this trait as very important (24.23%) or of great importance (37.63%). Only a negligible minority, i.e., 6.19%, consider this aspect as unimportant.

One of the interview participants, Dr Sissoko integrated critical ethical considerations in CBDC design, implementation, and operation encompass privacy and data security, financial inclusion of all citizens, protection against cyber threats, interoperability with other currencies and payment systems, fairness of algorithms, environmental sustainability minimization, financial stability preservation, respect for national sovereignty, and the requirement for user education and awareness. Prioritizing these aspects will help develop CBDCs that are fair, secure, and beneficial to society.

- **Trend:** privacy and protection from data breaches are part of primary concern; consequently, it is expected that a great part of the respondents surely supports strong measures in safeguarding CBDC design.

Promoting Financial Inclusivity and Accessibility

- **Key Observations:** In this category, responses are more dispersed, and Important is the most

frequent level of importance rating at **31.44%**, followed by Moderately Important at **30.41%**. Remarkably, **23.71%** rated this as Extremely Important. And finally, **14.43%** ranked this category as less important (Not Important: **1.03%,** Slightly Important: **13.40%**)

- **Trend:** Given that consideration of inclusivity is a big factor-but not quite as urgent as privacy-there is a wide-ranging agreement on its importance, but fewer respondents rate it "Extremely Important" compared to privacy.

Preventing Misuse and Fraud

- **Key Observations:** In this category, **39.69%** of the responses are in the Extremely Important category. An incredibly minuscule **1.03%** come out as seeing it as Not Important-an almost unanimous view of its importance.
- **Trend:** Preventing fraud is an issue close to the hearts of the respondents, with almost half considering it to be extremely important. This validates the growing concern about the potential misuses and fraud with digital currencies, especially given the nature of the decentralized systems.

Maintaining Transparency in Transactions and Governance

- **Key Observations: 35.57%** rate transparency as Extremely Important, while almost the same rate of **35.05%** assigned of their opinion to Important. Very few consider it to be only Moderately Important or less.
- **Trend:** Similar to the rankings of privacy and fraud prevention, transparency has received a very high ranking; many seem to view this as a keystone in an ethical CBDC implementation. This should tend to indicate that people place considerable emphasis on visibility and, through that transparency, accountability in digital currency systems.

Upholding User Autonomy and Control over Personal Financial Data

- **Key observation:** Once more, the two highest importance levels, Extremely Important and Important, dominant here at **36.08%** and **30.41%,** respectively, while there is little support for lower importance ratings.
- **Trend:** User autonomy is considered a very vital ethical dimension, congruent with considerations about privacy. Persons would most likely be concerned with how much control they can retain over their personal financial data within a CBDC framework.

	Not Important	*Slightly Important*	*Moderately Important*	*Important*	*Extremely Important*
User Privacy and Data Protection	6.19%	9.79%	22.16%	24.23%	37.63%
Promoting Financial Inclusivity and Accessibility	1.03%	13.40%	30.41%	31.44%	23.71%
Preventing Misuse and Fraud	1.03%	11.86%	26.29%	21.13%	39.69%

Transparency in Transactions and Governance	2.58%	8.76%	18.04%	35.05%	35.57%
Autonomy and Control over Personal Financial Data	1.55%	10.82%	21.13%	30.41%	36.08%

Table 16: Importance of Privacy, Financial Inclusivity, and Fraud Prevention in CBDCs

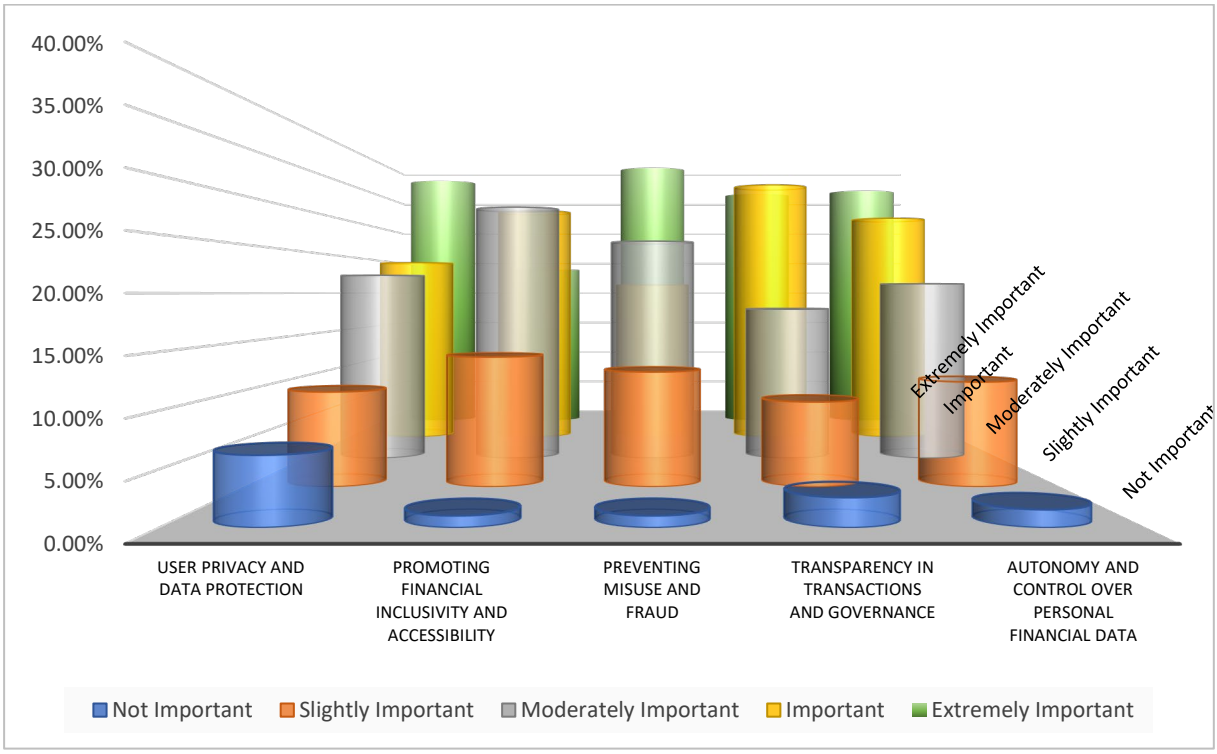


Figure 28: Importance of Privacy, Financial Inclusivity, and Fraud Prevention in CBDCs

- ***Challenges of CBDC systems in terms of AML-CFT-CFP regulation***

The majority of the respondents feel that challenges related to integrating the CBDCs with regulations are perceived to be moderate to significant at **79.48%,** while the need for updating these regulations is urgent at **83.00%**. Similarly, **68.91%** perceived that aligning the CBDC operations with international regulations is difficult.

	Aligning CBDC with International Regulations					***Integrating the CBDCs with Regulations***					***Updating These Regu***		
Category	**Not difficult**	**Slightly difficult**	**Moderately difficult**	**Difficult**	**Extremely difficult**	**No Challenge**	**Minor Challenge**	**Moderate Challenge**	**Major Challenge**	**Significant Challenge**	**Not Urgent**	**Low Urgency**	**Moderat Urgenc**
%	4.15%	26.94%	40.93%	24.87%	3.11%	4.62%	15.38%	41.54%	22.56%	15.38%	5.15%	11.86%	31.96

Table 17: Challenges of CBDC systems in terms of AML-CFT-CFP regulation - 1

Regarding the economic impact, **78.35%** of the interviewees believe that CBDCs would have a neutral to very positive effect on the traditional banking sector. As for AML regulation conformity, **76.80%**

find it to be from moderate to very effective, though only **23.20%** considered it not effective, which is evidence that there is still room for improvement.

	Economic Impact of Implementing CBDCs					Effectiveness of CBDC Systems in Meeting AML-CFT-CFP				
Category	Very negative	Somewhat negative	Neutral	Somewhat positive	Very positive	Not effective	Slightly effective	Moderately effective	Effective	Highly effective
%	4.12%	17.53%	42.78%	23.71%	11.86%	4.64%	18.56%	50.00%	22.68%	4.12%

Table 18: Challenges of CBDC systems in terms of AML-CFT-CFP regulation - 2

Category	Significance	Summary
Challenges in Integrating CBDCs with Current Regulations	79.48%	Nearly half (37.94%) of respondents perceive integrating CBDCs with existing regulations as a considerable or significant challenge.
Urgency in Evolving Regulations	82.99%	The majority (51.03%) believe there is a considerable or extreme urgency in evolving regulations to address CBDC compliance challenges.
Difficulty in Aligning CBDC Operations with International Regulations	69.00%	A significant portion of respondents (28%) view aligning CBDC operations with international regulations as difficult to extremely difficult.
Economic Impact of Implementing CBDCs on the Traditional Banking Sector	78.35%	A slight majority (35.57%) of respondents view the economic impact of CBDCs on the traditional banking sector as somewhat or very positive.
Effectiveness of CBDC Systems in Meeting AML-CFT-CFP Regulations	76.80%	The majority (26.80%) find current CBDC systems effective in meeting AML-CFT-CFP regulations, but only 4.12% consider them effective or highly effective.

Table 19: Summary of challenges of CBDC systems in terms of AML-CFT-CFP regulation

iii. Cybersecurity Challenges with CBDC

The following survey data depicts how the respondents perceive the importance of cybersecurity risks related to CBDCs. Below is an in-depth analysis of the risk categories identified and their importance by ratings applied by participants in the survey.

- ***Ethical Challenges***

A substantial 90.21% (175 out of 194 participants) reported no ethical challenges related to CBDC cybersecurity in their work. This reflects that either robust policies or negligible exposure to the ethical dilemma in question has reduced such apprehensions among a majority of professionals.

However, 9.79% (19 respondents) did bring up important issues, which include:

Privacy concerns: Safekeeping of personal information and unauthorized access are still crucial challenges.

Operational barriers: Digital signature barriers, 3D password operations, and verification processes hamper user experience.

Fraud and threats: Spams, identity theft, and fraud in mobile banking, more specifically in Mali, indicate that there is some localized vulnerability.

Each of these issues underlines demands for strong data protection, friendlier technologies, and region-specific solutions that may make CBDC ethical.

- ***Data Breaches***

The critical problem with data breaches named the highest percentage of respondents. In particular, 63 respondents (32.64%) scored this risk as "Extremely Significant," while 51 (26.42%) considered it of "Major Significance". Together, 59.06% of respondents cast data breaches as a critical risk to CBDCs. However, 22.28% assigned "Moderate Significance" to this risk, indicating that although it is a concern, it is not always viewed as the most pressing issue. Only 7.25% of respondents described data breaches as "Not Significant". That would suggest that there is an overall acknowledgment of the risks that data breaches could present, in particular, because CBDC systems would involve highly sensitive and large financial and personal data.

- ***Identity Theft***

Ranking second amongst high-priority cybersecurity threats was identity theft, for which 72 respondents viewed as "Extremely Significant" (37.70%) and 42 respondents (21.99%) who rated it to be of "Major Significance". That brings up to nearly 60% of respondents that hold identity theft to be an area of significant priority. A large share of respondents (28.27%) also marked "Moderate Significance" to this risk, meaning that although identity theft is commonly understood as important, to some participants, it seems to be somewhat less serious in comparison with other risks. Only 2.09% considered the risk of identity theft as "Not Significant". Such findings call for strong mechanisms in CBDC systems for identity verification and protection against possible fraudulent use of personal information.

- ***Transaction Manipulation***

The risk of transaction manipulation was also pointed out as being of top priority. 60, or 31.25%, of the respondents rated it as "Extremely Significant," and 55, or 28.65%, rated it as having "Major Significance". Together, 59.90% of respondents consider this issue to be of high importance. Another 27.08% assigned "Moderate Significance" to this risk, indicating that while it is considered serious, it may not be the most critical cybersecurity threat. A marginal 1.56% rated transaction manipulation as "Not Significant," meaning virtually all respondents consider ensuring that CBDC system transactions are secure and not subject to tampering is of utmost importance. This strengthens the argument toward advanced encryption, enhanced monitoring of transactions, and systems designed to be impossible to manipulate so as to protect trust and transparency.

- ***System Vulnerabilities***

System weaknesses and their critiques through the survey method were determined as one of the top risk ratings. 54 participants accounting for 28.57% chose this risk category as "Extremely Significant" followed by 67 participants, which is 35.45% who marked it as having a "Major Significance" Towards Total. So, the total percentage of those who regard system vulnerabilities as highly significant is 64.02%. A further 25.40% labeled it as having "Moderate Significance," while only 2.12% ranked it as "Not Significant". The results reveal a widespread concern over vulnerabilities in the CBDC systems, which could encompass programming errors, outdated software, or lack of security features. These system weaknesses need to be fixed in order to guarantee the integrity, dependability, and robustness of the CBDC platforms.

- ***Unauthorized Access to Data***

Data breaches have the highest use as a risk in the area of cybersecurity, unsupported by 73 respondents assigning "Extremely Significant" to it 38.02% and 51 respondents marking "Major Significance" to this issue26.56%. Together, 64.58% of respondents believe that unauthorized access to data is of high concern a ranking that gives this risk factor the highest urgency level across all the risk categories surveyed. Another 23.44% assessed the level of this risk to be of "Moderate Significance," whereas 1.04% felt this was "Not Significant". Results show that rigid access controls and authentication protocols in CBDC systems should be imposed to prevent rogue agents from leveraging sensitive financial information.

These results really denote great confidence in these measures as far as cybersecurity is concerned, but they bring into sharp focus utter concerns about probable system vulnerabilities and the security of data.

	Data breaches	Identity theft	Transaction manipulation	System vulnerabilities	Unauthorized access to data
Not Significant	7.25%	2.09%	1.56%	2.12%	1.04%
Minor Significance	11.40%	9.95%	11.46%	8.47%	10.94%
Moderate Significance	22.28%	28.27%	27.08%	25.40%	23.44%
Major Significance	26.42%	21.99%	28.65%	35.45%	26.56%
Extremely Significant	32.64%	37.70%	31.25%	28.57%	38.02%

Table 20: Cybersecurity Challenges with CBDC

iv. *Effectiveness of Security Measures in CBDC Systems*

- ***Encryption Technologies***

It is assumed that encryption technologies fall under CBDC cybersecurity. In fact, the majority of respondents, 58.64%, considered encryption use to be "Highly Effective" at 26.70% or "Very Effective"

at 31.94%. This would entice a great level of confidence in the deployment of encryption as an effective security measure. Further, 27.75% found encryption "Somewhat Effective," which again means while effective, there is room for improvement in its implementation or application. Of those, a further 9.42% thought encryption was only "Slightly Effective," and just 4.19% saw it as "Not Effective". This is a reminder that there should be an ongoing development of better methods of encryption to earn the public's trust and meet new challenges to cybersecurity.

- ***Strong Authentication Mechanisms***

Respondents also scored strong authentication mechanisms multi-factor and biometric verification highly. Combined, 61.46% of respondents ranked these either "Highly Effective" (31.77%) or "Very Effective" (29.69%). Another 26.04% found these mechanisms "Somewhat Effective," meaning they work well but could be optimized further. A smaller proportion, at 11.98%, considered them "Slightly Effective," while only 0.52% rated them as "Not Effective". These results point out that robust authentication is a trusted measure for ensuring secure access to CBDC systems, although continuous refinement is vital to address any residual doubts.

- ***Continuous Monitoring Systems***

The continuous monitoring systems, which track system activities in real time in order to identify and mitigate threats, had overwhelming approval from the respondents: 56.25% rated them as either "Highly Effective" (25.52%) or "Very Effective" (30.73%). In addition, 32.29% viewed them as "Somewhat Effective," which represents a moderate degree of trust in their ability to manage risks. Only 11.46% found them to be "Slightly Effective," and no one ranked them as "Not Effective". From the results, the critical aspect in the observation of security was the continuous monitoring; at the same time, the improvement in the threat detection and response may make them effective.

- ***Regular Security Audits***

Regular security audits are among those highly rated as a security measure which involves systematic reviews of system vulnerabilities and compliance. A significant 61.78% rated them as either "Highly Effective" at 26.18% or "Very Effective" at 35.60%, indicative of great confidence in being able to both spot and mitigate risk. Another 27.23% considered them "Somewhat Effective," and that reflects that even though people trust them, improvements can still be made. 9.95% considered audits "Slightly Effective," and a mere 1.05% considered them "Not Effective". The report reflects that security audits must regularly occur in order to maintain CBDC systems secure and reliable.

- ***Privacy-Enhancing Technologies***

The technology that protects private information and complies with privacy regulations received a lot of approval. 62.30% rated them "Highly Effective" (29.84%) and "Very Effective" (32.46%). 26.18% considered them "Somewhat Effective," with a considerable level of confidence in them. Smaller proportions, 8.90% and 2.62%, rated them as "Slightly Effective" and "Not Effective," respectively.

These results clearly bring into light the huge importance of the role that privacy-enhancing technologies play in dealing with data protection and trust-building across CBDC systems.

	Encryption technologies	Robust authentication mechanisms	Continuous monitoring systems	Regular security audits	Privacy-enhancing technologies
Not Effective	4.19%	0.52%	0.00%	1.05%	2.62%
Slightly Effective	9.42%	11.98%	11.46%	9.95%	8.90%
Somewhat Effective	27.75%	26.04%	32.29%	27.23%	26.18%
Very Effective	31.94%	29.69%	30.73%	35.60%	32.46%
Highly Effective	26.70%	31.77%	25.52%	26.18%	29.84%

Table 21: Effectiveness of Security Measures in CBDC Systems

4.4.7. Summary and Conclusion of Survey Results

The results from the survey show that the development and implementation of CBDCs have to be based on ethical consideration. Some of the big ethical issues that have been recognized by respondents include user privacy, data protection, fairness, and transparency; as many as 95% of the participants insisted on the dire need for strong privacy measures in protecting sensitive financial information. Also, transparency in governance was another area well placed in focus 80% stated this would help gain the trust of users. Additionally, 86% emphasized equal access because CBDC systems should be inclusive to avoid the marginalization of some sections of society.

The survey shows optimism in the ethical implementation of CBDCs with 65.6% in agreement that ethical principles can be upheld. Concerns around fraud prevention, misuse, and cybersecurity risks still persist. System vulnerabilities were pointed out by 87% of the respondents, followed closely by unauthorized access to data at 85%. These results show that advanced security measures such as encryption, strong authentication mechanisms, and monitoring systems are necessary. More than 85% of the respondents found these technologies effective, but the lingering feeling of vulnerability suggests there is room for improvement.

Among several, one more significant question also regulatory concern issue: about 80% stated that aligning CBDC with existing regulations has shown pretty high challenges in general. And then, many noted with urgency the updates of regulatory frameworks to deal specifically with unique digital currency risks around AMM/CFT topics. The systems put into place were considered to meet the requirements of AML/CFT standards, hence developing deeper fraud prevention-misuse, taking into consideration different ideas as suggestions.

The survey also aimed to identify ways in which financial inequality and the digital divide could be reduced. Among the measures suggested by respondents were subsidized internet access, accessible

CBDC accounts for the unbanked, and educating users about digital currency systems. The study has established that tiered access to CBDC services and ease of use were effective strategies in improving accessibility. In the context of cybersecurity, the most highly rated technologies have been privacy-enhancing technologies and regular security audits; more than 60% of the respondents found them to be highly effective in mitigating risks such as identity theft, manipulation of transactions, and data breaches.

These challenges notwithstanding, the results of this survey illustrate the possible positive economic impact of CBDCs. About 78% of the respondents answered that CBDCs would have a very positive to neutral effect on the traditional banking sector. Emphasis on privacy, transparency, and inclusiveness underlines commitment toward the development of ethical CBDCs, in line with values of society and regulatory requirements.

The survey hence gives a balanced view of the promise and challenges from the implementation of CBDC. While there is confidence in current technological and regulatory frameworks, much effort will have to be made to address the continuing vulnerabilities of security, improve regulatory alignment, and ensure ethical considerations remain at the heart of CBDC development. Such findings should provide a roadmap for enhancements in the future and would assure continued innovation and collaboration on the part of stakeholders in their quest to build secure and inclusive digital currency ecosystems.

4.5. Secondary Data Analysis

Material for this thesis will be retrieved from official records, physical and digital files, and computer-based records. One of the highly appropriate approaches in this research to collecting secondary data is a comprehensive document and record review method. Data for this thesis came from painstaking compilation through the exhaustive review of the following key sources:

- **Academic Journals:** These provide peered-reviewed insights and analysis relevant to the implementation of CBDCs.
- **Government and Regulatory Publications:** Offering valuable perspectives from official regulatory bodies, laws, and compliance frameworks regarding CBDC implementation.
- **Online Databases:** Accessing real-time data and records from CBDC trackers, international monetary bodies, and central banks.

Document and record review is, therefore, justified for a number of critical reasons. First of all, this approach allows the researcher to collect numerous, deep, and multi-faceted datasets that would not require direct interviews or interaction with any individual, which in itself makes this approach highly reliable and effective. The already existing data means that big volumes of information could be

elaborated without posing any burden on third parties or respondents.

This method has the added advantage of economy, since the data would have already been compiled in public and institutional records. This makes it particularly practical for research whose topic coverage is wide-ranging and complex, as in the implementation, regulation, and compliance frameworks of the CBDCs.

Thirdly, the inclusion of historical and comparative data provides in-depth analysis, where trends and patterns formed over time can let a study of the changes in the landscape of digital currencies be done. Moreover, the fact that this approach introduces only minimal bias truly strengthens the credibility of the research findings.

Lastly, reliance on CBDC databases and trackers will ensure access to a set of data that is accurate and in real time-something quite paramount in analysing the current state and future projections of CBDC adoption and its consequent effects on monetary systems and financial stability. This approach forms a strong foundation for the in-depth analysis undertaken in the remaining chapters of this thesis.

4.5.1. Academic Journals

For this purpose, an extended and exhaustive research has been carried out using the enriched resources available to us from our university library. Selinus University puts at its students' fingertips a very valuable collection of research materials. In fact, the Uniselinus Online Library represents a very remarkable collection of 108 million of High-Quality Records, over 29,000 e-books, dozens of subject-specific databases, and more than 15.9 million full-text and full-image articles. It acts as an open-access platform that may help students and researchers be informed of recent developments and trends in their respective fields.

Aside from using the available resources from the university, we extended our research to scan more than 100 academic publication pages from various global research portals. Our approach was highly selective to ensure that only the top academic works were included in our study, so that the best and most credible materials could be provided on how CBDCs are implemented in compliance with relevant requirements. A total of 44 academic research journals were cautiously analysed and yielded an in-depth analysis that matched and supported our findings from the surveys.

This study focuses on the following key themes: Monetary Policy and Economic Impact, Ethical Considerations and User Privacy, Challenges in Cybersecurity, and the needed Regulatory and Legal Frameworks required for successful implementation of CBDCs. The following chapters discuss these studies in greater detail, as their respective key themes are analysed and discussed. The list of all the

academic papers reviewed is contained at the end of the document, on the "Table of Literature Provided by Interviewees".

4.5.2. Government and Regulatory Publications

The next section summarizes a selection of governmental and regulatory publications that put a special mark on findings about regulatory frameworks, policy considerations, and macroeconomic implications with respect to the CBDCs and e-money. World regulatory portals were screened, and nine key regulatory documents from this study were reviewed. In particular, for most of the elements under discussion in the present paper, such as compliance, AML, CFT, and CPF, considering regulatory safeguards is the appropriate means to keep such risks in CBDC under control.

Ethical discussions also touched on privacy and data protection, which were put on the line to ensure the usage of financial data is very transparent and accountable. Furthermore, cybersecurity was taken as one of the focal points because "the security of the CBDC system" is paramount in preventing cyber threats and keeping stability in financial systems.

These themes are discussed in the following chapters in more detail, considering the emphasis given to compliance, AML/CFT/CPF, ethical issues, and cybersecurity challenges within the context of the implementation of CBDCs. The final listing of the Government and Regulatory Publications reviewed are also listed at the end of the document, on the "Table of Literature Provided by Interviewees".

4.5.3. Online Databases:

This section will review two of the most important online databases for the review of the global landscape with respect to CBDCs. Both of these two databases are in real time, updated continuously and tracking status and developments on projects related to the CBDC in different countries due to their deep insight into the progress of its implementation across the world.

World CBDC Tracker (cbdctracker.org)

The World CBDC Tracker puts into perspective the present state of play on CBDCs across the world. It categorizes countries in their stages of development, including:

Cancelled: Countries that have taken down or canceled their projects related to CBDCs. Research: Countries that have just begun doing preliminary exploratory research on CBDC. Proof of Concept: Countries at an advanced stage of research and published a proof of concept on CBDCs.

Pilot: Countries testing a CBDC in real-world conditions, either on a small or larger scale. Launched: Countries that have fully launched a CBDC for public use.

CBDC Tracker by Atlantic Council (atlanticcouncil.org/cbdctracker/):

The CBDC Tracker is an interactive database that, on behalf of the Atlantic Council, tracks the rapid developments around CBDCs, mainly in large markets. It currently tracks over 130 CBDCs in development and provides insight into how digital currencies are shaping the future of money on a global scale. This tracker covers each country's CBDC project in its various stages-from research to full implementation.

These databases have been instrumental in this study and results analysis are presented on the next chapter. These data provided updated information on various CBDC initiatives and the status of such initiatives, which has helped in an in-depth analysis of how different regulatory environments and economic contexts influence the issuance of CBDCs.

4.6. Finding and Results

Secondary data analysis carried out in this research was highly useful for extracting information with regard to regulatory mechanisms, policy aspects, ethical dimensions, and economic consequences of the introduction of CBDCs. The deliberative search of academic journals, government and regulatory publications, and online databases thus formed a very strong backbone for understanding complex challenges and opportunities that CBDCs are likely to pose in term of ethic, compliance with different regulatory texts and cybersecurity.

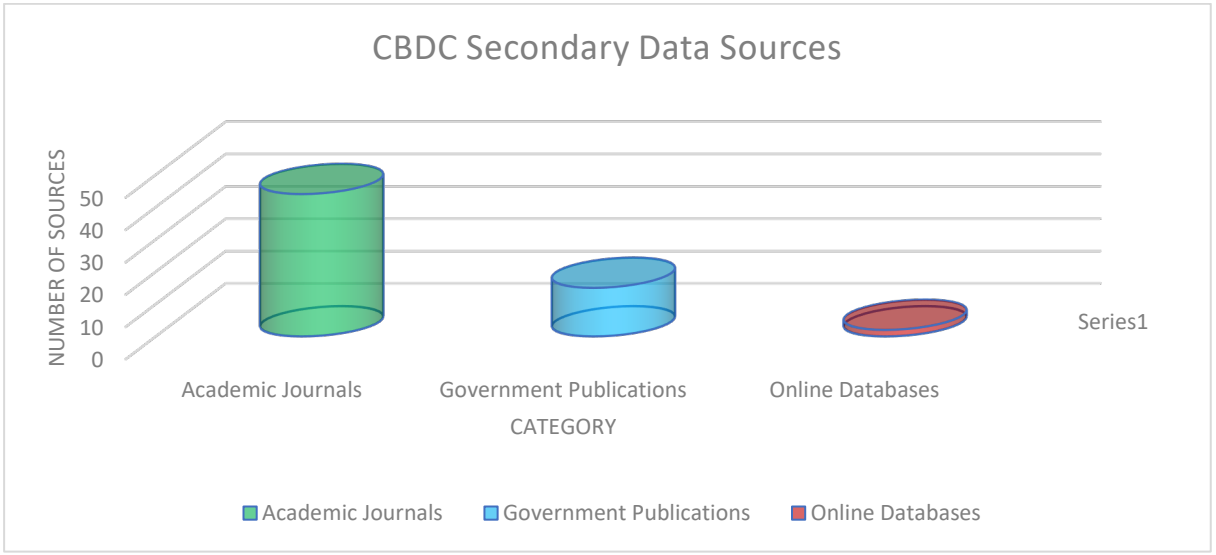


Figure 29: CBDC Secondary Data Sources

This review indeed provides light from **44 academic journals** on basic, core, monetary policy issues and their effect on the economy, ethical concerns regarding user-privacy, cybersecurity issues, regulatory framework, and necessary legislation in support of CBDCs. These sources helped validate

the results from our primary surveys and also provided a conceptual basis for considering discussions on wider ramifications of the uses of CBDCs.

Government and regulatory publications underlined considerations important to the successful execution of CBDCs, including compliance and AML, CFT, and CPF. Moreover, these documents underlined a sound regulatory panoply, privacy protections, and cybersecurity measures that will ensure the security and stability of the digital currency landscape.

The **online databases** applied in this review include the World CBDC Tracker and the Atlantic Council's CBDC Tracker, which were able to provide real-time data on both the status and progress of CBDCs around the world. These databases have made it quite possible to conduct a comparative analysis in terms of how various countries are moving past the regulatory and economic obstacles in their CBDC journeys.

These sources are, in fact, a certain amount of secondary data that will form the bedrock of this broader analysis. The data will come out with findings that will be used as the basis for the analysis in the ensuing chapter, which gives the holistic results derived from the secondary data. Critical insights from these data provide knowledge with respect to usage, opportunities that may arise from the use of CBDCs, and various risks. The further analysis is given to profound implications that the CBDC has and will pose to financial systems, regulatory environments, and cybersecurity.

All these would form the backbone of understanding, in return, the broad context in which the CBDC would have wide ramifications on the financial system, regulatory regimes, and also on economic stability.

SECTION THREE:
INTERPRETATION AND CONCLUDING REMARKS

V. DISCUSSIONS

5.1. Introduction

The following section provides a critical analysis of the empirical material collected in the context of the present study. The results reveal several critical features in terms of CBDC implementation, mainly on issues of compliance, AML/CFT/CPF, cybersecurity, and relevant regulatory frameworks.

First, it discusses the issue of compliance and regulatory frameworks in the implementation of CBDC. Since the use of digital currencies is becoming more familiar nowadays, it is increasingly important that governments and financial institutions should provide strict legal frameworks to keep the inherent risks at bay while exploiting the potential benefits that may be availed from CBDCs. Of course, proper regulation would stop financial instability and any other misuse.

Next, the paper addresses the CBDC possibilities in AML, CFT, and CPF enforcement. On one hand, an increase in traceability, as well as greater transparency of CBDC transactions, opens new avenues to improve measures against financial crimes. On the other hand, there is still an urgent need to balance regulatory oversight with individual privacy protection.

Cybersecurity, on the other hand, is an important factor. Cybersecurity is one of the most urgent issues for CBDC adoption due to the inherent weaknesses of a computer-based finance system. The appropriate measures need to be implemented so that threats could be defended, keeping the CBDC systems safe, reliable, and resistant against such cyber-attacks.

It economically provides the potential benefits of monetary policy and economic management in CBDCs, such as improvement in liquidity control and improvement in the transmission mechanism of monetary policy. However, reduced deposits and its resultant impact on the lending capability of commercial banks are also potential risks leading to destabilization.

Finally, some ethical considerations on privacy issues are discussed. Digital CBDCs transaction involves ensuring data privacy for users while considering the transparency that must be performed in regard to regulatory compliances. Ethical frameworks should underpin the development and deployment of CBDCs to engender trust and protection regarding personal financial information.

Essentially, what this discussion evidence is that while CBDCs are considered to be a game-changing

improvement by fostering financial inclusions, easing monetary policies, and fighting against financial crimes, the success will be pegged to well constituted regulatory frameworks and cybersecurity measures that guarantee adequate user privacy care in ethics. These elements are going to be vital in determining what role CBDCs may effectively assume in the future global financial architecture.

5.2. Analysis of Key Findings

While CBDCs are gaining their momentum globally, implementations promise enormous opportunities and potential challenges in view of renewing conventional banking and financial systems. Further on, the review reflects principal findings of interviews and answers given by interviewed experts on various practical, ethical, and technical aspects of adopting the CBDC system.

The analysis therefore highlights the following key themes: technical barriers at the institutional level of implementation, ethical dilemmas regarding data privacy and surveillance, and the challenges of compliance with regulatory regimes in a state of constant evolution. It further contemplates the transformation in the CBDC system brought about by emerging technologies like blockchain and artificial intelligence, considering the rising importance of cybersecurity in the protection of digital currencies. The findings also continue to reveal regional variations in adoption and how these CBDCs advance the protocols of AML, CFT, and CPF.

This analysis offers an in-depth look at the challenges and innovations driving the adoption of CBDCs, providing a useful set of information for stakeholders seeking to better understand the complex landscape of digital financial compliance and security. In this light and through the data obtained from interviews, the online questionnaire and the secondary data review that we presented in the previous section, we obtained crucial learnings that are important for this study and for the future and that we consider as key findings that will allow us to definitively resolve the questions that we have raised and that have prompted this research:

1) **Regulatory Environment and CBDCs:**

- How have global regulations adapted to the specific challenges and opportunities of CBDCs?
- What are the ethical considerations these changes in regulations have with regard to equity and access in finance?

2) **Cybersecurity and CBDCs:**

- Due to the nature of digitization in CBDCs, what unique cybersecurity threats does it face?
- How are these threats challenging the ethical standards of cybersecurity in the banking domain while refining them?

3) **Comparative Analysis of CBDCs:**

- How do CBDCs from different national and regional central banks compare in terms of ethical

considerations, compliance requirements, and cybersecurity measures?

- What can be learned from the varied approaches, successes, and challenges each CBDC presents?

We have categorized these key findings into four key points: ethical findings, compliance findings, cybersecurity findings and convergence of themes.

5.2.1. Current Findings of CBDC in Study Regions

This, in turn, reflects various challenges and opportunities which CBDC faces amidst the local infrastructure, regulatory environment, and socio-economic settings, even while getting widespread adoptions across most markets. This chapter reviews the status of CBDCs in Mali, Burkina Faso, and Nigeria regarding ethical issues, compliance, data protection, and AML/CFT/CPF.

5.2.2. CBDC Status in Mali and Challenges

Although CBDC is not implemented, the discussion has taken place with regard to the implementation of an institution of digital currency in Mali. As regards this country, through the financial institutions or central banks inside the regional economic arrangement of WAEMU, a feasibility study on possible CBDC has been made. Simultaneously, it faces many great challenges, such as small-scale digital infrastructures, low financial literacy of its citizens, and regulatory fragmentation.

i. Ethics Challenges

The adoption of CBDC in the nascent digital ecosystem in Mali presents significant ethical concerns. A certain fear of the violation of privacy has been quite evident throughout the survey and interview data. For instance, 73.47% of the participants stated that too much surveillance may provide unauthorized people with sensitive financial information. The people are afraid that CBDC might be used as an instrument for illegal surveillance by state and financial institutions, hence compromising user autonomy. The issue of ethical consideration further extends on the aspect of inclusivity. Considering the condition of basic unavailability of digital gadgets and bad internet connectivity in rural and deprived areas, exclusion of such poor people in Mali in the application of CBDC is quite high. This CBDC would catalyze current inequalities and marginalize large chunks of the population financially without strategies that make this technology usable.

ii. Compliance, Data Protection, and AML/CFT

The regulatory landscape of Mali lags in keeping pace with the technological demands for CBDC implementation. Mechanisms for compliance with AML/CFT and CPF remain underprivileged in Africa although 81.77% (Continuous Monitoring Systems) of respondents noted this, most of them located outside Africa, caused by a lack of real-time transaction monitoring systems. Institutions are heavily

reliant on outdated manual processes that do not meet the speed and complexity of financial crimes attributed to digital currencies.

The state of data protection frameworks in Mali is also underdeveloped. Interview findings stressed that users become highly vulnerable to data breaches, fraud, and unauthorized data exploitation in case of regulatory gaps. Stronger legislation and technology solutions, such as end-to-end encryption and user consent mechanisms, will be required to establish trust in a possible CBDC system.

5.2.3. CBDC in Burkina Faso and Challenges

At the same time, just like Mali, Burkina Faso is in the exploratory stage of CBDC adoption within the WAEMU bloc. Although the BCEAO has made it known that it wants to implement a cross-border regional digital currency, serious infrastructural and socio-economic challenges have so far delayed such implementation.

Mr. Jean Claude Kassi Brou, Governor of the Central Bank of West African States, spoke on Tuesday in Lomé that the BCEAO is considering having its own digital currency. "We are working today on a digital currency to complete the whole range of uses we already have of electronic money in the mobile banking space," he said during the closing round table of the second edition of the African Financial Industry Summit that the Togolese capital hosted on **November 28 and 29, 2022**[75].

i. Ethics Challenges

Ethical concerns about CBDCs in Burkina Faso emanate from socio-economic inequalities. From the survey data, 61.85% chose inclusivity among the most important ethical aspects. In this logical line of argument, it could be assumed rationally that due to the deficit of digital gadgets and internet connections, especially in rural areas, a big section of the people might be deprived of the chances of using the CBDC.

Furthermore, there is growing mistrust in the use and storage of personal financial data. According to interviewees, low levels of public awareness about CBDCs have resulted in fear that any government or third-party operator may misuse or mishandle users' data. Ethical challenges for Burkina Faso, therefore, lie in creating trust and ensuring equal access by focused public awareness campaigns and transparency within governance frameworks.

ii. Compliance, Data Protection, and AML/CFT

[75] https://www.aa.com.tr/fr/%C3%A9conomie/la-bceao-travaille-sur-sa-propre-monnaie-digitale/2751835

No serious means of compliance exists in financial systems in Burkina Faso. It largely runs operations on AML/CFT processes manually, which do not exactly satisfy the real-time operational imperatives of CBDC. Those interviewed emphasized that, ideally, there is a real demand to identify financial crimes through automated mechanisms or systems.

Another critical challenge is data protection. Burkina Faso has not put in place comprehensive cybersecurity policies, and therefore financial systems are highly vulnerable to data breaches and fraud. Such vulnerabilities can only be resolved through cooperation between domestic regulators and international financial bodies in developing interoperable and secure systems.

5.2.4. CBDC in Nigeria and Challenges

Nigeria has launched eNaira, a CBDC, the first African nation to do so and one of only five countries worldwide. Launched on 25 October 2021, eNaira has been developed to complement Nigeria's physical currency, not replace it. About 500 million eNaira (US$1.21 million) have been "minted"[76]. Meanwhile, the acceptance of eNaira has generally been poor because of problems around public trust and infrastructure issues associated with usability problems.

i. Ethics Challenges

While the eNaira was a big achievement in the adoption of CBDCs, much ethics is still in question. Results showed that 14.87% felt rural accessibility has not been well solved by the digital currency. Besides the potential for uptake and usage, poor infrastructure and financial literacy impede the eNaira from effectively reaching the unbanked.

Other pressing concerns relate to privacy: some respondents mentioned even that the government might, through the eNaira system, monitor and eventually track activities. This is exacerbated by the complete lack of clarity regarding how user data is collected, stored, and used. To be able to overcome these ethical challenges, privacy-by-design principles need to be a priority for Nigeria, coupled with effective public communication strategies that build trust.

ii. Compliance, Data Protection, and AML/CFT

Although there has been great improvement in the inclusion of AML/CFT requirements within the eNaira system, full compliance is yet to be achieved. There have been loose ends concerning real-time monitoring of transactions, besides concerns raised over inconsistencies within cross-border regulatory systems that might be manipulated by malice actors.

[76] https://research.hktdc.com/en/article/OTAzODAwODAz

Data protection frameworks in Nigeria need to be further developed. The survey showed **12.02%** of respondents still worried about the adequacy of proposed measures against cyber threats. In fact, to have confidence in the eNaira, global best practices like multi-factor authentication and advanced encryption technologies should be followed by Nigeria.

5.3. Ethical Concerns – Findings

5.3.1. Privacy and Data Protection

Privacy and Data Protection Privacy and data protection was the most important ethical issue overall in the survey, with 73.47% of all respondents giving this topic a rating of "important" or "extremely important". This near unanimity reveals the increased sensitivity of the general public to the possible risks that may be associated with CBDCs, such as data breaches and unauthorized access to personal financial records. These risks are not mere speculations; they are in line with the general increase in cybercrime and the increasingly complex threat landscape against financial infrastructures.

i. Technological Safeguards: Priorities and Challenges

The respondents placed much emphasis on technological safeguards. The use of strong encryption technologies received support from 85.34% of participants, underpinning the important role it plays in securing sensitive financial and personal data against unauthorized parties. This is to ensure that the data will always remain inaccessible by malicious actors in case breaches might happen, hence forming the modern cornerstone of cybersecurity practices.

Yet another major finding entailed the pronounced support of anonymization techniques (Encryption technologies) **58.64%** were for it. It shows that new creative methods of ensuring privacy, while preserving information clarity, are in demand. Among such techniques, particularly promising are those like pseudonymization, where identifiable information is replaced by a pseudonym, and zero-knowledge proofs meant to perform validation of transactions without exposure of underlying data.

Despite the unmistakable advantages of these technologies, major hurdles still persist. There is a very critical trade-off between privacy and regulatory transparency. On one hand, regulators and law enforcement agencies require access to transaction data to enforce standards of AML, CFT, and CPF. On the other hand, too much surveillance might deprive users of trust and avoid the adoption of CBDCs. Achieving this balance is critical and should be done by baking privacy-by-design principles into the CBDC systems from the outset.

ii. Regional Differences and Cultural Sensitivities

Regional differences in how privacy is envisaged emerge from the interview and survey data across Mali, Burkina Faso, and Nigeria. These differences reflect the different levels of regulatory maturity

and cultural attitudes toward data protection in the regions. For instance, jurisdictions with more evolved data protection laws, like the General Data Protection Regulation by the European Union, raise the bar higher compared to less regulated environments. Resulting differences at local contexts will demand solutions also according to international standards.

iii. Collaborative Approaches to Privacy Frameworks

That is to say, these findings go to imply that issues of privacy and protection of data cannot be addressed in isolation by central banks and regulators on the one hand, but require cooperation with technology providers. Even though central banks may take the lead to define the standard on privacy, they cannot do so without inputs from technical experts and legal luminaries.

Other important aspects pointed out by respondents and interviewees relate to data policy transparency. In other words, transparency in data policies also plays another important role: there is a need for users to be well-informed about the collection, storage, and use of their data. The lack of this transparency may undermine public trust in CBDCs and put them at risk.

iv. Future Directions: Investment in Privacy-Enhancing Technologies

Therefore, investment in privacy-enhancing technologies will continue. Among the techniques promising to meet privacy and regulatory requirements harmoniously are homomorphic encryption-that is, performing computations on encrypted data without actually decrypting it. And more is coming from AI: essentially, automatic identification and mitigation of privacy risks in real time. The emphasis on privacy and the protection of personal data is in line with general trends within digital transformation, where trust from users was the cornerstone in technological adoption. Placing such considerations to the fore will thereby make it possible for financial institutions and central banks to establish safe, ethical, and widely accepted digital financial systems.

v. Analysis on Privacy and Data Protection

While these results strongly underline the aspect of privacy and data protection, some open questions still remain. How would central banks ensure interoperability between CBDCs with different privacy standards? How would smaller or less-resourced countries keep pace with advanced technological and financial requirements imposed by high-class privacy? These are questions where further research and discussion need to be done in order to refine ethical and operational frames for CBDCs. Promising though these might sound, technological fixes like encryption and anonymization are themselves not foolproof. For example, newer threats like quantum computing could render currently applied forms of encryption null and void; thus, it will be prudent to prepare in advance for the development of quantum-resistant technologies. The human link in information security encompasses insider threats or operational errors, which is also a cause that cannot be excluded.

Conclusively, the results underline that privacy and personal data protection are not only technical problems but also a matter of moral standing. An integral approach with technological, regulative, and design aspects all centered on the user will go a long way toward ensuring success and sustainability in CBDC. It is only this multi-dimensional strategy that can enable the necessary next steps for handling the challenges in systems of digital currency in order to create a secure, inclusive financial future.

vi. Interoperability Between CBDCs with Differing Privacy Standards

The interoperability of CBDCs will also be very critical in making seamless cross-border transactions across various countries with different levels of privacy standards. It will definitely require:

- **Harmonised Privacy Protocols:** International organizations such as FATF and the IMF should develop a single set of principles regarding privacy, which may achieve the minimum set for all types of CBDCs.
- **Layered Privacy Features:** The CBDCs can be designed to permit setting different privacy parameters, thus enabling them to suit the needs of different jurisdictions. Whereas a jurisdiction might require granular data on transactions, another might need only anonymized data.
- **Interoperability Gateways:** These are technological means that ensure data on the transaction is transmitted securely with data privacy maintained. Operating as relays, they will translate or filter data as local regulatory needs might require.

vii. Assisting Less-Resourced Nations

High financial and technical challenges also impede the implementation of a strong privacy framework in smaller or less-resourced nations. Solutions include:

Technical Assistance Programs: International collaborations under the World Bank and IMF, and regional organizations, are able to send technical assistance, training, and financing to help the less-resourced nation achieve global standards in privacy and security.

- **Scalable CBDC Models:** Developing scalable, modular infrastructures of CBDCs that enable countries to incrementally add on privacy features as their capabilities develop.
- **Public-Private Partnerships:** Partnerships between the central bank and private technology companies will share resources and expertise that may reduce the costs and accelerate the deployment process.

viii. Quantum Computing Threat

Quantum computing threatens, in the longer term, many current encryption methods. Preparing for this requires:

- **Quantum-Resistant Cryptography:** R&D investment in quantum-resistant algorithms, including lattice-based cryptography, should be done so as not to be susceptible to possible quantum computer attacks.

- **Continuous Update:** Ensure the design of CBDC systems will enable seamless updating and adaptability to new cryptographic techniques that will be developed over time.
- **Global Collaboration:** This collaboration by the central banks, universities, cybersecurity companies, and quantum research centers keeps the sector in step with what might be forthcoming.

ix. Mitigating Insider Threats and Operational Errors

Human factor still remains a critical vulnerability in the field of privacy and data protection. With regard to this:

- **Lively Training Programs:** To provide regular training to staff on data privacy policies, best cybersecurity practices, and ethical handling of financial data.
- **Access Controls:** Design and implement role-based access to "need-to-know" policies whereby only the authorized personnel approach sensitive data.
- **Auditing and Monitoring:** Audit and monitoring are necessary to handle continuous auditing of the systems and to avoid insider threats and malfunctioning.

x. Ethical Implications of Balancing Privacy and Transparency

Ethically, it has to balance regulatory compliance with called-for transparency as shown below :

- **Privacy-by-Design Frameworks:** The frameworks of privacy-by-design require embedding aspects of privacy right into the CBDC architecture such that they are not afterthoughts but intrinsic to the design.
- **Stakeholder Engagement:** Representation from Civil Society, consumer rights bodies, and the industry itself goes to create a fine balance between the requirements of privacy and transparency.
- **Clear Policies on Data Usage:** Clearly publishing data usage policies is perhaps the second best way to assure citizens that they are not over-surveilled by these CBDCs.

xi. Public Trust for CBDC Privacy

The public trust forms the very foundation for any successful mass adoption of CBDC. For trust, there is incorporation of

- **Transparency**: Complete transparency about how data will be acquired, stored, and applied.
- **Independent Oversight:** Independent oversight boards to reassure the citizenry through demanding compliance with privacy standards, listening to public grievances.
- **Public Awareness Campaigns:** Public awareness through campaigns about privacy safeguards, misinformation removal, and confidence-building.

Addressing the critical issues of privacy and data protection around CBDCs requires a holistic and

proactive approach. Addressing interoperability, preparing those nations that are less resourced, protecting against quantum threats, mitigating human vulnerabilities, and weighing ethical arguments will eventually help central banks build safe and trustworthy digital financial systems. In such a scenario, collaboration among regulators, technology suppliers, and international organizations would become pivotal in guaranteeing long-term viability and acceptability of CBDCs.

5.3.2. Financial Inclusivity and Accessibility

Ethical Considerations-Financial Inclusion and Access The implicit ethical base in the context of CBDC is financial inclusivity and access. The introduction of digital currencies changes the financially, the purpose of achieving equity in access notwithstanding. From the survey results, 48.72% of the respondents believe financial inclusion is "important" or "very important"; thus, it is a very important element in the design and implementation of a CBDC. This high consensus reveals the potential of CBDCs in mending current gaps in financial inclusion, especially for the under-served and unbanked communities. By placing inclusiveness at the forefront, CBDCs can fuel economic empowerment and help achieve various sustainable development goals.

i. *Offline Functionality: Breaking Infrastructure Barriers*

The key feature identified by a majority of the respondents is the need to be able to operate when they are offline. 45.36% are of the view that CBDC policy offering free or subsidized access to the internet would be fairly effective in the prevention of CBDCs contributing to financial inequality or a digital divide, which is furthered by making accessibility challenges apply satellite-connected mobile phones that will bypass internet infrastructure and widen reach for CBDC services. In this way, by putting together offline functionality with innovative connectivity solutions, CBDCs can be even more inclusive and widely accessible.

This is to say that infrastructure disparities are an inherent component in the adoption of CBDCs at times when internet connectivity cannot be relied on-for example, in rural or poorer parts of the world.

Again, this is supported by interview data, as participants from Mali and Burkina Faso indicated that this functionality is essential in their respective local contexts because of intermittent connectivity. As one participant explained, "For many in rural areas, access to the internet is spotty at best. Offline capability isn't a nicety-it's a necessity for financial inclusion". Allowing CBDC transactions to be completed without real-time connectivity, central banks can widen the use of digital currencies and will not leave any community behind.

Offline functionality also tries to address the affordability challenge in the regions where such digital infrastructure comes at a price. This is because, with the provision of alternative access modalities like

low-tech hardware, SMS-based solutions, among others, dependency on high-cost smartphones and high-speed access to the internet would be reduced. Hence, this falls within the broader framework of inclusivity, ensuring that persons who are already at a marginal position on the grounds of economic incapacity are not denied such an opportunity.

ii. Digital Literacy: Bridging the Knowledge Gap

The next big challenge after infrastructure has been digital literacy. This is evidenced by the fact that results from the survey showed 47.43% of the respondents mentioned systems that accommodate low digitally literate users. This shows the sensitivity of designing user-friendly and intuitive interfaces for all demographics.

Interview feedback reinforced this point, with participants highlighting the challenges faced by older adults, low-income groups, and rural populations unfamiliar with technology. One respondent from Nigeria observed, “If the system is too complex, it will alienate the very people it’s meant to include. Simplicity and accessibility must be the guiding principles”. Features such as multilingual support, visual aids, and streamlined onboarding processes can empower users with limited technical skills to engage confidently with CBDC platforms.

In addition, dedicated education programs can help reduce the gap in digital literacy. Public awareness through campaigns, community workshops, and training will go a long way in demystifying the use of CBDCs to the end-user and building user trust in using them. This should be done in partnership between governments and financial institutions to ensure that even the most vulnerable populations are reached and thus have a sense of inclusion and ownership.

iii. Socio-Economic Impact: Beyond Access

Beyond mere access, the benefits of financial inclusion accrue to a broad set of socio-economic goals. As a means of extending digital financial tools to the disadvantaged, CBDCs have the capability to ameliorate economic inequality, improve financial education, and increase economic activity for different socio-economic groups. These benefits are most pronounced in areas where traditional banking systems are underdeveloped.

The interviewees stressed that CBDCs can facilitate microfinance and small business. According to one of the respondents, “CBDCs can open up avenues for small businesses to access credit and payment systems without barriers created by conventional banking”. In this respect, integrating the unbanked people into formal financial systems, CBDCs may become an important driver for economic growth and upward mobility.

Besides, financial inclusivity using CBDCs aligns with international goals of sustainability in reducing inequality and ensuring resilience in economies. In this respect, central banks should position CBDC as instruments of empowerment that ensure such new technologies truly bring benefits to all parts of

society.

iv. Teething Issues and Strategic Coordination

Achieving financial inclusivity, however, does not come without challenges. Integration of functionality offline and user-friendly interfaces have to balance cost-effectiveness, technical feasibility, and regulatory compliance. For example, the introduction of offline functionality brings along questions of security, particularly in the protection of transactions from fraud and integrity of data.

Scalability is also a concern: the more popular CBDCs become, the more systems will need to expand to handle larger user groups without sacrificing performance. According to interview participants, strategic planning is indispensable for attaining these ends, and as one participant aptly highlighted, "Inclusivity cannot come at the expense of system reliability. We need scalable solutions that grow with demand". The call is, therefore, for strong collaboration between central banks, fintech providers, and policymakers to pursue innovative, sustainable solutions.

We have notice that regional disparities in both digital infrastructure and literacy demand bespoke approaches. While for some advanced technologies may be the emphasis, for others, low-tech solutions might better address local realities. International cooperation and sharing of knowledge will be helpful for central banks to consider best practices while making inclusivity effective and sensitive to contexts.

v. A Blueprint for Inclusive Finance

Ethically, the implementation of CBDCs draws extensively from the grounds of financial inclusivity and accessibility. The nooks of barriers in infrastructure and literacy open up great vistas for transformational potential, thus empowering the underserved to break into economic equity.That says it all: offline functionality, intuitively designed systems to enable wider-scale adoption, bridging the digital divide.

All that would be a dream possible only with committed and sustained zeal, teamwork in fact. To achieve scalable, secure, and inclusive solutions, central banks need to be aligned with technology providers and policymakers. It would be basic to building trust and engaging in educational publicity and public awareness.

Which of course means that the inclusiveness of CBDC as a medium of money will very much depend upon how well adaptability to diversities in use is balanced out against its ethical and operational integrity. Inclusive development of CBDCs could mean a fairer financial future wherein technological advancement benefits all strata of society. Such inclusiveness would add much to economic participation, therefore making CBDCs an even better tool in the social and economic empowerment of

its citizens.

5.3.3. Transparency and Accountability

CBDCs demand unprecedented levels of transparency and accountability for confidence in their use. The issue of fairness, security, and inclusion has been partly addressed using these principles since the conceptualization going into operation. As clearly indicated by the survey results, 70.62% of the interviewed subjects prefer transparency in processes and governance related to transactions. This desire for visibility is not only a public expectation but also a pre-condition for the CBDC system to be credible and work effectively. This focus on transparency will mean that central banks gain confidence and demonstrate their commitment to establishing a sound and inclusive digital currency framework.

i. The Role of Frequent Updates in Enhancing Transparency

The respondents said the frequent updates were primarily instrumental in maintaining transparency. In fact, about **50.96%** of the respondents emphasized that urgent policies and regulations update, operational updates, and reasons for significant decisions are highly needed. It not only clears uncertainties but also helps to make the system administrators, regulators, and stakeholders accountable. These updates can hence bridge the gap between technical experts operating CBDCs and the general public relying on such systems.

The interviews supported this very point. More than a few of the participants noted that updates in good time go a long way in dispelling misinformation and establishing public confidence in the system. As one noted, “Clear, consistent updates on the CBDC policy create a sense of stability and create trust among those users who are skeptical about the implications of digital currencies”. This becomes even more relevant for regions where digital literacy is low and misinformation about new technologies can easily spread like wildfire.

ii. Establishing Clear Communication Channels for Engagement

Transparency in CBDCs also involves intelligent frameworks that allow communication between users and system operators. What the respondents have sought is not a change in users regarding changes to operations but, in fact, open communication about how CBDC systems work, protection of user data, and how complaints or worries may be aired. Good communication does not only drive out skepticism but fosters active users of the innovation.

Practical measures that were suggested from the interview data include multilingual support, community outreach programs, and the use of AI to provide automated assistance to users. According to one of the interviewees, “A truly transparent system is empowering for the users in offering them tools with which to understand and interact with it, be they technical or not”. This supports the call for inclusivity so that even non-technical people can feel safe in using the system.

iii. Technical Transparency and Oversight

Transparency needs to extend into the CBDC's technical features: system architecture, security protocols, and auditing processes. The responses generally echoed support for independent third-party testing and access to governance reports as essential in building operational and ethical integrity. Open documentation and audits help to mitigate public concerns as well as build mechanisms of accountability for developers and regulators alike.

However, technical transparency itself poses some challenges to prevent the cost of security. Several participants pointed out that too much detail might be shared in the documentation regarding system vulnerabilities. One stated, “While it is important for people to have trust, and part of it requires transparency, making too much known about how systems are designed invites cyberattacks”. It is, therefore, fundamentally tied to considerations of balance, openness, and the protection of system security.

iv. Balancing Transparency with Security and Efficiency

There needs to be a synthesis of accountability and operational efficiency in transparency. Too little openness and it will result in erosion of public trust, too much disclosure will expose sensitive security information that could result in vulnerabilities. The respondents believed in differential transparency where, based on the role and stakeholder groups, different levels of access to information should be considered in order not to compromise security by giving the right level of detail to each party.

However, technical transparency itself poses some challenges to prevent the cost of security. Several participants pointed out that too much detail might be shared in the documentation regarding system vulnerabilities. One stated, “While it is important for people to have trust, and part of it requires transparency, making too much known about how systems are designed invites cyberattacks”. It is, therefore, fundamentally tied to considerations of balance, openness, and the protection of system security.

v. Transparency based on Trust

Transparency and accountability, far from being simply imperatives of ethics, are important strategic tools to be used in building public trust for wide CBDC adoption. Updates provided regularly and clearly opened communication channels nurture an inclusive and participatory environment, while independent oversight mechanisms guarantee ethical compliance. On the other hand, evidence from both survey and interview data suggests that regional and cultural contextualization should also be well-thought-out in transparency initiatives. For instance, countries with stringent data protection laws may have more stringent requirements on transparency, while countries with limited or less regulatory oversight may pay more attention to operational efficiency.

Transparency also plays a significant role in the alignment of the CBDC systems with the set expectations of the different stakeholders. Transparency requirements are varied for different financial institutions, regulators, and end-users. Involving the stakeholders in workshops, public consultations, and interactive forums can make transparency measures more effective and inclusive.

Findings indicate that transparency and accountability are key in the successful implementation and management of CBDCs. They are bases for anchoring public trust, operational efficiency, and regulatory compliance. The manner of meeting these ideals has to be innovative and nuanced. In building secure, efficient, and trusted systems, central banks and policymakers look to leverage key technologies such as blockchain, adopt role-based transparency frameworks, and maintain consistent levels of communication with stakeholders for CBDCs. Above all, in the very ethical and sustainable deployment of CBDCs, transparency and accountability are not goals per se but strategies.

5.3.4. User Autonomy and Control

User autonomy and control have remained at the top of the critical list of ethical considerations that are to be kept in mind while designing, issuing, and regulating CBDCs. As many as 66.49% of the survey respondents consider the factor "important" or "very important" to ensure user autonomy and control. This finding underscores the imperative of placing individual rights and agency at the core of CBDC designs in a manner that ensures public trust and confidence in their use.

i. Surveillance and Privacy Concerns

One of the leading concerns indicated by respondents was that there is a high probability of excessive surveillance in the CBDC systems, and therefore 73.47% are concerned about that possibility. Respondents shared concerns that CBDCs might be used to track personal financial activities, essentially undermining privacy and opening the door to the dismantling of personal freedoms. This is particularly concerning in jurisdictions where such a surveillance tool might be used for purposes other than regulation-for instance, political or social control.

Indeed, the interviewees furthered explanations on these very concerns, with specialists referring to historical cases of abuses in monetary systems oversight. Unless transparent limits are put in place regarding data collected and used, said the experts, public trust in CBDCs will be irreparably compromised. They went on to advise that data governance be made transparent and that rigorous countermeasures against the misuse of CBDCs as a tool of social control be put in place.

Similarly, participants recommended privacy-by-design principles in which privacy considerations would be inculcated right from the development stage of the CBDC system. The exact measures endorsed anonymization techniques, including pseudonymization and zero-knowledge proofs, which

allow for the confirmation of transactions without revealing sensitive user information. These technologies balance regulatory demands for AML, CFT, and CPF and user privacy.

ii. Control Over Financial Data

The high percentage of the respondents (66.49% giving "Important" or "Extremely Important") indicates that people value highly autonomy and control over their financial data. People indicate a need for the ability to control the use, accessibility, and sharing of their information. This highlights the need for CBDC systems to incorporate user-centric design principles that provide people with full control over their personal data. Therefore, the survey and interviews showed that users are more suspicious of a centralized system where authorities or a third-party entity would have sole management over their data. Measures for personalizing privacy settings, consent to data-sharing conditions, and opting in/out of the system features were requested by the participants.

The experts also called for robust user controls, just as in modern data protection legislation across the world today, such as the General Data Protection Regulation in Europe. They indicated that CBDC systems should have functions such as "selective disclosure," permitting users to expose only that data which is needed in specific transactions. For example, if one needs to prove eligibility for a subsidy, this may involve the disclosure of income level but not transactional histories. This enables users while keeping regulatory demands met.

Legal and Regulatory Safeguards Most survey participants and interviewees recommended a basic legal framework as a means of protecting user rights in the context of CBDC ecosystems. Such frameworks need to draw lines on the acquisition, processing, and sharing of financial information. Such frameworks should also define mechanisms for redress to enable users to contest the unauthorized use or access of their data.

The respondents argued that a critical analysis of existing financial systems demonstrated legal protection gaps, especially in jurisdictions with weak data protection laws. They believe that the realization of CBDCs offers a great opportunity to shore up such a legal framework to protect individual autonomy from inappropriate interference by central authorities or malicious actors. Besides, embedding accountability measures such as regular audits and third-party assessments will help gain trust among users.

iii. Balancing Autonomy and Compliance

Among the issues posed by the discussion pertains to how to balance compliance with regulatory standards and ensuring user autonomy. Central banks and regulators, on one side, must have access to transactional data in order to successfully enforce AML, CFT, and CPF programs. The other side is that this requirement is typically at odds with individuals' right to privacy. To mitigate this tension, the

participants proposed enabling collaboration between developers, regulatory bodies, and central banks to develop frameworks that harmonize user freedom with compliance demands.

Technological solutions include homomorphic encryption and secure multi-party computation. Both of these methods make the analysis of data possible without the need for exposure of the confidentiality of underlying raw data, hence enabling the regulatory body to trace any illicit activity within a set of transactions without intruding into user privacy. While still at infant stages of development, these technologies do already appear to hold a lot of potential in solving the huge problem presented here.

iv. Implications for CBDC Adoption

These findings of this report amplify a more central consideration in the matter of user control and agency to the ethical development of CBDCs, transcending pure matters of legality and technicality. Both interview and survey respondents emphasized that control over surveillance and data issues is paramount to public trust establishment. These institutions stand to alienate users and undermine objectives such as financial inclusion and digital innovation by overlooking such concerns.

The consultations further revealed regional attitudinal variations regarding control and autonomy. For example, users in those jurisdictions where there is more robust data protection law had higher expectations of user-centered designs compared to users in those jurisdictions where there are less robust regulatory regimes. This highlights the needs for locally specific legal and cultural solutions.

Finally, user control and autonomy are critical to the functional and ethical success of CBDCs. By addressing surveillance concerns, ensuring robust data protection measures, and putting financial data control in the hands of the users, institutions can ensure that CBDCs are ethical and build trust. In the future, there will be a need for central banks, regulators, and technology providers to cooperate in devising systems that can offer a trade-off between compliance and human freedoms. It is only from these focused aspects that extensive use will be made possible with CBDCs and pave the way to attain an inclusive, equitable, and secure digital financial system.

5.4. Compliance Findings

5.4.1. Regulatory Frameworks

Implementation has revealed that it is extremely difficult to reconcile the new systems with prevailing regulatory systems; for example, 37.94% of the respondents believed that integrating CBDCs into current regulations was either a “considerable” or “significant challenge”. These findings give an indication of the challenge of harmonizing extremely rigid, long-set regulatory systems that were generally designed for conventional fiat currencies with the fast-developing technologies brought about by CBDCs.

i. *Adapting Regulatory Frameworks*

A majority of 65.6% of all respondents felt the need to revise the regulatory structures in order to accommodate the rollouts of CBDCs as “extremely high”. This indicates the perception that current laws are incapable of dealing with new dimensions and risks introduced by digital currencies. Conventional financial frameworks are established based on fiat money, and regulations are drawn up with physical money or traditional electronic payments in mind. The regulations are not equipped to handle anything from digital identification to data security and cross-border compatibility, foundation elements of CBDC business.

Survey participants also pointed out gaps in the regulatory frameworks for privacy, cross-border payment, and digital transaction monitoring. Indeed, participants suggested most of these have been fragmented: a reflection, in fact, of the insufficient international standardization of financial regulation. For example, while high priority and therefore stringent data-privacy law form part of a country's landscape, lax protections in other regimes create a divided regulatory environment against which CBDC adoption may stall.

ii. *Harmonization of National and International Regulations*

Yet 27.98% consider the process difficult, which suggests that regulatory harmonization poses a considerable challenge to a notable proportion of respondents. It reflects the considerable effort required to harmonize CBDCs with international regulations. While the majority of respondents consider the process somewhat difficult, the notable proportion that considers it difficult or very difficult reflects the need for greater international collaboration, enabling frameworks, and technological solutions to ease regulatory compliance. Resolving these issues is essential to CBDCs fulfilling their complete potential in an internationally integrated financial system.

Finance has become increasingly global, and among the primary advantages of CBDCs is viewed as their promise for improving cross-border payments. Yet, differing regulations among nations pose a significant barrier. During the interviews, the participants noted that various legal approaches to digital assets can result in inefficiency or increased costs for cross-border transactions. Therefore, they stressed the pressing necessity of coordinating regulatory regimes across various nations on an international scale.

To solve the problem of regulatory differences, the respondents recommended that the development of common standards and means of collaboration between regulatory institutions across borders must be worked on. Some of them would be consistent interpretations on the AML/CFT regime, similar approaches to consumer protection, and information security. Standardized regulations would not only mean simpler cross-border transactions but also trust from the final users and other stakeholders in this

global financial ecosystem.

iii. Balancing Compliance with Innovation

A core insight developed in the survey and interviews is compliance-innovation balancing: very severe regulations choke innovations and minimize all the benefits arising, while too little oversight makes the risk of money laundering, cyber threats, and financial instability grow. The adaptive regulatory framework needs to be responsive and able to evolve iteratively as knowledge and experience in the CBDC domain continue to grow.

Here, the balance will be achieved through regulatory sandboxes. In addition, such controlled environments allow developers to test new CBDC-related technologies within existing laws. With sandboxes to promote collaboration, regulators and innovators collaborate; the regulations are strengthened without harming technological development.

iv. Regional and Cultural Contexts

Interview data underlined most poignantly the necessity of embedding regulatory frameworks into their regional and cultural contexts. As much as global harmonization is needed, regulations are going to have to account for local market conditions and user behaviors. For example, the jurisdictions with the highest financial inclusion rates may see interoperability with existing banking infrastructure as a bigger priority, and regions with significant unbanked populations place a premium on offline functionality with seamless onboarding processes.

Developing economy respondents voiced concern over compliance costs, since the especially restrictive regulations will heighten the already severe strain of limited financial and technological resources. They also call for international cooperation, along with technical support other than financing for countries which have low resources to tackle such challenges.

v. Innovation vs. Risk Mitigation

These participant interviews unraveled the dual role of regulations in fostering innovation while reining in risks. While participants recognized the transformative potential of CBDCs, the major risks that consistently come out are increased vulnerability to cyberattacks and regulatory arbitrage. Regulation should strike a balance between allowing innovation and ensuring security.

One of the key areas that certainly required attention was the infusing of AML/CFT/CPF requirements into CBDCs. Most respondents reported that appropriate reporting mechanisms with state-of-the-art transaction monitoring tools must be in place to deter illegal activities. While doing so, regulations must

ensure user privacy and autonomy while ensuring that CBDCs are not used as a tool for over-surveillance.

vi. Update Regulatory Frameworks

Both the survey and interviews underline that setting the regulatory frameworks of CBDCs is not an easy task. Regulations developed within traditional fiat systems cannot always provide the necessary flexibility to cope with the new features of digital currencies. Here, modernization will have to be provided in terms of data security, interoperability over borders, and verification of identity to make smooth the transition into CBDCs.

Another suggestion he put forth was basically how national and international regulations have to be streamlined. He also expected common standards and methodologies to help international adoptions be relatively easy. As already mentioned above, regulatory frameworks must balance a compliance-innovation trade-off with respect to promoting technological developments and mitigating related risks.

The only way this can be achieved would be through joint and concerted efforts among central banks, regulators, developers of fintech, and international organizations. All these institutions contributing to dialogue and coordination in an effort to set up dynamic, inclusive, and secure regulatory environments that realize the full potential of CBDCs. Well-designed regulatory frameworks will embed confidence, security, and inclusion into the global financial ecosystem, bedrock of modern finance.

5.4.2. AML/CFT/CPF Compliance

The most crucial challenges that the CBDCs will have to go through relate to the compliance with AML/CFT/CPF. Such measures will be fundamental in ensuring that the financial systems are not abused and trust of the public and privacy of individuals remain intact. Most of the surveyed participants, 73.47%, identified the challenge regulators must balance between stringent regulatory requirements and keeping users' privacy. It was a dual challenge underlining the complexity inherent in the design and governance of CBDCs. Integration of CPF: A Multifaceted Challenge.

In a way different from both AML and CFT, CPF demands the system capability for detection and interference in using digital currencies as far as proliferation financing a serious threat relating to WMDs is concerned. To this extent, addressing the problem calls for a framework or a system that detects and intercepts these operations: highly robust, multilayered. What the respondents emphasized in this direction was CBDC systems that could adapt to changing threats without losing efficiency and user confidence.

E-survey participants underlined that these challenges need innovative responses. More concretely, 67% of the interviewees supported the introduction of AI-based transaction monitoring tools into CBDC systems. By making use of high-performance algorithms, such AI-based solutions will be in a position to detect suspicious operations in real time with minimal involvement by humans and at significantly higher efficiency of compliance functions. AI-powered systems process volumes of data, identify patterns of suspicious activity, and raise alerts on abnormalities to be reviewed. It therefore heightens AML/CFT/CPF compliance with minimal intrusion into the privacy of users, an important factor in securing continued public confidence.

i. *Enhancing Compliance Through Advanced Technologies*

AI-powered transaction monitoring has become one of the game-changing solutions for compliance in a CBDC ecosystem. This will go a long way to help regulators and financial institutions analyze large amounts of transactional data with great efficiency for early detection of high-risk behaviors with much better accuracy and much faster than manual processes. For instance, it may be utilized to identify anomalous patterns in transactions, track geographic trends, or recognize behavioral anomalies that would reveal money laundering, terrorist financing, or proliferation activities.

Additionally, the systems may be enhanced for the maintenance of privacy and employ methodologies such as federated learning and homomorphic encryption algorithms. Such techniques enable the artificial intelligence model to operate on encrypted data alone so that sensitive user information is safeguarded against exposure. Consequently, such efforts at compliance can fulfill ethical standards of safeguarding individual rights and necessary standards.

ii. *Transparency in Data Governance*

Data governance transparency goes a long way in making CBDC systems trustworthy to their users. Sensitivity in the collection, storage, and sharing of data should be clearly communicated in a transparent manner, according to the respondents. Rigorous safeguards against unauthorized access and misuse of data should be built into the system architecture. The use of compliance tools, too, needs transparency in their deployment, with public disclosure of their capabilities and limitations to guarantee accountability.

In itself, cross-border transactions add another level of complexity to AML/CFT/CPF compliance. Due to the global nature of digital currencies, there should be harmonization of international standards to deter regulatory arbitrage and compliance gaps. Respondents repeatedly emphasized how collaborative frameworks that bring about consistency in AML/CFT/CPF measures between different jurisdictions would facilitate better interoperability while maintaining strict oversight.

iii. Balancing Compliance and Privacy

Making users use CBDC requires careful consideration of regulation and anonymity of users. Excessive enforcement of rules might scare off the users and adversely affect their trust in the system, while a lack of regulation might attract other abuses in CBDC systems. Privacy-by-design principles must underpin the CBDC system, respondents underlined. This would ensure that all considerations of privacy are integrated at each step of developing the system, right from architecture design to operational protocols. Addressing concerns about privacy, the respondents felt, could be better addressed with customizable privacy settings that allow users to set the level of data shared with regulators and other entities. Users can give way to enhanced privacy modes for nonsuspicious transactions, yielding their ground for high-value or cross-border transfers. In that case, they will have more confidence in taking part in the financial system and be assured of their rights.

iv. The Role of Harmonized Frameworks

International collaboration is critical to the effectiveness of AML/CFT/CPF compliance in CBDC environments. Participants emphasized the importance of harmonized regulatory frameworks that would align compliance efforts across borders. This encompasses the development of common reporting standards, interoperable transaction monitoring systems, and collaborative enforcement mechanisms. Harmonization not only enables efficient oversight but also minimizes compliance expenses for financial institutions with operations in various jurisdictions.

Survey participants also encouraged the creation of international task forces with the mission of implementing AML/CFT/CPF policy in CBDC systems. International task forces would cover technical assistance, the sharing of best practices, and bringing consistency to how compliance standards would be rolled out in countries. The way this can help in making the global financial system resilient to illicit activity, combined with increasing the trust and collaboration among stakeholders.

These findings emphasize that AML/CFT/CPF compliance is one of the most significant success factors for CBDC rollout. Advanced technologies, such as AI-powered transaction monitoring, can be added to the CBDC platforms in order to provide greater regulatory oversight without infringing on the privacy and self-sovereignty of the end-users. Open data governance and modifiable privacy settings are necessary to be implemented for enhancing public trust by compliance controls that are well aligned with ethical considerations.

The need to address cross-border transactions and inconsistent regulation systems therefore calls for inter-border harmonization of the AML/CFT/CPF systems. It is a task demanding collaboration between the central banks, regulators, and technology providers. This will include the development of compliance solutions in order to realize dynamic, scalable solutions that provide user privacy protection.

Abuse protection, though not unique to CBDC environments, will make them reliable and inclusive instruments for modern financial infrastructure.

v. *Customer Due Diligence (CDD)*

The process of onboarding clients for electronic money (e-money) and CBDC accounts in Mali and Burkina Faso necessitates strict adherence to customer due diligence (CDD) and KYC obligations. This will help to accomplish legal and regulatory requirements for the purpose of combating money laundering, terrorist financing, and proliferation. KYC is much more than document gathering; it's about the perception of risk profiling of customers, ensuring their future transactions are in congruence with the information provided at account opening or periodic reviews. It stands at the very center of the whole AML/CFT/CPF regime.

Required Due Diligence for Financial Institutions

These institutions, in both Mali and Burkina Faso, are subject to compliance with national and regional laws that include UEMOA's Regulation 15/2002/CM and the revised AML/CFT/CPF Law of 2024. The following must be done:

1) **For Individuals:**
   - Valid identification documents from recognized authorities should be collected: national ID cards and passports.
   - Proof of address: utility bills or certificates of residence.
   - Due diligence for PEPs, including proof of income and source of wealth.
2) **For Legal Entities**
   - Validate the registered address of the entity's headquarters.
   - Confirm the identity and authority of associates and company executives
   - Ensure the entity's legal constitution with documents such as a recent Trade Registry certificate
   - Obtain certified financial statements, meeting minutes, and annual reports to confirm operational legitimacy

Mitigating Risks of Shell Companies[77]

Shell companies represent considerable risks in that the concealment of beneficial ownership makes possible corruption, money laundering, and terrorist financing. From other jurisdictions, Mali and Burkina Faso have learned the need for improvement in transparency: indeed, the obligations have been

[77] Banking Compliance in Senegal and in the UMOA Zone (La Conformité Bancaire au Sénégal et dans la zone UMOA)" by Moussa Sylla - 2023

imposed on the creation of a register of beneficial owners with:

- Full identification details.
- The nature and extent of control.
- Dates of acquisition or cessation of ownership.

Risk-Based Approach to CDD

After completing KYC, financial institutions can categorize clients based on their risk levels:

- **Standard or Simplified Due Diligence (SDD):** For low-risk clients.
- **Enhanced Due Diligence (EDD):** For high-risk clients, such as PEPs, entities in high-risk sectors, or those located in jurisdictions flagged by the FATF[78].

Supervision: The institutions should monitor sectors highly exposed to AML/CFT risks. Extractive industries in Mali and Burkina Faso and even in Nigeria are generally exposed to high corruption and illicit financial flows. The threshold defining beneficial owners in these sectors should be lowered in line with international best practice, and even far below the normal threshold of **25%** to address the higher risk involved.

Cross-Border Risks

Cross-border transactions, in particular those with jurisdictions that have poor AML/CFT controls, increase the risk. Financial institutions in Mali and Burkina Faso should be extra vigilant by applying enhanced scrutiny over transactions involving countries identified by the FATF or the EU as being high-risk.

Importance of Ongoing Monitoring

KYC processes shall be dynamic and should include regular updating of the account information where the clients develop changing risk profiles. For example, if after onboarding it is realized a person has PEP, heightened measures shall apply immediately. Correspondingly, Institutions shall monitor suspicious transactions irrespective of the client profile upon onboarding.

E-money and CBDC ecosystems must have appropriate, robust measures of KYC for effective mitigation of the AML/CFT/CPF risks in Mali and Burkina Faso. Compliance can only be complete

[78] FATF (2023). International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation. FATF Recommendations: https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Recommendations%202012.pdf.coredownload.inline.pdf

where there is full adherence to international standards, increased transparency, and a risk-based approach so that it does not impede financial inclusion or innovation.

5.4.3. Institutional Preparedness

Institutional preparedness is one of the most important preconditions to effectively implement CBDCs. Against this backdrop, it becomes really worrying that most experienced interviewees believe that financial institutions are not well-prepared to deploy CBDCs and that the deployment would not be possible without disrupting ongoing services. They interpret from that: skepticism results from questions concerning system integration, operational complication, and transformation in nature.

i. Legacy Systems: A Significant Barrier

During the interview, Dr Sissoko pointed to one of the biggest challenges being contributed by legacy systems: most of the traditional structures within the financial ecosystem were built for legacy fiat-based operations and thus cannot support some of the agility and scalability needs of CBDC transactions. This is because most of the underlying infrastructures of these legacy systems are not natively built for high-speed processing of CBDC-related transactions, integrated security measures, and interoperability requirements. The upgrade path requires heavy investment in hardware and software technologies, plus extensive reconfiguration efforts.

These are really the problems with which small and medium-sized financial institutions are disproportionately affected, while they usually have a serious lack of finance and technical resources to perform such upgrades. The cost of modernization is pretty substantial, including software development, hardware installations, and workforce training. Training is especially important, as staff must be firmly trained in the subtleties of CBDC system operations, from pure back-office transaction processing to compliance with AML/CFT/CPF standards.

ii. Operational Risks during Transition

Apart from infrastructural issues, during the transition to CBDCs, operational risks are looming large. The integration downtime is huge, as it can disrupt the ongoing financial services and may even break the trust of customers in it. Every institution obviously has to be more vulnerable to cybersecurity threats whenever new technology is integrated into a system. Adding to this complex transition, CBDCs require very high real-time processing demands and thus require strong systems in order to resist high loads of transactions without affecting their speed and security. Others include interoperability with existing financial systems and international payment networks, since seamless connectivity is central in the efficiency of CBDC.

iii. Preparedness Recommendations by Respondents

A number of strategic suggestions were given by the respondents to get over these challenges, which

include;

1) **Phased Implementation**

There was extensive support for implementing CBDCs using a staggered approach, a strategy allowing an institution to get adapted over time with less disruption of ongoing services. Through staged implementation of the CBDC, financial systems could be tried, refined, identify and eliminate problem areas and allow confidence among participants.

2) **Public-Private Partnerships**

The engagement in collaboration with technology providers between the central bank, financial entities took center stage in the respondent's view as very fundamental. For instance, public-private partnerships might be used to share knowledge, resources, and best practices to achieve innovative solutions for CBDC-compatible technologies. Partnerships can also distribute the financial burden of system upgrades among more players, making the transition more viable for smaller entities.

3) **Regulatory Incentives**

Another key driver for modernization was highlighted: regulatory incentives. Tax benefits, grants, or subsidized loans to institutions that invest in resilient and scalable platforms would, when designed for CBDC compatibility, provide incentives for the adoption of CBDC-compatible systems. Policymakers are well-placed to create an enabling ecosystem for innovation and growth in the financial sector.

iv. Role of Central Banks and Technology Providers

Central banks and technology providers will be crucial in playing a supportive role in institutional preparedness. The central banks can give full guidelines and technical support to smoothen the transition. Technology providers can develop solutions that may be tailored for different types of institutional needs. Open-source platforms and modular technologies would be of particular help in integrating CBDCs into the running operations with any effect of complete system change.

v. Building Resilience and Efficiency

Institutional preparedness is not only about managing current challenges; it's also an opportunity to make the financial system more resilient and efficient. Modernization of legacy systems to accommodate CBDCs can result in more comprehensive benefits, including faster transaction processing, enhanced security, and better customer experiences. Only through investment in modern, scalable infrastructure will financial institutions position themselves for long-term growth and innovation.

vi. In-depth examination

While the concerns this survey has raised do underline serious barriers to the adoption of CBDCs, they also emphasize how important it is to deal proactively and collaboratively with these challenges. The

strategy of phased implementation necessary to support institutions through the complexity of the integration of CBDC requires public-private partnerships and regulatory incentives.

The one area that needs deliberation is the role of smaller financial institutions. Whereas large banks may be able to upgrade their systems, smaller ones might not keep up with the pace. Policymakers and central banks need to ensure that the transition toward CBDCs does not widen inequalities within the financial system. Very relevant is the need for cybersecurity measures which can handle unique risks associated with CBDCs without impacting efficiency.

The other concern is the possibility of divergence in approaches in different jurisdictions. In their absence, international coordination may lead to divergence in regulatory regimes and technological standards that can impact the interoperability of CBDCs across borders. There is a need for cooperation among central banks in developing common norms and standards that promote harmonization and consistency.

Finally, successful implementation of CBDC is significantly influenced by institutional preparedness. Though serious challenges exist, they are not impossible to overcome. In fact, the road to full-scale CBDC infrastructure can be achieved through phased implementation strategies, public-private partnerships, and regulatory incentives. Central banks and technology providers will have to assume active roles in supporting these processes and seeking the transition so that it is smooth, secure, and inclusive.

This would be an opportunity to further improve the efficiency, resilience, and inclusiveness of the financial sector by modernizing the financial system in preparation for the absorption of CBDC. With the right strategy and support, institutions will be in a position to succeed at overcoming today's challenges and unleashing digital currencies' transformative power.

5.4.4. Consumer Protection

In the light of the results, consumer protection seems to be one of the pillars of CBDC adoption, as 61.86% of the surveyed subjects ranked the topic of consumer protection measures as Very Important or even “critical”.

Almost consensus speaks to how urgent this is in terms of users' and the CBDC system's security. Proper consumer protection is not just risk reduction alone; it is also the basis of trust and mass adoption.

i. Key Areas of Concern

1) Fraud Prevention

Fraud in the digital currency world is a headache of enormous proportions. The world of CBDC is at higher risk due to cyber attacks; hence, fraud prevention methods need to be very sophisticated in order to protect the users better. Some of those would be:

- **Real-time monitoring:** There should be systems that track, second by second, the occurrence of unusual transactions and anomalous trends that may indicate fraud.
- **Robust encryption technologies:** use of superior encryption methods, ensuring sensitive information of users remains beyond the access or breach by unauthorized parties;
- **Multifactor authentication:** protection of accounts behind multi-type authentications, using biometric on top of either password or tokens.

These would bring a long way in raising security for CBDC systems and thus build users' confidence if applied accordingly.

2) Dispute Resolution

The survey is one that spoke to the need for effective and efficient mechanisms to resolve disputes arising in transactions. A failed resolution of a dispute or a transaction breakdown would lead to a loss of faith in the CBDC. Some key aspects are:

- **Error correction procedures:** Efficient mechanisms related to the correction of unauthorized transactions or system faults can foster fairness and accountability.
- **Accessible customer support:** The mechanisms for customer support should be available and operational to facilitate users in seeking easy resolution of their problems.
- **Independent mediation bodies:** There is a dire need to establish independent arbitration committees that can handle complex disputes and create trust in the impartiality of the system.

These steps demonstrate how an institution can effectively address complaints of users and prevent dissatisfaction, which is essential for establishing trust.

3) Education and Awareness

The majority of the responses reflected the susceptibility of the users for reasons of insufficient digital literacy. Awareness and education programs will strengthen the users and reduce risks.

- **Public awareness campaigns:** creating adequate awareness about the use of CBDCs, the accruable benefits, and risks that are likely to emanate from their use.
- **Targeted training programs:** Need-based programs for less technologically savvy groups, like the elderly or rural communities, to make them feel safe and secure with CBDCs.

These programs will be important for the consumers, both in understanding and reducing potential exploitation or abuse.

ii. Proposed Consumer Protection Measures

1) Regulatory Safeguards

The CBDC regimes should be subject to mandatory standards that guarantee the same level of fraud detection, dispute resolution, and data protection. The regulations must be clear, actionable, and updated periodically to keep up with emerging vulnerabilities.

2) Liability Frameworks

Accountability structures are the necessary ingredient for consumer complaints to be addressed and for fraud and system breakdown to be ascribed with blame. Transparency in liability frameworks provides clarity and limits disputes by informing users about their rights and their redress.

3) Feedback Loops

The instituted consumer feedback mechanisms ensure that the vulnerabilities within institutions are noted in real time, and their rectification is done accordingly. Loops like this provide a sense of inclusion in that users believe their concerns are being heard and catered to.

iii. Instilling Confidence and Trust

esults from the survey show that protection for consumers is at the heart of earning public confidence in CBDCs. The meaning from the responses was that without adequate security and ease of use, the adoption of CBDCs will be grossly hindered. Financial institutions and regulators should focus on:

- **Security:** Security, for this reason, shall be of the highest order in protecting the asset and information of users.
- **Transparency:** Clearly communicating the measures in place to protect users and how potential issues are handled.
- **Inclusivity:** The design of systems to be used by a wide variety of users, especially those with limited access to, or familiarity with technology.

iv. Analysis findings on Consumer Protection

While consumer protection is very important, strong systems are difficult to implement. This means that needing a system which continuously monitors for activity and does multi-factor authentication can make things cumbersome and might potentially seriously slow down transaction times. Such trade-offs need to be balanced by seeking innovative solutions which make the systems more secure, yet don't lose any aspect of their usability.

Another challenge will be the harmonization of consumer protection measures at different jurisdictions. The differences in legal and regulatory frameworks may leave loopholes that malicious actors will take advantage of, especially in cross-border transactions. International cooperation is vital for consistency

and effectiveness.

In addition to this, consumer education programs should be more accessible. The programs must be adapted to fit the groups they will be used with and the resources must be presented in various languages. These efforts require considerable investment, which may strain the budgets of smaller institutions.

To conclude, consumer protection is indeed one of the critical pillars of the successful execution of CBDCs. Fraud prevention, dispute resolution, and education, in light of the issues raised by the survey, are important in creating a secure and convenient environment. This effort is further enhanced through regulatory safeguards, liability frameworks, and feedback loops.

At the end of it all, consumer protection means increased credibility and sustainability for CBDCs as well. The financial system and regulators can work together to bring about a secure digital currency ecosystem that inspires confidence and encourages widespread adoption. Indeed, shaping a robust, secure, and inclusive financial future will depend on being conscious of the need to get CBDC systems right on consumer needs.

5.5. Cybersecurity Findings

5.5.1. Data Security Risks

The large-scale transformation of Central Banks into CBDC has come with the problem of cybersecurity threats. Among them, in the data security area, it has been one of the key ones. Unauthorized access, data breaches, and identity theft pose the greatest threat to the integrity of CBDC systems, consider 64.58% of the total distribution of respondents. These risks will lead to compromised sensitive user data, along with making the core reason for using the CBDCS-ideal trusted relationships-pessimistic.

i. Key Data Security Risks

1) Unauthorized Access

One of the worst identified risks to CBDC systems is unauthorized access. Terror groups and other ill-willed users can always find vulnerabilities in digital systems to gain unauthorized access to sensitive data and transaction records. Such breaches may result in extensive harm, from financial loss to loss of reputation for institutions and central banks.

2) Data Breach

Identity theft was another risk identified, where breached security measures would allow the intruder to be able to steal user identities. Such breaches could facilitate unauthorized transactions, which, again, dampen confidence in CBDCs and be problematic to provide ways of recovery for those affected.

3) Identity Theft

Another risk was identity theft, where compromised security protocols could result in the attacker being able to steal user credentials. Such breaches could facilitate unauthorized transactions, which, again, dampen confidence in CBDCs and be problematic to provide ways of recovery for those affected.

ii. *Mitigation Strategies*

1) Advanced Techniques of Encryption

An overwhelming percentage of 58.64% supported advanced methods of encryption in order to safeguard data both while in transit and at rest. Encryption ensures that even if the data is intercepted by unauthorized parties, such data will not be accessible. Utilizing end-to-end encryption, and other advanced cryptographic protocols from the financial institutions would significantly reduce the exposure risk of the data. Some of the encryption techniques include:

- ✓ **Homomorphic encryption:** "balances privacy with regulatory needs, critical in compliance-driven environments like CBDCs.
- ✓ **ZKPs (Zero-Knowledge Proofs):** They give the highest privacy while still doing verification transparently. This was the last and most talked-about technique during the interview. According to Dr. Julian, this zero-knowledge proof will be able to enable the user in giving the proof for the validity of transactions without revealing any sensitive information. Implementation of hierarchical digital wallets that separated small, anonymous payments from large, verifiable transactions.
- ✓ **Post-Quantum Cryptography:** Ensures future-proofing, protecting CBDCs from next-generation threats.

2) Multifactor Authentication

Another highly recommended solution was multi-factor authentication. Respondents stressed that it would add extra layers to user accounts for security. Multi-factor authentication needs a number of verifications-like password combinations, biometric verification, or security tokens-to allow access. This helps to considerably reduce unauthorized entry and enhance the protection of user accounts.

3) Security Audits on a Regular Basis

Participants suggested frequent security audits in order to locate vulnerabilities before actual attacks take place. Auditing will help an institution find weak links within its systems and maintain their defenses at strength. Auditing also keeps cybersecurity policies and practices current.

iii. *Advanced Technological Solutions*

1) Artificial Intelligence and ML for threat monitoring

In this respect, the interviewees referred to proactive threat monitoring including the integration of AI and ML technologies. The integration of technologies allows for real-time analyses of patterns of transactions, which will define unusual behavior that signals breach in security. Early detection, therefore, makes it easier and faster for a financial institution to respond and contain the damage.

2) Zero Trust Architecture

Another recommendation was the implementation of a zero-trust architecture where no user or system component is intrinsically trusted. Access is given only after strict verification; even internal systems have to go through severe checks. This will greatly reduce the chances of unauthorized access or internal breaches.

3) Incident Response Plans

Robust incident response plans, which are identified as very crucial in mitigating the impact of cyberattacks or data breaches, should clearly outline the steps required for identifying, containing, and resolving security incidents, and also strategies that will ensure quick recovery. An effective framework ensures that there is minimum disruption to users and strengthens confidence in CBDC systems.

iv. Strategic and Policy Recommendations

The survey also exposed a large gap in strategic coordination between central banks, financial institutions, and technology providers. As such, this is a challenge that cannot be met effectively by one stakeholder and requires cooperative input from various stakeholders. Various strategies will include:

1) Policy Development

Governments and regulating bodies have to enact strong cybersecurity laws that deal with specific CBDC challenges. The laws have to require minimum encryption levels, authentication procedures, and periodic audit requirements to guarantee system integrity.

2) Capacity Building

Institutional staff training programs, along with public awareness campaigns, will be highly effective in making all stakeholders aware of their responsibilities in upholding cybersecurity. It can also make users more attentive to best practices, such as phishing detection and credential management, to reduce vulnerabilities.

3) International Cooperation

Since digital currencies are global in scope, international cooperation will be required. International harmonization of cybersecurity standards and threat intelligence sharing could enhance collective defenses against advanced cyber threats.

v. *Addressing Challenges Proposal*

Although the strategies presented offer a solid foundation for maintaining data security, challenges remain. In fact, improvements to advanced encryption methods and zero-trust architectures add to system complexity and higher operational costs. For banking institutions, especially smaller ones, adopting these improvements is very challenging in terms of both their resources and technical expertise.

The challenge is how security will be balanced with user experience. Strong security controls, for example, can be very vexing for the end-user, such as frequent MFA prompts or longer verification codes, and could therefore hold them back from using the solution. This means that institutions will have to create systems to incorporate seamlessly with options for security, not at the cost of usability.

Thus, data protection takes top precedence in CBDC implementation. Unauthorised access, data breaches, and identity theft were mentioned as pressing concerns by 61.45% of the participants; hence, cybersecurity must take precedence. Adoption of advanced technologies like encryption, multi-factor authentication, and AI-driven threat detection will be effective, along with periodic audits and strong incident response mechanisms.

Finally, it will be the ability of central banks and financial institutions to safeguard user data that will engender public trust in CBDCs. The financial sector will have to be actively and collaboratively involved, achieve a trade-off between security and usability, and will carry the responsibility of resiliency and integrity for CBDCs. A host of vulnerabilities being prevented for the users by experience in data security concerns stands as a very good grounding toward a secure, inclusive digital future.

5.5.2. System Vulnerabilities

System vulnerabilities are one of the major concerns when implementing CBDCs. In the survey, **28.57%** of respondents rated system vulnerabilities as “extremely significant,” while another **35.45%** rated them as “significant”. These findings emphasize the importance of addressing architectural weaknesses to guarantee the functional reliability of CBDCs and earn the public's confidence.

i. *Key Challenges*

1) Legacy Systems and Scalability

One common fear expressed by many respondents was reliance on legacy systems, which are usually incapable of supporting the CBDC requirements. Most of these systems are not designed to scale for millions of transactions that a digital currency would entail and thus act as a bottleneck to wider diffusion. The question among respondents was whether current infrastructures could resist an ever-increasing level of cyberattacks, which might also leverage scalability and interoperability weaknesses.

2) Software Vulnerabilities and Threat Detection

The second vulnerability related to the exploitation of vulnerabilities in software. Since digital systems interlink many elements, their failure may cause cascading effects leading to disruptions of services, fraud, financial losses, and even system-wide collapses. Poor threat detection mechanisms increase the risk of such events since CBDC systems then cannot operate with full protection against threats by advanced persistent threats and malicious actors.

ii. *Mitigation Strategies Proposed*

1) Continuous Monitoring

The most proactive strategy for risk detection and mitigation, according to the suggestions of the majority of the participants **56.25%**, is continuous monitoring of system activities. Advanced analytics with AI will be able to detect in real time suspicious behaviours such as unauthorized access attempts and irregular transaction patterns. It also helps the institution take remedial action before minor threats metamorphose into major breaches, thus strengthening the overall resilience of the CBDC systems.

2) Penetration Testing

The most effective means, periodic penetration testing, was supported by surveyed, since it uncovers hidden vulnerabilities. Simulated cyberattacks against CBDC systems allow the financial institutions to locate weaknesses that may not be evident during the course of routine business. This process will allow the institution to take early measures to strengthen security and reduce the probability of vulnerabilities being exploited by bad actors.

3) Secure Software Development Practices

It is very important that secure development practices be emphasized, including vigorous testing during the development phase and timely updates to patch known vulnerabilities. Secure coding standards and vulnerability assessments are industry best practices that can go a long way in reducing the risk of software flaws. Another very important aspect is to collaborate with external cybersecurity experts and auditors for independent verification regarding system robustness.

4) Cyber Resilience Frameworks

The survey proved a rapport of including robust cyber resilience frameworks with both preventive and recovery mechanisms. The preventive measures, such as firewalls and intrusion detection systems, may help foil a potential breach, while recovery mechanisms ensure that there is minimal damage in case such an incident occurs. Incident response plans and backup systems were two recommendations that came handy from respondents for speedy recovery and continuity.

5) Training and Awareness

Training for IT staff on a periodic basis was cited as one of the most important elements in reducing system vulnerabilities. The nature of cybersecurity threats, as respondents explained, is ever-evolving, and staff need to be continuously educated about new risks and how to respond to them. Improved training optimally equips personnel with knowledge regarding the detection and response to threats.

While these strategies are very viable as a starting point to help nullify the identified system vulnerabilities, a number of challenges arise in their implementation. Continuous monitoring and penetration testing require huge investment in cutting-edge technologies and expertise, which may be a limiting factor for small financial institutions. Integration of such measures into existing infrastructures is not always easy and resource-intensive without disruption of operations.

Besides, another key consideration is the trade-off of security against usability. For example, strong security, such as monitoring all the time or stringent access controls, complicates the system and influences user experience. Financial Institutions need to create solutions that will fit into user workflows while not compromising high standards of security.

Besides, cyber threats are also rapidly changing; hence, system security should be dynamic. Institutions should be observant and agile in updating their defenses against the emerging risks. This shall call for collaborations across stakeholders-the central banks, regulators, and technology providers-to develop, adopt, and implement appropriate cybersecurity frameworks.

Success in the usage of CBDCs demands the respective responses to the vulnerabilities within the systems. Results of this survey put in place various proactive measures which include continuous monitoring, penetration testing, and secure software development to mitigate risks. Second, setting up robust cyber resilience frameworks and regular training of IT personnel would help further strengthen CBDC platforms against any potential threats.

By prioritizing these strategies, financial institutions will increase the operational integrity and security of the CBDCs, consequently engendering public confidence and belief in the digital currency ecosystem. Though there are still challenges ahead, cybersecurity will be significantly ensured through collaborative and adaptive methods that will make CBDCs resilient and reliable, hence smoothly integrating into the global financial system. This way, CBDCs will realize their potential in being secure, efficient, and inclusive tools for the future of digital finance.

5.5.3. Fraud Prevention

The measures that offered a way to prevent fraud were a very high priority in CBDCs, with 61.86% of the respondents considering that it would be important to keep such a digital system secure and

trustworthy. Because of the pure digitality of CBDCs themselves and the scale into which they are applied, counteracting fraud requires effective anti-fraud measures for deterring, detecting, and responding to fraud.

i. Key Fraud Risks

Respondents indicated that financial fraud has become very sophisticated, using even the latest schemes such as phishing attacks, manipulation of transactions, and identity theft. In a CBDC environment, because these systems are interlinked, this could escalate a single incident throughout the network, leading to a disaster situation of significant financial loss and loss of public confidence.

The phishing attacks, whereby users were conned into revealing their sensitive information, and identity theft, where the unauthorized individuals took up the identities of legitimate users, were noticed as critical. Moreover, participants pointed to the access privileges of insiders that could be exploited easily, meaning a need for solid internal controls.

ii. Advanced Technological Solutions

1) Machine Learning in Fraud Detection

Application of machine learning technologies should be one of the cornerstones of fraud prevention. ML algorithms can parse enormous volumes of transactional data in real time to pick out anomalies-spending habits that fall outside of the norm, attempts at unauthorized access, unusual volumes of transactions, etc.-and flag these for further investigation. In turn, institutions can take proactive steps via ML tools in order to minimize losses and protect users' data.

2) Behavioural Analytics

Other participants also suggested including behavioral analytics into fraud detection systems: these systems create a pattern of 'normal' user behavior and flag deviations from normal behavior that may indicate fraudulent intent. Behavioural analytics can be of particular value in combating insider threats, where fraud is conducted by subjects with authorized access who seek to exploit the system. This underlines the role of combining behavioural insights with ML to empower institutions in the identification of-and response to-complex fraud schemes.

3) Multi-Tier Authentication Mechanisms

Another of the very important recommendations was to introduce multi-channel authentication mechanisms in order to introduce security. This would mean that at any point, biometric, OTP, and token-based authentication would ensure there is just no way a person could get access without proper authorization. This ensures that it allows only valid users to either operate or view sensitive information on the CBDC platforms.

iii. User Education and Awareness

Besides technological solutions, education and awareness campaigns were also pointed out by participants as something which is very much part of the fraud prevention. The users have to be educated on the way in which common frauds are being committed, such as phishing and social engineering, along with best practices in digital security. Educating users allows them to identify and avoid fraudulent schemes, which reduces the overall fraud risk to the system.

Similarly, regular training for the personnel dealing with CBDC systems was considered necessary. With this, the personnel can be kept abreast of emerging threats and the latest security measures in order to remain vigilant and respond effectively to potential risks.

iv. Strategic Recommendations

It is observed based on the discussion that various suggestions of fraud prevention came up involving advanced technology, awareness of the users, and stringent systems' control. They involve:

Real-Time Monitoring and AI Integration

Provide real-time monitoring of transactional behavior using AI-driven tools and immediate alerts in case anomaly behavior is detected.

Enhanced Authentication Protocols

Implement multi factor authentication and biometric recognition to improve access control.

Blockchain Implementation

Utilize blockchain to register all CBDC transactions in a tamper-proof and transparent ledger to avert fraud and facilitate regulatory compliance.

Public Awareness Campaigns

Inform users about fraud risk and prevention measures through multiple awareness campaigns to promote a culture of awareness.

Staff Training and Development

Provide regular training to the CBDC system's administrators and staff on how to effectively handle emerging fraud.

v. Analysis on Fraud Prevention

While these solutions furnish a formidable framework for fraud prevention, there are many challenges associated with their practical implementation. Advanced technologies such as AI and blockchain demand huge investments in addition to technological expertise, which may be beyond the capability of smaller financial institutions. Besides, the trade-off between security and usability remains a pressing concern. For example, a very complex authentication mechanism may discourage users from adopting a service; some people might have poor digital literacy.

Also, the dependence on technology introduces new vulnerabilities, such as faulty AI algorithms or

vulnerability in blockchain systems. This means therefore that institutions should be dynamic in creating and updating their fraud prevention measures considering the ever-evolving nature of the threats.
Fraud prevention is one of the main bases of CBDC cybersecurity and needs to be addressed by an approach that blends advanced technologies with user education and system controls. Using machine learning, behavioural analytics, and, importantly, blockchain technology, financial institutions will be able to identify and discourage fraud while maintaining user trust.

These initiatives further get complemented by educating the users and the staff about risk identification and how to manage risks. Although concerns persist in security, ease of use, and cost combinations, the suggested paths form a broad-based route towards the assurance of integrity within the CBDC system. Financial Institutions can let proactive measures and innovation keep CBDCs secure, trustworthy, resilient against modern financial digitization.

5.5.4. Emergence Operational Resilience

Operational resilience has been a focus of CBDC cybersecurity concerns, brought to prominence through the perspective of participants for System and Operational Risks and Resilience Planning. This reflects the need to incorporate redundancy measures into the design and ensure disaster recovery process protocols. Since CBDCs are designed to be at the forefront of modern financial architectures, they must be resilient as well to be able to provide unbroken continuity of services in all circumstances.

i. What is Operational Resilience

Operational resilience concerns the minimization of the impact resulting from unexpected events such as cyberattacks, natural disasters, system failure, or other operational disruptions. From the perspective of the interviewed, CBDC system disruptions could have potentially important spillover consequences, such as public loss of confidence in financial systems, financial instability, and even possibilities for malicious actors to exploit such vulnerabilities.

ii. Redundancy Mechanisms

Several of the participants considered redundancy mechanisms to be a core strategy for operational resilience. The redundancy mechanisms included backup systems and infrastructures at different locations that allow operations to continue in the case of disruptions in localized areas. These included:

1) **Geographically dispersed data centers**

CBDC systems reduce the risk of single-point failures by spreading out vital infrastructure at a number of locations. In case one data center goes down, others can cover up immediately, and services will never be cut off.

2) **Distributed Ledger Technologies (DLTs)**

With DLTs, there is greater resilience since the decentralization in the validation of transactions implies that no node is critical to the operationalization of the system at any moment in time, given that no node is needed in the case of the centralized systems. In effect, the entire system is much more resilient to attack or technical failure.

3) Cloud-Based Backups

The real-time replication of vital information using cloud-based systems enables non-stop access amidst downtime. Cloud backups also offer scalable redundancy, which is useful for expedited service recoveries/restorations.

iii. Disaster Recovery Protocols

The other equally significant consideration that was taken into account has to do with end-to-end disaster recovery protocols. The idea behind these protocols is to develop a clearly defined and highly tested response plan aimed at the speedy restoration of services following an outage. The interviewees suggested the following interventions:

1) Routine Disaster Recovery Drills

Drills enable organizations to rehearse their recovery plans, flag loopholes, and sharpen their plans to prepare themselves better for the real event.

2) Automated Recovery Systems

Automation shortens recovery time by resuming operations quickly without the need for human intervention. Automated systems can redirect traffic, recover lost data, and restart services with minimal disruption.

3) Communication Plans

Communication with customers during service disruptions must be open and transparent in order to manage public perceptions. Notifying customers of expected repair times, the security measures in effect, and what is being performed to resolve the problem helps to build trust and prevent panic.

iv. Real-time Monitoring and Predictive Analytics

It places special emphasis on real-time monitoring and predictive analytics in operational resilience. More advanced, AI-driven solutions can identify anomalies in their nascent stages, such as suspicious patterns of transactions or latency issues. Detection at an early stage allows institutions to mitigate problems in advance before they become large-scale disruptions. Predictive analytics also increase resilience by forecasting potential risks from historical events and current trends.

v. Zero-Trust Security Architecture

This is succeeded by another main recommendation-deployment of zero-trust security architectures. In

the zero-trust design, no component of the system, device, or user is trusted by default. There needs to be the ability for constant verification with regard to access and the validity of any transaction. This would reduce any threats of unauthorized access or system failure, hence retaining the integrity of the CBDC systems.

vi. Collaboration and Standardization

According to the interviews, this can be achieved only if the central banks, technology firms, and regulatory authorities are able to work together in building one model of resilience. This initiative will provide enhanced interoperability across national boundaries, thereby allowing the global financial industry to respond more effectively to new problems arising. This comprised:

- Standard directives with regard to redundancy measures and disaster recovery systems.
- Incident reporting guidelines in facilitating a coordinated response to disruptions.
- Best practices in augmenting system resilience were shared.

vii. Transparency and User Trust

Another keynote in providing resilience is maintaining user trust through transparency. The revelation of resilience methods and response times, facilities for the protection of users, and other means of care go a long way in managing public expectations and doubts about anticipated outcomes. Institutions are challenged to give adequate information to provide reassurance to users while simultaneously guarding sensitive information that could potentially undermine security.

Operational resilience as a foundation of CBDC cybersecurity renders digital currencies stable and strong even in disruptors. In a word, redundancy mechanisms, strong disaster recovery procedures, real-time monitoring, and collaborative structures guarantee that CBDC systems are well protected from the possible contingencies of a financial institution. These measures protect not only technical infrastructures but also public confidence in CBDCs as a secure and stable foundation of tomorrow's financial system. The chance for central banks and their partners to create robust systems cognizant of the strongly rising demands of this radically changing digital world lies in early planning and forward thinking.

5.5.5. Cybersecurity and Public Trust

Centrals Bank Digital Currencies need public confidence to work and find broad acceptance. It is disquieting, though, that a total of **59.06%** had concerns about the **Data breaches** measures, 59.69% about **Identity theft**, **59.90%** about **Transaction manipulation** and **64.02% System vulnerabilities**, **64.58% Unauthorized access to data**. If this were an area in which transparency were not valued highly, it could bring down that public confidence.

In this respect, trust in financial systems and especially digital innovations like CBDCs is highly dependent on a person's view about security features that exist to protect the transactions and data of the users. The concerns were raised by the respondents that if the cybersecurity protocols remain uncommunicated and undiscussed, skepticism will be evoked that may prevent the persons from adopting and using them. For instance, users may doubt whether fraud protection, identity theft protection, and protection against unauthorized access-one of the most rudimentary ways to safeguard one's financial activities-are comprehensively covered.

These would be a concern over the necessity of calls for increased transparency within cybersecurity practice. In this respect, one would consider:

- Clearly communicating the security policy to the public on encryption, authentication protocols, and system monitoring mechanisms.
- Regular information on the creation of security measures, with special attention to significant emerging threats.
- Public awareness of how cybersecurity mechanisms function, and hence the perception of safety and trust by the general public.

Another related one was the establishment of independent oversight bodies for auditing the state of cybersecurity measures in the CBDC systems and reporting publicly. If such audits were publicly available in easily readable format, this would be a further boost to credibility and institutional commitment toward robust security.

The respondents, on the contrary, pointed out that consultations with the stakeholders on cybersecurity issues include end-users. Public forums, surveys, and advisory panels help discuss user concerns and integrate feedback as the system designs unfold to meet the expectations of the public and institutional strategies.

Another key issue was that of accountability frameworks. Accountability for security breaches, combined with transparency in incident reporting, will give users confidence that the operator of a CBDC is ready and willing to assume its responsibilities if things go wrong. It is also one way of gaining trust in that it affirms commitment to the protection of user interests, even under unfavorable conditions.

In fact, this will directly improve perceived security by means of functions like notifications about unusual activity, along with easier dispute resolution. It puts the user in control and reinforces trust through the perception of being in control of one's financial transactions.

Another important point was that the respondents argued that trust in public is not only a question of

technical security but also of risk and response communication. In other words, in case of data breach or interruption of service, timely and transparent communication reduces speculation, hence reassures users about recovery measures already available.

In a nutshell, transparency about how cybersecurity is done within CBDC systems and perceived reliability would be the basis on which public confidence could be based. Proactive communication of security strategies with involvement, and using accountability frameworks facilitate building and maintaining trust in the commitment of financial institutions to success in the adoption of CBDCs. Thus, the gap between technological advance and public confidence in such systems can be minimized or bridged by an approach of transparency and user focus.

5.6. Convergence of Themes

5.6.1. Balancing Ethical and Security Needs

CBDC implementation presents an interesting meeting point of ethical, compliance, and security issues that demand the realization of a proper balance between protection of individual rights and strict regulatory requirements. In fact, only **9.79%** reported having cybersecurity issues as **Privacy concerns, Operational barriers**, **Fraud and threats**, and these can affect user privacy and strong compliance and cybersecurity requirements. This sets up one of the central dilemmas in the ethical implementation of CBDCs.

More precisely, privacy emerged as an ethical dimension that is often in conflict with compliance frameworks such as AML/CFT/CPF, which demand data gathering. These are regulatory requirements that, while necessary to impede criminal activities, could easily be seen as intrusive and therefore might destroy trust in the use of the CBDC system. Therefore, how CBDC systems will be designed to meet regulatory requirements without necessarily compromising privacy and undermining user autonomy is a challenge.

i. Privacy-by-Design as Solution

Among the participants in the interview questionnaire, three (**37.50%**) supported the application of the privacy-by-design principle as core strategy to balance this trade-off. Accordingly, privacy-by-design embeds privacy protection into the very architecture of CBDC systems at the outset. Such mechanisms would thus be designed by their core features to protect user data by default:

- **Anonymized Transactions:** This would allow the verification of transactions without actually **exposing who was involved in a transaction.**
- **Selective Data Disclosure:** Only enough to be compliant with regulators, while everything else would remain private.
- **Decentralized Data Storage:** Keeps data collections to an absolute minimum and reduces the

risk of data breaches and misuse.

These measures were singled out by the respondents as vital for maintaining the confidence of the users, while meeting the demands placed by the regulatory bodies. As said by the participants, the presence of such features in the system architecture would give more confidence in the technology while being a good balance between privacy and oversight.

ii. *Multi-Layered Security Frameworks*

The respondents also recommended that multilayered security frameworks should be developed that support privacy-preserving technologies. Proposals that exemplify this approach consist of:

- **Zero-Knowledge Proofs:** Enabling the validation of transaction authenticity without disclosing confidential user data.
- **Role-Based Access Controls:** Limiting access to sensitive information to those who will use it, reducing the chances of misuse.

These systems will therefore allow CBDC systems to operate in both an impenetrable and moral manner, respectively addressing all compliance and privacy concerns. These solutions ensure that only necessary information is shared and accessed, maintaining user data integrity while supporting regulatory necessities.

iii. *Global Standards Harmonized*

Another important thread throughout the survey and interviews was the need for collaboration on the part of regulatory bodies, technology providers, and financial institutions. The respondents emphasized the importance of harmonized global standards in closing the gap on privacy protection and compliance requirements. This would ensure better interoperability between systems, reduce the inconsistencies of regulatory practices throughout jurisdictions, and ensure that the implementation of CBDCs is non-discriminatory and transparent.

Harmonized frameworks would also make cross-border transactions much easier, one of the key use cases for CBDCs, and reduce data-sharing and sovereignty issues. The meeting participants underscored that this type of collaboration would call for inputs from all stakeholders: central banks, policymakers, and civil society groups.

iv. *Clear Communication and Inclusion of Stakeholders*

The most relevant determinant for the ethical-security gap was identified as transparency. Clear, understandable communication of how data are collected, stored, and used within the CBDC system is important for trust. It was necessary that users were informed about their rights and protection measures placed with respect to their privacy.

Thirdly, the guideline and policy development with stakeholders involves an ethical yet functional framework. In this respect, the approach of the institution on users, regulators, and technology providers in decision-making creates a system that reflects multiple perspectives with the advantage of predatory concerns.

v. *Analysis of the Challenges between privacy and compliance*

The whole implementation process of CBDC requires a balance between privacy and compliance, which is an essentially complex procedure. Most probably, solutions can be found by allowing viable solutions due to privacy-by-design and multi-layered security frameworks; not all challenges can be avoided.

For example:

- **Technological Constraints:** Cutting-edge privacy-preserving technologies, i.e., zero-knowledge proofs, demand enormous computational power and technological expertise. At a bare minimum, this would render it a significant issue for smaller institutions or technologically less developed regions.
- **Resistance to Regulation:** There may be resistance to the development of harmonized global standards by some jurisdictions due to a reluctance to compromise on sovereignty and data control.
- **Skepticism from the Public:** Public skepticism in this context may persist where there are instances of government overreach or inadequate data protection legislation.

vi. *Way Forward*

Addressing these challenges will require a multi-pronged approach:

- **Investment in Technology:** Financial institutions and central banks should invest in leading-edge technologies that implement features of data protection without weakening system efficiency or compliance.
- **Innovation in Regulation:** Policymakers need to create flexible regulatory frameworks that fit the peculiar CBDC characteristics and further the protection of individual rights.
- **Public Engagement:** It is pertinent to build confidence by way of a right public education campaign with clear information and dispelling misconceptions regarding the use of CBDCs.
- **Global Collaboration:** Standardization must be the outcome of worldwide cooperation, such that CBDCs should be able to operate well internationally.

Finally, there are certain important plans and creative solutions needed in order to achieve a balance in the adoption of ethical and security requirements for CBDCs. The main characteristics are privacy-by-design principles, multi-layered security architectures, and transparency. Security, ethics, and wide-based trust in a CBDC system will be ensured through the establishment of cooperation between stakeholders and investments in technology and public engagement on the part of financial institutions.

This would be a balancing act that is not just necessary for the effective implementation of CBDCs but also for their viability and acceptance in the long run in the overall scheme of the global financial order.

5.6.2. Collaborative Governance

Whereas CBDCs are hailed to be disruptive forces in financial systems, only collaboratively purposed governance mechanisms assure their workability. That, according to 50.00% of respondents, collaborative contributions by the central bank and its regulatory institutions need to concur on ways that define what could be meant as CBDCs. From that, regulatory capture is overcome in a kind manner that seeks consistency with changes in technologies, which also makes service provision adequate according to customers' needs.

i. Shared Accountability and Inclusive Decision-Making

Collaborative governance encourages shared accountability through wide representation within the decision-making processes. This runs from financial regulators down to technology firms, consumer advocacy groups, to central banks within a framework inclusive of diverse input. This approach reduces the possible risks of oversight, which includes missing critical ethical considerations or points of technical vulnerabilities.

According to the participants, inclusivity in governance ensures a balancing of interests and priorities. Such a balance is critical to the design and implementation of CBDC systems that are fully cognizant of their wide ramifications in society, ethics, and technology. In that respect, collaborative governance will keep potential challenges at bay through pooled knowledge from different sectors, consequently strengthening the system.

ii. Tapping Private Sector Knowledge

The most positive sides of collaborative governance involve ways to source private sector knowledge and innovation. Especially companies operating in the blockchain, cybersecurity, and data privacy sectors are able to bring technical know-how contributing to an improved infrastructure for CBDCs. Their participation will result in the development of user-friendly interfaces, system resilience, and advanced mechanisms of data protection.

The participants reiterated that collaboration with the fintech companies would be necessary in making access to CBDC platforms easier and safer. This is because fintech firms can implement state-of-the-art solutions in ensuring that CBDCs are user-friendly but also appealing for use. Their experience in handling digital ecosystems can help central banks and regulators better anticipate and mitigate risks more effectively.

iii. Setting Ethical and Regulatory Standards

In a collaborative governance model, the stakeholders work out the ethical and regulatory standards together and with the legal frameworks. Key Responsibilities:

- **Global Standard Harmonization:** The standards, under a regime of collaborative governance, may get harmonized across the globe. This way, CBDC transfer in cross-border transactions will be easy, allowing for local diversity. There will be resultant assurance of compliance harmoniously and across borders.
- **Monitoring and enforcement:** There need to be oversight mechanisms for enforcing such ethical principles, with a special emphasis on the areas of preserving privacy and facilitating financial inclusion.
- **Risk Assessment and Response:** underpinning this joint work in determining emerging risks, establishing some form of common action concerning cybersecurity threats facing CBDC could raise resiliency within CBDC systems.

iv. Independent Advisory Boards and Public Engagement

A number of the respondents underscored the need for independent advisory boards drawn from both the private and public sectors to oversee CBDC rollout. Such boards would be able to advise on ethical concerns, compliance, and wider societal impacts, ensuring that governance arrangements keep pace with both ethical and operational priorities.

The public also requires openness: the provision of accessible channels for user feedback, whereby end-users can relate directly to governance mechanisms themselves and make regulatory systems more responsive to their needs. This way, the whole process of increased transparency promotes trust and inclusiveness in the CBDC ecosystem.

v. Balancing Innovation and Regulation

Another balance that is needed in the collaborative governance is that of innovation versus regulation. A binding regulatory framework may hamper technological progress. In turn, if there is not enough regulation, systems can fall prey to fraud, data leaks, and financial instability. In collaborative governance, such a balance is possible to achieve when the regulatory knowledge is mixed with technological innovation.

For instance, embedding privacy-preserving technologies in CBDC systems will answer ethical concerns but not at the cost of regulatory imperatives. Likewise, global standards for cybersecurity will ensure resilience in these systems and engender international cooperation.

This is the reason why collaborative governance is basic for successful CBDCs implementation: it works

in such a way that the strengths of central banks, regulatory bodies, and private sector experts are combined to make CBDCs ethical, secure, and efficient. Shared accountability, private sector innovation, and regulatory effort harmonization thus put a strong framework in place to address the complex challenges of CBDC adoption.

Transparency and public engagement further bolster collaborative governance by gaining the public's trust and making sure that it is inclusive. These ingredients fill the gap between innovation, regulation, and people's confidence to allow for the adoption and sustainability of CBDCs in the economy. It is, therefore, discernible that in as long as financial ecosystems are progressively changing, collaborative governance will be continuing to couple technological development with social and ethical concerns.

5.6.3. Future-Proofing System

For any CBDC application to succeed in the long run, it must be scalable, adaptable, and resilient in the face of continuous technological advancements and regulatory shifts. This need for future-proofing is strongly reflected in survey responses, with 57% of participants emphasizing that it is “very important” for CBDC systems to be designed to withstand evolving demands and challenges.

Future-proofing, of course, is much more than simple technical uptakes: scalability, agility, and continuous innovation to make sure CBDCs remain relevant and effective in the ever-changing financial landscape. By integrating these proactive elements, the infrastructure of CBDCs can sustain long-term usability, security, and compliance for continued confidence in digital currency systems.

i. Scalability: Preparing for Increased Demand

The more use of digital currencies, the more those underlying systems in CBDC future-proofing have to be able to manage scalability with volumes of transactions soaring without losing a single ounce of speed or stability. The majority of payment infrastructures today collapse under heavy volumes of transactions, particularly during peak usage hours of the day, which again drives home the need to develop CBDC systems that:

- **Support High Volumes:** CBDC systems must be capable of processing high volumes for an increasing number of customers without generating downtime.
- **Cross-Border Payments:** Interoperability between the national systems of CBDCs is very significant since cross-border payments are crucial to the very existence of international finance.
- **Integrate Emerging technology:** CBDC is to be implemented on each modern payment platform, such as blockchain, digital wallets, and decentralized finance, because of frictionless users' experience.

ii. Agility: Ability to Adapt to Regulatory and Technological Changes

Agility, in addition to scalability, is the cornerstone of CBDCs in keeping up with the fast rate of advancements in financial regulations and technology. According to the responses, there is a need for:

- **Dynamic System Architectures:** Systems must be designed with the ability to accommodate evolution in regulatory requirements, such as AML/CFT/CPF.
- **Implementing Enhanced Cybersecurity Measures:** CBDC system architecture needs to be dynamic in nature so that new defense can be added against new and advanced cyber threats. This includes the use of quantum-resistant cryptography and artificial intelligence to detect threats.
- **Adoption of Cutting-Edge Technologies:** A future-proof system should have the ability to integrate state-of-the-art technological advancements in artificial intelligence (AI), machine learning (ML), and quantum computing to maximize efficiency, security, and overall user experience.

iii. Long-Term Vision and Continuous Improvement

Future-proofing of CBDC infrastructure would need to be underpinned by a long-term vision through ongoing investment in R&D. In particular, the following requirements were emphasized by the respondents:

- **Innovation Centres:** Setup an innovation center where new technologies can be tested and perfected under the most perfect settings before widespread application. Cooperation with academia as well as the innovators within the private sector helps in implementing state-of-the-art solutions.
- **Modular Infrastructure Models:** Embrace modular or cloud-based systems that will support incremental upgrading without the replacement of the whole infrastructure. The strategy reduces costs and minimizes disruption, while allowing for scalability and flexibility of the system.
- **Ongoing Research:** Central banks and financial institutions need to carry on researching on newer methodologies and technologies to get themselves prepared, predict, and handle future issues efficiently.

iv. Stakeholder Collaboration for Future-Ready Systems

It also touched on the cooperation between the stakeholders at higher levels of government, central banks, and businesses in the private sector to international regulatory bodies for the same effect. This would align future-proofing with probable global financial and technological advancements. Some of the proposals according to these needs are:

- **Standardization:** Standardized CBDC design and implementation frameworks allow greater interoperability, which reduces adaptation costs to heterogeneous systems.
- **Global Cooperation:** A partnership with international allies will help address concerns that

transcend geographical borders and guarantee that CBDCs are aligned with worldwide monetary goals.

- **Private-Public Partnerships**: The private innovators take the lead in the technology while regulators will be kept informed.

v. Overcoming Challenges to Future-Proofing

Where necessary, future-proofing is not without its challenges. Let us illustrate this with these following cases:

- **Balancing Innovation and Regulation:** One would not want too much regulatory action that could curtail creativity, nor too little, which would make systems vulnerable to illicit practices and fiscal instability. Interactive governance arrangements are able to ease the attainment of this subtle balance.
- **Resource Constraints:** Budget constraints present obstacles to smaller institutions attempting to invest in infrastructural upgrading to future-proof. Strategies such as public-private partnerships and regulator incentives might provide the necessary funding needed.
- **Cybersecurity Threats:** They would, therefore, as the CBDCs rise in integration into the core of the financial system, be a target for cyber threats. Due care in proactive threat detection and robust incident response are important for operational resilience.

It means that the perpetual success and sustainability of CBDCs are accomplished by constructing future-proof systems: scalability regarding the volume of transactions, flexibility concerning ever-changing regulatory requirements, leveraging innovation in using new technologies. As stated, such features indeed provide a very sound basis for CBDCs, which might be much better prepared against all odds in store for the future, even with collaborative governance, standardization, and public-private partnership.

These, in turn, can be seen as investments by central banks and financial institutions in future-proof measures that provide robust CBDC systems, engendering trust in both users and stakeholders. Besides assuring operational reliability in CBDCs, positioning them at the frontier of global financial innovation and inclusiveness will be achieved. Future-proofing, therefore, is not all about being prepared for the unknown but about making systems adaptable, efficient, and resilient in a changing world.

5.6.4. Impact of Emerging Technologies

The advent of new and innovative technologies, especially blockchain and AI, is continuously transforming the way CBDC is being used. While the emerging technologies have tremendous improvements in terms of transparency, security, and efficiency, they pose a series of compliance, ethical, and growth challenges.

i. *Blockchain: Revolutionizing Transparency and Security*

This renders blockchain technology a foundation in the development of CBDCs because of transparency and security. Blockchain records are immutable, meaning there is a guarantee of integrity of data of the transactions with little, if any, opportunity to alter the already-stored history of the transactions. As much as this aspect would deter fraud, another imperative advantage introduced is giving users confidence because every transaction will be traceable via an auditable record.

Both interviewees and survey respondents remarked on blockchain's potentially revolutionary effect on financial systems, considering its decentralized approach to transaction verification with reduced requirements for intermediaries. We have noted that, the verification of transactions by consensus mechanisms reduces the occurrence of errors, cuts processing time, and decreases the overall cost of cross-border payments.

Blockchains in turn introduce a series of complications derived from their decentralized and, at the same time, unchangeable character-some linked to the fulfillment of certain data protection regulations, such as the European Union's General Data Protection Regulation. In contrast, this demands the right to suppression, better known as the "right to be forgotten", in tension with blockchain's immutability. Several respondents noted that this legal uncertainty demands consideration of hybrid models. These models will combine blockchain's decentralized features with the presence of some central administrator, whereby data can be changed or deleted if certain conditions are met but still retains its intrinsic safety and transparency.

Meanwhile, other vulnerabilities emerge with increased operational security due to blockchain. For example, participants did raise concerns with the scalability aspect of blockchain systems when transaction volumes go up. To make the blockchain more scalable, advanced consensus protocols such as proof-of-stake or sharding can be used without giving up security.

ii. *Artificial Intelligence: Transforming Data Management*

AI is also the other force of change in the application of CBDCs, particularly in the processing volumes of data from digital transactions. Such was the indication, for instance, by 75.00% of respondents who saw the need to have AI-powered tools that make the processes for compliance with AML/CFT requirements less onerous. Machine learning algorithms can analyze transactional data in real time, recognizing suspicious patterns and flagging illicit activity in ways that are superior to traditional methods.

Com plaintive uses go beyond that. AI-driven behavioural analytics can improve fraud detection by spotting behaviour that is out of the pattern for a specific user's behaviour. These are proactive means of improving security, enabling an institution to nip an emerging threat in its bud. Respondents also

noted AI can help improve overall operational efficiency through automating routine tasks, such as monitoring transactions and customer service.

Meanwhile, the deployment of AI in a CBDC system also has ethical issues. Algorithmic transparency and fairness are some of the major concerns here. In this respect, the interviewees show apprehensions regarding how biased AI tools could be if the datasets or algorithms were defective. For example, a biased algorithm might flag disproportionate numbers of transactions coming from particular demographics or geographic regions as suspicious, which is uncalled for. These are biases that strict testing, continuous monitoring, and ethical oversight can ensure AI systems are free of, and that their applications remain equitable. Solving Challenges of Ethics and Compliance will therefore create a very delicate balance between innovation in the features and compliance with regulatory requirements for the integration of emerging technologies into CBDC systems.

What became underlined is a need for further clarification of the ethical use of AI and blockchain for transparency in how these technologies are used. For example, it would be required that the institutions show what criteria were used by algorithms for flagging transactions and provide mechanisms for users to raise objections against decisions perceived as unfair.

In this respect, the collaborative governance models highlighted here represent a critical strategy for trying to handle such challenges. As regulators, technologists, and consumer advocates together build and oversee CBDC systems, institutions can ensure that emerging technologies are implemented in a way that reflects ethical principles and regulatory requirements.

This, of course, goes hand in glove with a greater standardization of blockchain and AI protocols across jurisdictions, thereby easing interoperability across borders while lowering compliance costs. For instance, a set of international standards regarding data privacy, security, and algorithmic transparency would provide guidance about how CBDCs should be implemented to ensure that ethical and operational parameters are uniform.

iii. Hybrid Systems and Privacy Preservation: Recent Developments

New technologies open up new avenues of innovation in the design of CBDC. Hybrid blockchain models are another promising avenue, still in its infancy, to strike a balance between transparency and privacy. These are combinations of the decentralized advantages of blockchain with centralized oversight that may allow regulators selective visibility into data while safeguarding user privacy.

Similarly, technologies enhancing privacy such as zero-knowledge proofs that allow verification of

transactions without leaking sensitive information have a very promising outlook for the solution of the privacy-compliance paradox.

iv. Stakeholder Collaboration and Future Outlook

The research showcased the potential success of harnessing emerging technologies through the cooperation of all stakeholders. Central banks, technology providers, and regulators need to collaborate in order to create a framework that can maximize benefit and minimize risk for both blockchain and AI. There was also focus on ongoing investment in research and development by the respondents in order to remain ahead of emerging technological trends and cybersecurity threats.

Looking forward, the incorporation of emergent technology into CBDC systems will rely on the successful trade-offs they can achieve in scalability, security, and compliance. Future work in modular blockchain architectures and explainable AI is highly promising, given the nature of these challenges. A culture of ethical innovation and cooperation will ensure that CBDCs not only meet current needs but continue to be resilient and responsive to the challenges that are yet to arise.

But the incoming innovative technologies in blockchain and AI might completely reshape the CBDC systems into more transparent, secured, and effective ways. All the same, their onboarding process has to be steered by solid ethical principles grounded in strong structures of compliance. Data privacy issues, scalability issues, and questions of algorithmic fairness hang around. It calls for all institutions to adopt innovative solutions, guarantee coordination among stakeholders, and maintain ethical standards to achieve the highest possible potential of the available technologies so that CBDCs act as an enabler of a secure, inclusive financial system.

5.6.5. Cybersecurity Threats and Responses

It has increased the need for stringent cybersecurity controls with the rise of CBDCs. It is not just the disruptive characteristics of CBDCs related to payment systems, but they also expose financial institutions to new risks. The gamut of threats varies from those facing systemic integrity, such as cyber attacks, to compromises in user confidentiality. The integration of the technology in digital currency and cybersecurity demands a holistic response to sophisticated technology for protective measures, human monitoring, and strategic partnerships in the interviews.

i. Emerging Cybersecurity Threats

CBDCs operate in a highly networked digital space and are therefore vulnerable to sophisticated cyberattacks. Interviewees in the interviews singled out attempts at hacking to take advantage of system weaknesses as being of concern. Institutions early on in CBDC development and implementation simulated cyberattacks on their defenses and identified vulnerabilities in communication protocols and

redundancies in systems. Pilot program penetration testing, for instance, identified exploitable weaknesses in the authentication layers that could then be used to access sensitive financial information unauthorized.

Yet another paramount threat presented on top of the above was that criminal parties can attack via ransomware, whereby CBDC platforms are hijacked and access is only granted upon payment of a certain amount. Distributed denial-of-service attacks were also depicted as threats because they would take CBDC systems out of their availability and undermine users' confidence in financial stability. These emerging risks make it abundantly evident that strong and secure security measures need to be embedded in the design of CBDC.

ii. *Proactive Cybersecurity Responses*

Such kind of threats necessitates the need for financial institutions to be agile in the improvement of their cybersecurity. It is here that elliptic curve cryptography, among other emerging techniques, became the state of the art for encrypting transaction data and, broadly speaking, communications. While these cryptographic techniques were more secure, they had added benefits of being computationally efficient and thus suitable for large volumes.

These CBDC infrastructures also have real-time threat-detection systems powered by artificial intelligence. The systems under perpetual surveillance of transaction patterns and system activities look for any anomaly that could raise a red flag as a warning of a breach. AI algorithms can detect unusual transaction patterns differing from set baselines, allowing the institutions to act swiftly in order to contain potential threats.

The participants rendered the zero-trust security framework highly essential; that is, no system component or user is deemed trusted. The model would have rigorous verification mechanisms at all points of access, with only authorized and authenticated entities allowed to communicate with the CBDC system. To a great extent, suggestions have been put forward on having multi-factor authentication mechanisms in place for enhancing access controls, where users need to authenticate their identities using multiple layers of authentication.

iii. *Institutional Strategies for Cyber Resilience*

The interviews also identified the importance of continuous monitoring and regular security audits in ensuring cyber resilience. Thus, continuous monitoring helps the institutions to detect and respond to

threats in real time and therefore minimize the possible effects of the attacks. Regular security audits, such as penetration testing, assisted in identifying and preventing vulnerabilities from being exploited by attackers. The audits make CBDC systems robust and sufficiently agile to act against developing cybersecurity threats.

The most prevalent institutional cybersecurity practices documented in literature are training and awareness programs for employees. The interviewees highlighted the need to provide the workforce with the skills to detect and respond to new threats. The interviewees argued that it will be important to equip the workforce with the relevant skills of detection and response towards new threats. These cybersecurity training programs include phishing attempt detection, vulnerability awareness in ransomware attacks, and data protection best practices. Therefore, a culture of vigilance and responsibility is instilled within the financial institution.

iv. Collaboration and Standardization

Participants in the roundtable emphasized that cybersecurity threats have a multistakeholder dimension at various levels, including central banks, technology providers, and regulatory bodies. There is a greater need for standardization of cybersecurity frameworks in order to ensure coherence and interoperability across borders. This will implement consistent security practices, allow cross-border cooperation, and raise the general resilience of the financial system against dynamic cyber threats. They would define best practices on encryption, threat detection, and incident response establishing a consistent way towards securing CBDC systems.

The solution, in this instance, is in those public-private partnerships that will bring innovation in cybersecurity. Such partnerships with the technology firms that are experts in blockchain, AI, and cybersecurity enable the financial institutions to obtain cutting-edge solutions in their defenses. Collaboration between the public institutions and private organizations will also promote sharing threat intelligence, so that the stakeholders remain ahead of threats.

v. Balancing Security and Usability

While cybersecurity can't be overlooked, respondent institutions also cited the need to strike a balance between security and accessibility for users. Otherwise, very complex security features might actually discourage people from adopting CBDCs, especially those not fully literate in using the technology. In this regard, institutions are looking at user-friendly security features, including biometric authentication and seamless MFA processes. These measures provide strong protection without damaging the user

experience. The other point is transparency: cybersecurity practices were also underlined as being of utmost importance in ensuring public confidence. Respondents supported the idea of clear communication on how the user data is protected and how institutions respond to possible breaches. Show users that information about measures being taken toward cybersecurity helps in building trust in the safety and reliability of CBDC systems.

vi. Future Directions

Going forward, institutions need to stay ahead of such a changing cybersecurity environment. One such proactive step for CBDC systems was the incorporation of quantum-resistant cryptographic algorithms that would insulate them from the future threat of quantum computing. Additional opportunities are available with growing developments in the area of AI and machine learning, providing means to further enhance the capability of detection and response. With CBDCs being more integrated into the world's financial systems, it can't be overstressed enough that robust cybersecurity be taken into account. This can be through the newest technological protection implementations, partnering and sharing, and putting emphasis on education of the users so that by design, the system is safe and resilient. Essentially, this will eventually guarantee the integrity of virtual currencies to attain the trust required for wide acceptance and success.

We then confirm that cybersecurity is among the cornerstones of CBDC implementation, which forms the foundation for public trust and system integrity. They reiterate the demand for more sophisticated encryption, real-time monitoring, and collaborative frameworks that will successfully bear emergent threats. Through their innovation and enhancement in cybersecurity, the institutions are therefore paving the way toward a secure and sustainable digital currency system that can meet needs in an ever more connected financial world.

5.6.6. Regional Variations in CBDC Adoption

The trend in the adoption and implementation of CBDCs varies strongly between regions, with some reflecting differences in the development of digital infrastructure, financial literacy, and governmental priorities. These are more than technical issues but indicate larger socioeconomic and geopolitical factors at play in how different nations decide on CBDC strategies. It also illustrated, using the same interview and questionnaire data, the difficulty of adapting the frameworks of CBDCs to disparate regional needs and therefore showed one important need: namely, adaptive, inclusive, and region-specific approaches.

i. *Advanced Regions: Accelerated Adoption in East Asia*

Countries with advanced digital infrastructures-including East Asia-have witnessed rapid adoption of CBDCs. To illustrate this, the pilot program for the Chinese digital yuan is riding on strong smartphone penetration and some of the most widespread digital payment ecosystems, such as WeChat Pay and Alipay. According to interviewees, these systems provide a ground layer to enable the smooth integration of CBDCs with little disturbance.

Governmental support has also played an important role in those areas. Policies toward digital transformation, combined with a culture of technological innovation, accelerated CBDC implementation. Availability of 5G networks and high levels of digital literacy mean that users were ready and accepting of the new currency. Even in advanced regions, though, there remain difficulties to be overcome-for instance, ensuring privacy protection and international regulatory conformity of CBDCs.

ii. *Developing Regions: Barriers in Sub-Saharan Africa*

Meanwhile, Sub-Saharan Africa remains one of those regions with multiple serious hurdles on the way to implementing CBDCs. The poorly developed digital infrastructure, unsecured access to the Internet, and the relatively low extent of smartphone diffusion comprise some larger barriers toward progress.

Interviewees emphasized that these technical challenges exacerbate financial exclusion among already underserved populations, eroding one of the main visions for CBDCs: the improvement of financial inclusion.

A typical example is most rural areas in Sub-Saharan Africa, specifically in Mali, Burkina Faso and Nigeria, where basic feature phones and offline cash-based transactions are the norm. According to respondents from such regions, offline-capable CBDC solutions can help address the gap in this regard. Moreover, such a system will require educational campaigns to increase financial literacy by reducing misconceptions and building public trust in digital currencies.

In addition, many governments in these regions face resource constraints that make investment in intensive infrastructure upgrades hard in several aspects of CBDC implementation. In this respect, respondents suggested that partnerships with international development organizations and private technology firms could bring support in many of the relevant areas.

iii. *Implementation Strategies-Tailored*

The regional differences in CBDC adoption also bring to the fore the need for country-specific implementation strategies that address peculiar requirements and problems within the different markets. In less digitally literate areas, the focus of institutions is on educational programs to acquaint users with the functions and security associated with CBDCs. For instance, training classes in vernacular languages and picture charts can help to make CBDC systems more user-friendly to non-technologically savvy people.

Infrastructure development also takes center stage in underdeveloped areas. Indeed, the respondents believed in finding ways to establish public-private partnerships that finance and develop necessary digital infrastructures comprising investments in the expansion of mobile networks, affordable smartphone distribution programs, and energy-efficient data centers that host the CBDC system.

The interviewees also advocated for scalable models of CBDC that would grow and mature with the regional infrastructure. For instance, using a modular design approach; institutions can deploy basic functionalities in regions where the capabilities are poor while scaling up if and when the conditions in the economy improve.

iv. *The Role of Policy and Governance*

Any CBDC trajectory is of necessity highly entwined with governments. In the regions of proactive governmental support, such as that of East Asia, innovation-friendly policy and collaboration between public and private sectors have created a conducive environment for the development of CBDCs. Where regional policy frameworks are fragmented or incoherent, developments have been more slow-moving.

Respondents emphasized that regional policies and regulations should be harmonized to align with international standards that support cross-border CBDC transactions. This, for example, would be taken to mean uniformity of CBDC policies across economic union regions-for example, the WAMZ region-in a way that solves interoperability issues, or otherwise, at lower implementation costs.

v. *Lessons from Regional Disparities*

Various experiences of different regions in taking up CBDCs provide interesting insights into best practices and pitfalls. Advanced regions show the benefits that can be derived from leveraging existing ecosystems for digital technology in place and also from aligning CBDCs with user expectations. Developing regions bring to light that gaps in infrastructure and literacy must be correctly identified to make sure about inclusivity.

These lessons impress the need for flexibility in design and implementation. Central banks should, according to respondents, pursue a CBDC implementation strategy that first puts pilot projects into place to allow the testing and adjusting before full implementation. This will enable them to solve real-time problems and, at the same time, collect feedback from users and stakeholders.

vi. Shared Solutions

To this end, cooperation across regions, international organizations, and private technology companies can be an incentivizing factor in squaring up disparities in regional CBDC adoption. Advanced regions share technological experiences and lessons learned with developing regions, while international organizations support them with financial and technical aid in bridging resource gaps.

However, the respondents also supported regional CBDC working groups to share experiences and coordinate views. These groups would discuss the development and refinement of regional protocols and solutions with interoperability considerations in mind.

These regional differences in CBDC adoption reflect a broader disparity in infrastructure, literacy, and policy frameworks. Advanced regions can show the potential for seamless integration when digital ecosystems and government support align. In contrast, developing regions highlight the challenges of building an inclusive CBDC system in resource-constrained environments.

The implementation needs to be institution-specific, adapted to the needs, and of an inclusive nature in respect of infrastructure development, education, and regional collaboration. In so doing, CBDCs draw from various experiences around different regions and further encourage global partnerships that would realize their full potential for better financial inclusions, improved systems of payments, and economic growth within diverse contexts.

5.6.7. Advancing AML/CFT/CPF Protocols

The game-changers in the fight against financial crime are CBDCs. In a more detailed fashion, CBDCs promise improved protection against money laundering, the financing of terrorism, and proliferation. Just think about what has been stated in terms of inherent transparency or traceability for CBDC transactions, which itself would be one important reason whereby banks and financial regulators get better grounds to try to detect and hamper undesirable financial practices. It's not, however, all smooth sailing. We have to be creative and work together in making the most of these new tools while protecting people's privacy and keeping things running efficiently. In 1970, the United States enacted the Bank

Secrecy Act in order to fight money laundering caused by drug cartels[79]. The law obliged US financial institutions to report cash transactions of $10 000 or more per day and suspicious activity reporting to FINCEN. Aside from those, the law mandated CDD, staff training, and record-keeping up to five years. After the September 11, 2001 attacks, the U.S. tightened up its AML regime with the Patriot Act. The law reinforced KYC and the cross-border monitoring of transactions. These moves set the pace for what today is globally regarded as AML/FT compliance, thereby making regulatory frameworks an important ingredient. As many countries in the world began initiating similar measures, the Financial Action Task Force was established in 1989 during the G7 summit in Paris.

The 40 Recommendations laid down by the FATF have formed the basis of most of the AML/CFT systems across the globe[80]. For example, Mali and Burkina Faso went a step further to implement these recommendations by amending their legal and regulatory frameworks, thus creating an enabling environment for e-money and CBDCs.

i. *AML/CFT/CPF Legal Obligations of Financial Institutions and Electronic Money Issuers (EMEs)*

The platforms of e-money and CBDC are high risk from money laundering and terrorism financing during the placement and layering stages. To mitigate these risks the legislation of Mali and Burkina Faso require robust AML/CFT compliance programmes. A recent Burkina Faso law specifies that:

"Financial institutions must develop and implement harmonized programs for preventing money laundering and terrorist financing".
These programs include:

- Rigorous KYC procedures for both regular and occasional customers.
- Keeping a record of customer documentation in detail.
- Continual monitoring and reporting of suspicious or unusual transactions.
- Systemic filing of suspicious activity reports with authorities such as the CENTIF.
- Identification and monitoring of PEPs.
- Freezing of assets for sanctioned individuals.
- Stringent management of cross-border correspondent banking relationships.

Risk-Based Approach

[79] https://www.fincen.gov/resources/statutes-and-regulations/bank-secrecy-act
[80] https://www.fatf-gafi.org/content/dam/fatf-gafi/recommendations/FATF%20Standards%20-%2040%20Recommendations%20rc.pdf

An effective AML/CFT compliance system begins with a risk assessment. In other words, the institution must classify its customers, products, and services into money laundering and terrorist financing risk categories. FATF has recommended this risk-based approach so that resources are used effectively on the highest-risk areas.

In addition, considering the rapid increase nowadays in the usage of e-money and CBDCs in both Mali and Burkina Faso, digital vulnerabilities and cybersecurity risks need to be included in the risk assessment process. Relevant factors contributing to low risk, particularly for these risks, are infrastructure security, data protection, and monitoring cross-border transactions.

ii. *AML/CFT/CPF in the Context of E-Money and CBDC*

The wide diffusion of E-Money, together with the growing use of CBDCs, presents a huge challenge in the area of AML/CFT/CPF and Country Financial Law.

The regulatory frameworks for AML/CFT in Mali and Burkina Faso are based on the FATF recommendations and regional directives of the West African Economic and Monetary Union (WAEMU)[81]. The issuance of WAEMU Directive No. 02/2015/CM/UEMOA gave impetus to national AML/CFT laws underlining customer due diligence, monitoring of financial transactions, and risk-based approaches. Those measures have evolved with the growth in digital financial services and need to be adapted to deal with the new risks that E-Money and CBDCs pose.

In Mali, **Law No. 2016-008** and its most recent one, the ordinance **No. 2024-011/PT-RM of August 30, 2024, regarding the AML/CFT/CPF**, provide the legal framework for the fight against money laundering and the financing of terrorism. On its part, **Burkina Faso's Law No. 036-2015 is in line with WAEMU** directives in order to observe international standards. The two countries have equally created financial intelligence units the CENTIF in Mali and Burkina Faso who have the mandate to investigate suspicious activities and enforce compliance measures.

The Role of E-Money and CBDC in Financial Inclusion

[81] https://www.fatf-gafi.org/content/dam/fatf-gafi/fsrb-mer/GIABA-Mutual-Evaluation-Mali-2019.pdf.coredownload.inline.pdf
https://www.fatf-gafi.org/content/dam/fatf-gafi/fsrb-fur/GIABA-FUR-FR-Burkina-Faso-2021.pdf
https://documents1.worldbank.org/curated/en/825181468021012685/pdf/700700ESW0P1150urkina0Faso0May02011.pdf
https://www.afdb.org/sites/default/files/documents/projects-and-operations/multinational_-_capacity_development_project_on_anti-money_laundering_and_combating_the_financing_of_terrorism_in_west_africa_transition_states_cd4aml-cft_-_project_appraisal_report.pdf

In this respect, Mali and Burkina Faso have been at the forefront in expanding financial inclusion in electronic money platforms, with most offering mobile money services that allow customers to make payments, store value, or obtain credit without relying on bank-based structures. So CBDCs are also expected to complement these platforms as safe and regulated media for the exchange of value while, as stated, functioning at their core as digitized forms of central banking fiat money.

However, the wide adoption of those technologies also brings vulnerabilities; the anonymity and speed in digital transactions make them quite attractive for illicit activities related to money laundering and terrorist financing. Such risks require mitigation through deep knowledge of the regulatory landscape, supported by state-of-the-art compliance frameworks.

Regulatory Challenges Posed by E-Money and CBDCs

1) **Anonymity in Transactions**

E-money platforms facilitate mostly small and frequent transactions, which can make it difficult to establish the origin of funds. Similarly, CBDCs may be designed with features that allow for pseudonymity, making it difficult to trace the origin of the funds flow. Such anonymity presents the biggest hindrance in determining and observing high-risk individuals and transactions.

2) **Cross-Border Transactions**

Mali and Burkina Faso are bordered by high-risk jurisdictions such as Niger and the conflict zones of the Sahel region. Due to this ease of cross-border transfer of digital currencies, these platforms can equally be exploited for terrorist financing and other illicit activities.

3) **Decentralized Networks**

Because many e-money systems are operated through de-centralized agents and vendors, difficult for regulators to enforce compliance; the implementation of CBDC may alleviate some of these challenges by centralizing the monitoring of transactions, but concerns remain regarding its effective implementation.

4) **Proliferation Financing Risks**

It has been considered that digital platforms might be used to finance the proliferation of WMD. If compliance measures are weak, there will be a very easy way for persons and entities to abuse the digital platforms for these purposes.

iii. *Regulatory Frameworks and Compliance Measures*

1) Customer Due Diligence (CDD)

CDD is part of the founding concepts in money laundering and combating terrorism financing in order to let financial institutions stay within the limits of safety and transparency. Meanwhile, however, both countries-Mali and Burkina Faso-have implemented regulations that force the same obligation upon all financial services providers, such as E-Money operators, as one mechanism of tamping down on crime and raising observance with the AML/CFT regime.

These include measures that necessitate institutions to have sufficient processes for customer identification and verification before the establishment of a business relationship or in cases of a transaction above threshold limits. Key elements of a sound CDD framework include:

- **Customer Identification Program (CIP):** Verification of the identity of customers and beneficial owners through effective KYC processes.
- **Ongoing Monitoring:** Ongoing regular monitoring of customer transactions in order to detect suspicious patterns that could indicate money laundering or terrorist financing.
- **Appropriate assessment of customer risk:** Customer risk profiling to determine the level of vigilance.
- **Record-Keeping:** Institutions must maintain customer records and transaction histories for a specified period as mandated by local and international regulations, ensuring compliance and facilitating investigations if needed.

The issuance of CBDCs will require further actions to prevent misuse of such digital currencies. More stringent CDD measures, including biometric identification and blockchain analytics, can bring more transparency and security.

2) Risk-Based Approaches

A risk-based approach allows financial institutions to use their resources effectively by focusing on high-risk areas. This is especially topical for E-Money and CBDCs, where the number of transactions can overwhelm compliance systems. The main elements are:

• Risk rating of new products and services.

• Categorization of customers, transactions, and geographical regions based on their risk level

• Application of enhanced due diligence measures for high-risk customers, including PEPs and individuals in conflict zones.

3) **Transaction Monitoring and Reporting**

Financial institutions in Mali and Burkina Faso have to monitor transactions for suspicious patterns and report to their respective CENTIF. E-Money and CBDC platforms can have real-time monitoring systems integrated with machine learning algorithms to enhance detection capabilities. Thresholds for reporting can also be set up, along with automated alerts, to make compliance processes smoother.

4) **Public-private partnership:**

Effective AML/CFT compliance cannot be achieved solely by regulators and financial institutions; rather, it is best achieved through the combined effort of different players such as regulators, financial service providers, law enforcement, and technology companies. This will deliver a more robust financial system with clearer identification of financial crime, better prevention, and swift response. On the African scene, in particular, West Africa, such initiatives as the West African Digital Financial Compliance Task Force are important in harmonization efforts on AML/CFT within the region. These initiatives encourage the collaboration of both the public and private sectors in promising ways to improve information-sharing practices through better communication channels between financial institutions and regulators, developing advanced compliance solutions, standardizing regulatory approaches, and fostering capacity building.

iv. Enhanced Transparency and Traceability

The major benefit the CBDC affords is the creation of auditable, unalterable records of transactions. This comes across from interview data as one of the ways in which stakeholders viewed the furtherance of AML/CFT/CPF efforts. In this way, there is a limiting of money laundering, terrorism financing, and proliferation financing, as tracking and auditing each and every transaction in real time will grossly reduce opportunities for such illegal activities. This is highly valuable in cross-border transactions, where anonymity has conventionally been a real stumbling block. Adding CBDCs to international payment systems promotes smooth tracking and ascertains that all participants follow uniform compliance practices. Nevertheless, respondents underscored the need for interoperability between CBDC systems to ensure smooth global cooperation on combatting financial crimes.

v. Applying Advanced Technologies

Advanced technologies, like machine learning and artificial intelligence, are being resorted to by financial institutions in order to be able to cope with the huge volumes of data from CBDC transactions. These tools make it possible for real-time analysis of the patterns of transactions, identifying anomalies that can point out suspicious activity. For example, ML algorithms flag such transactions that fall outside

established behavioural norms; such as sudden spikes in transaction volumes or frequency of transfers to high-risk jurisdictions.

The interviewees pointed out that predictive analytics enhanced the pace at which AML/CFT/CPF programs were pursued. According to them, predictive models allow those institutions to detect risks before they can happen and thus take pro-active action by freezing accounts or referring suspicious cases for deeper scrutiny. Refining these technologies continually to keep pace with the adaptive methods of financial criminals was also something that the respondents believed in.

While the transparency of CBDCs aids in regulatory oversight, it creates concerns about user privacy. As identified by respondents, over-collection of data and electronic surveillance could damage public confidence in CBDC systems. The balance between transparency and privacy is thus a vital challenge in the furtherance of AML/CFT/CPF regimes.

Some of the strongest responses were calls for privacy-enhancing technologies such as zero-knowledge proofs and homomorphic encryption. These are technologies that can enable institutions to verify certain transactions without necessarily exposing the sensitive information of users. For example, zero-knowledge proofs will make compliance checks possible without exposing who the users are, thus their privacy rights are not breached while their activities remain in compliance with set regulatory requirements.

vi. Regulatory Harmonization and Collaboration

The global nature of the crimes necessitates a harmonized approach in handling AML/CFT/CPF. Indeed, respondents have pointed to a need for harmonization of regulatory frameworks across jurisdictions to accommodate efficient cooperation. Inconsistencies in national regulations open compliance gaps, which criminals can then exploit and which will weaken the integrity of CBDC systems.

The establishment of international standards for compliance of the CBDC was suggested by respondents to address this issue. Such standards should cover matters such as data sharing, transaction monitoring, and enforcement mechanisms. Some also advocated for a governance model that is collaborative between central banks, regulatory authorities, and private sector stakeholders in ensuring a uniform direction for AML/CFT/CPF efforts.

vii. Institutional Challenges and Recommendations

CBDC into AML/CFT/CPF systems is hugely challenging for the financial institutions in the present scenario. Most of them lack infrastructure and capacity for real-time monitoring of transactions. These

include, amongst others, high implementation costs, limited technical expertise, and resistance to change.

In addressing these challenges, participants suggested the following strategic interventions:

- **Capacity Building:** Institutional capacity building through investment in training programs that develop skilled compliance teams able to manage sophisticated analytical tools and interpret transaction data effectively.

- **Public-Private Partnerships:** Collaboration between public and private sectors could help drive innovation while lowering implementation costs. For instance, central banks can extend technical support and funding to smaller institutions to ensure equitable access to CBDC compliance tools.

- **Public-Private Partnerships:** Compliance systems can be built in modular form. It would, therefore, facilitate scalability whenever transaction volumes increase. Moving ahead, cloud-based platforms and AI-based analytics tools will emerge as reasonably priced solutions for processing large datasets.

viii. *Ethical Implications*

This also raises ethical issues concerning the integration of CBDCs into AML/CFT/CPF frameworks. The well-grounded concerns of the respondents included, among other things, potential misuse of the transaction data for purposes other than that of the regulator, unauthorized surveillance, and even discrimination.

Equally important, however, will be transparency about the handling and sharing of data. Response lines indicated a need for clear data governance policies regarding the scope of data collected, stored, and used. It should be communicated to users in a very usable manner to account for informed consent.

ix. *Case Studies*

1) Case Study: Mobile Money in Mali

At more than 60% of the population currently using the service, mobile money services have been strongholds of financial inclusion in Mali. On the other hand, this rise in mobile money usage has seen fraud and money laundering cases jump.

For example, during the course of 2022, the Malian CENTIF reported a spate of fraudulent transactions, one of which involved anonymous wallets. Mobile money operators are fighting these risks by

demanding higher KYC requirements for subscribers and enhancing their monitoring systems for transactions[82].

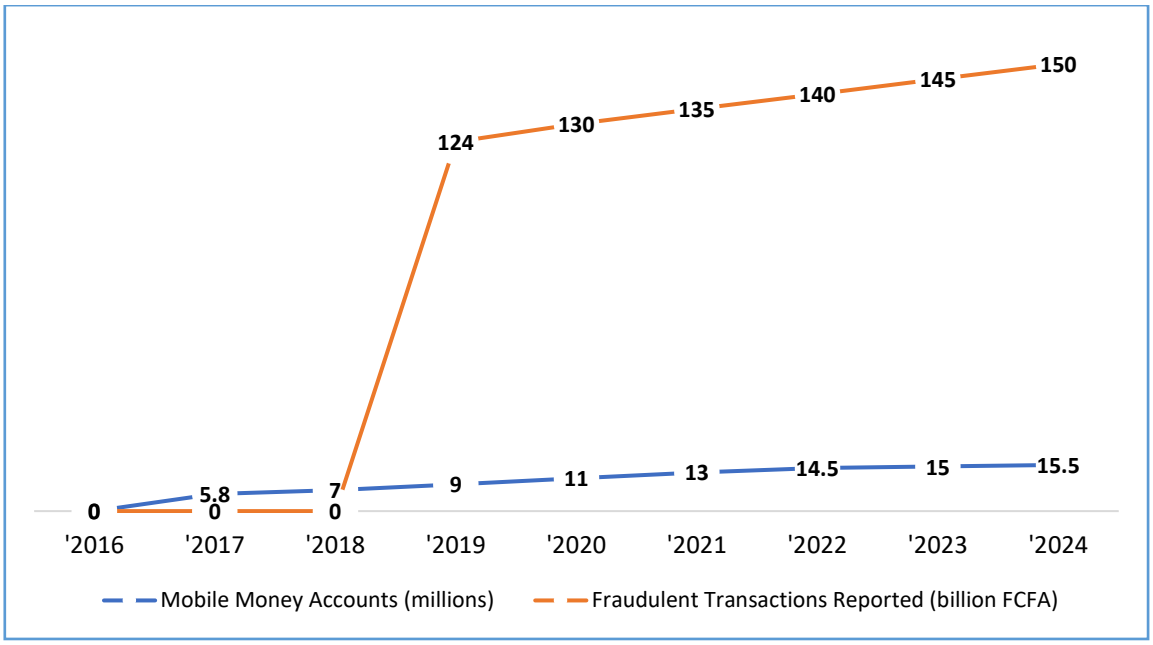


Figure 30: Mobile Money Usage and Reported Fraudulent Transactions in Mali (2004-2024)

2) Case Study: Blockchain Analytics in Burkina Faso

It has been in the forefront in addressing AML/CFT risks of online financial services before. Among those, in 2023, the government initiated a program to incorporate blockchain analytics into its compliance system. The technology enables financial institutions to track the source of funds and detect suspicious transactions in real time. The program has been significant in detecting money laundering associated with cross-border transactions[83].

x. *Emerging Trends Based on Findings*

1) Integration of Artificial Intelligence (AI)

AI-based tools are increasingly pertinent to the design optimization of compliance frameworks. They have the capacity to process big data, identify patterns, and foresee risks. AI in E-Money and CBDC

[82] https://www.ecofinagency.com/telecom/0306-45581-mobile-money-subscribers-surge-150-in-mali-over-five-years
https://www.maliweb.net/insecurite/blanchiment-de-capitaux-et-financement-du-terrorisme-au-mali-des-operations-suspectes-de-plus-de-124-milliards-recensees-en-2019-2917998.html

[83] https://www.bearingpoint.com/en/about-us/news-and-media/press-releases/the-finance-ministry-of-burkina-faso-traces-development-funds-by-using-blockchain-technology/
https://www.merklescience.com/enhancing-anti-money-laundering-efforts-with-advanced-blockchain-analytics

platforms can facilitate real-time risk assessment and automate compliance procedures, thus lessening the burden for financial institutions.

2) **Regional Harmonization**

Harmonization of AML/CFT regulations across all WAEMU member states will go a long way in dealing with cross-border risks. BCEAO has been very instrumental in leading uniform compliance standards and fostering cooperation amongst member states. The next efforts should be channeled towards building a centralized database of SARs to share information effectively.

3) **Strengthening Regulatory Oversight**

As E-Money and CBDCs continue to advance, regulators will need to modify the mechanisms of their supervision. This entails the revision of legal frameworks, investment in state-of-the-art monitoring systems, and capacity building of financial intelligence units. Regular audits and compliance checks can ensure that financial institutions adhere to AML/CFT/CPF standards.

The adoption of E-Money and the prospective introduction of CBDCs represent a tremendous step in the direction of promoting financial inclusion for Mali and Burkina Faso; still, these innovations open up new risks to AML/CFT/CPF compliance frameworks. Such an endeavor requires a multi-faceted approach that involves rigorous regulatory measures, innovation from the technological standpoint, and regional cooperation.

Advanced technologies such as blockchain analytics and AI could help financial institutions enhance their compliance ability and reduce risks effectively. Public-private partnerships and a harmonized regulatory environment will further reinforce security and make the financial ecosystem more transparent. Commitment to the standards of AML/CFT/CPF by every stakeholder will therefore be very critical in safeguarding the integrity of the financial system that will provide for sustainable development with the future growth of digital financial services.

The coming of CBDCs therefore presents one leap forward in bringing efficiency in AML/CFT/CPF protocols. Transparency and traceability of CBDCs thus introduce crucial power in combating financial crimes, while advanced technologies such as AI and ML allow better risk management. Realizing this full potential of CBDCs presents formidable challenges: infrastructural limitations, regulatory inconsistencies, and ethical dilemmas.

It provides an avenue for building robust AML/CFT/CPF systems through fostered collaboration among stakeholders, harmonization of regulatory frameworks, and leverage of privacy-preserving technologies. These efforts will not only strengthen the integrity of financial systems but also position CBDCs as a cornerstone of ethical and effective digital finance.

5.7. Synthesis of Findings

5.7.1. Theoretical Implications

The development of CBDCs creates an unparalleled interest across academia and industry for the multi-dimensional consequences on financial systems, ethics, compliance, and cybersecurity that CBDCs have. This survey and interview data highlight key messages that extend very substantial contributions not only to operational knowledge but also to theoretical constructs that guide digital currencies. These are novel contributions to knowledge, informing policy, and influencing practice in this developing area of study.

i. Key Insights: A Holistic Perspective

The key themes emerged on privacy and data protection, financial inclusion, transparency, user autonomy, institutional preparedness, cybersecurity, and compliance challenges. Each of them speaks to a core part of the broad ethical, operational, and regulatory CBDC landscapes. Considered together, they reveal the fundamental interaction between technical change, governance, and societal consequence in the digital currency landscape.

For instance, the emphasis on privacy and data protection-identified as "critical" by **73.47%** of the surveyed-falls squarely within more general discourses on ethical usages of technologies. The data indicates that while technologies of privacy preservation, such as zero-knowledge proofs, are important, they need to balance rigorous compliance requirements, bringing individual rights into tension with state obligations. This balance raises a series of theoretical questions about how digital financial ecosystems can balance these competing imperatives in a manner that promotes trust.

Similarly, financial inclusivity was ranked as "important" or "extremely important" by **61.86%** of the respondents and emphasized offline functionality and digital illiteracy. These aforementioned challenges put a demand on human-centered design approaches with innovative delivery models and, thus, open fertile ground for theoretical investigation on socio-technical systems that bridge the digital divide.

ii. Theoretical Contribution

1) Reconciling Privacy with Compliance:

One of the most important theoretical contributions of this work is the suggestion of privacy-by-design frameworks for balancing user autonomy with regulatory obligations. Such frameworks propose a new paradigm for the trade-off between transparency and confidentiality by embedding privacy safeguards within the very architecture of CBDCs. It extends the discussion of ethics in digital finance and indicates the way to reconcile the goals of individuals and institutions.

2) Operational Resilience as a Systemic Imperative:

The emphasis on operational resilience by **37.50%** of interview respondents extends the understanding related to system stability. CBDCs, being essential infrastructures within finance, should provide a redundant mechanism for disaster recovery procedures. This perspective underlines a systems theory approach that interprets adaptive and resilient systems as more likely to absorb shocks. This theoretically underlines how perspectives might be shifting from static resilience models to more dynamic frameworks that can provide predictive analytics with real-time responses.

3) Collaborative Governance Models:

Governance was a key theme, with 75.00% of respondents calling for collaborative / cooperation models between central banks, regulators, and private sector actors. This suggestion aligns with theories of multi-stakeholder governance, which contend that more inclusive decision-making is more legitimate and effective. The results add to this literature by identifying the distinctive challenges of CBDCs, including cross-border interoperability and ethical oversight.

iii. Implications for Policy and Practice

1) Policy Innovation:

The report recommends that regulation of CBDC should be proactive; it should focus on national and international harmonization and coordination for compliance challenges to be addressed. In the same way, ethics concerns over user autonomy, privacy, and inclusivity have to be paramount. This will ensure compatibility with social values if such values are infused into the intrinsic design of CBDCs at the point of creation.

2) Technological Design and Implementation:

This begets, among other practical results, that a CBDC needs to be a system capable of adaptation and change. Keen attention by institutions is required regarding the use of higher technologies as a means for introducing better security and efficiency with caution against excessive investment in technological capabilities at the expense of more human-centered approaches to access.

3) Educational and Awareness Campaigns:

Evidence exists to prove that there is a huge digital gap, particularly in areas where technological infrastructure is weak. For such gaps, specific education and empowerment of the users are needed for mass adoption. Central banks and financial institutions should liaise with educational and civic organizations to design and execute this type of campaign.

i. Contributions to Knowledge

We present our contributions to the field of CBDC research:

1) **Integrative Ethical Frameworks:**

By synthesizing findings across privacy, inclusivity, and governance, the study proposes a holistic ethical framework for CBDCs. This framework emphasizes the interdependence of individual rights, institutional accountability, and technological innovation, offering a comprehensive lens for evaluating digital currencies.

2) **Dynamic Compliance Models:**

Emphasizing AI-powered compliance tools together with privacy-preserving technologies, a new approach balances regulatory imperatives with ethical considerations. The model developed here pushes forward current theories by embedding real-time analytics into user-centered design principles.

3) **Socio-Technical Resilience:**

This discussion extends the theoretical understanding of digital infrastructures by focusing on the operational resilience of the study. By focusing on redundancy mechanisms, disaster recovery protocols, and predictive analytics, it presents a starter for future research in adaptive systems that could eventually work their way around complex financial ecosystems.

ii. Analysis and Future Directions

While valuable, the results also describe gaps and challenges that call for further research: for instance, the tension between privacy and compliance points to the limitation of technological fixes to solve ethical concerns; and the need for collaboration indicates a requirement for more empirical work on multi-stakeholder governance models.

Future research should also cover the long-term impact CBDCs will have on society in general, regarding economic inequality and the accessibility of financial services. Comparative studies across regions can help provide more detailed insights into how contextual factors shape the adoption and effectiveness of CBDCs.

Synthesis of the results of this study underlines the transformative potential for the CBDC in reshaping the form of global financial systems. On ethical concerns, strengthening compliance regimes, and operating resilience, the CBDC would be the bedrock necessary to help in delivering inclusive and secured digital finance. This, however, needs a collaborative approach with infusions of technological innovation, ethical foresight, and robust governance. These findings contribute not only to the academic discourse on CBDCs but also offer actionable insights for policymakers, practitioners, and researchers navigating this complex and rapidly evolving landscape.

5.7.2. Insights and Practical Reflections

The actual deployment of CBDCs raises unprecedented concerns about technological innovation, ethical challenges, and practical considerations. This section outlines the critical findings from the synthesis of survey results and interviews, underlining their theoretical and practical implications as well as offering novel contributions to knowledge.

i. Insights: Balancing Ethical and Operational Challenges

One of the most striking inductively derived findings in the study is the paradox between operational needs and ethical needs. Survey findings indicate that although 64.18% of the respondents pointed out the need for privacy (61.86%) and autonomy (66.49%), the same percentage also pointed out the requirement of stringently enforced compliance policies, such as AML/CFT/CPF regulations. This dualism is a key challenge: how to implement CBDCs that are simultaneously ethically robust and operationally resilient. Interviews showed that these dual concerns necessitate an active approach to governance and system structure alike. Privacy-by-design principles, respondents recommend, offer a basis in the balance between autonomy for users and requirements for compliance. Yet, all this presupposes that there will be transparent data use and real-time monitoring of all the transactions, making this work even more complex, given tensions between privacy activists and government agencies.

ii. Practical Reflections: How to Approach the Technical-Societal Gaps

On the practical level, there have been a number of gaps present in the preparedness of financial systems and institutions for CBDCs. The three most problematic areas based on the interviews of experts are given below:

1) Technical Infrastructure:

Most financial institutions still have legacy systems lacking the scalability and flexibility to accommodate CBDC. According to the respondents, investment in scalable infrastructure able to handle volumes of high transactions and interoperability with current payment systems is needed. This result is highly applicable in those areas where digital ecosystems are not so developed, and outdated infrastructures might be one of the issues for the adoption itself.

2) Digital Literacy:

Key barriers to this growth that were detected include limited general awareness of CBDCs; among those at higher risk in such conditions - that is, elderly and rural populations - reach areas not being reached would benefit from well-thought-of awareness campaigns and hence are most crucial to

ubiquitous attainment. To support different target groups of citizens, the multilinguality interface has been enabled to support simplification of their usability. Others include:

3) **Regulator Alignment**

The interviews conducted have revealed various inconsistencies in the regulatory approaches existing between jurisdictions. Without harmonized standards, it would be a hard operation and one that was highly non-compliant to execute cross-border CBDC transactions. Interviewees called for global regulators' cooperation so that there could be a certain framework that balanced security with inclusiveness and efficiency.

iii. Theoretical Implications: Reimagining Governance Models

The research makes a fresh contribution to the discussion of digital finance by presenting CBDCs' multi-faceted challenges with collaborative governance models for solution. In contrast to top-down traditional models of regulation, the underlying approach of collaborative models is inclusiveness, shared accountability, and dynamic adaptability.

Some important ingredients of this governance model include:

- **Stakeholder Engagement:** Inclusive governance brings together central banks, financial institutions, technology providers, and civil society organizations in a collaborative manner. This inclusiveness ensures that diverse perspectives are considered, enhancing the legitimacy and effectiveness of CBDC systems.
- **Transparent Decision-Making:** Transparency in the rule-setting and enforcement process engenders public trust. The ability of institutions to communicate the reasoning behind policy decisions openly can help reduce skepticism and build confidence in CBDCs.
- **Agile Adaptation:** Ever-faster technological development requires governance models to adopt in view of problems which only have recently come to light. Continuous improvements, with important elements including real-time data analytics and feedback loops, ensure that governance practices harmonize with user needs and regulatory developments.

iv. Practical Recommendations: Bridging the Gaps

Based on these challenges, a number of practical recommendations are hypothesized by the study:

1) **Technical Innovation:**

- Develop modular infrastructures that may be upgraded incrementally without interfering with operational activities.
- Incorporate AI and ML tools to enable real-time monitoring and threat detection.

2) **User-Centric Design:**
   - Provide accessibility through the development of intuitive and inclusive interfaces.
   - Develop offline functionality to cater to areas with unstable internet connectivity.

3) **Global Collaboration:**
   - Establish global task forces to harmonize with regulatory requirements for CBDCs.
   - Promote cross-border interoperability through standardized protocols and shared technologies.

4) **Ethical Safeguards:**
   - Adopt privacy-by-design principles to protect user autonomy while also supporting compliance requirements.
   - Data governance needs to emphasize transparency, where there is openness on how user data is collected, stored, and used.

v. *Opportunities and Analysis of Risks*

The report findings hold revolutionary promise linked to CBDCs but also entail significant risks. The balance between the notions of privacy and compliance is one of the key challenges, and inattention to the matter could compromise public trust. At the same time, reliance on advanced technologies exposes them to their weak points on many points, such as in the case of cyberattacks or system downtime that may compromise financial systems and undermine faith in CBDCs.

These challenges, on the other hand, provide avenues for innovation: inclusions of modern technologies like blockchain and AI in system security and efficiency. The shared governance structures can also serve as a template of governing CBDC implementation intricacies toward inclusivity and confidence across various stakeholders.

vi. *Contribution to Knowledge*

This paper advances the discussion on CBDCS by synthesizing ethical, operational, and governance perspectives into a consolidated framework. Contributions include:

- **Dual-Layered Approach to Governance:** Combining top-down regulatory oversight with bottom-up stakeholder engagement offers a new paradigm for managing digital currencies.
- **Compliance Models Preserving Privacy:** Implementing principles of privacy-by-design into AI-driven compliance tools alleviates the tension between individual rights and regulatory obligations and thus also forms a route to ethical CBDC implementation.
- **Infrastructure That Is Resilient and Scalable:** Emphasis on modularity and adaptability imbues a fresh dimension into the discussion of financial infrastructure. Central is the need for future-proofing in dynamic technological and regulatory environments.

The coming together of ethical, operational, and governance challenges in the implementation of CBDCs calls for innovative solutions that are inclusive, secure, and trustworthy. Indeed, through collaborative governance models, investment in scalable infrastructure, and integration of privacy-preserving technologies, institutions can successfully navigate these complexities. The study's results add to furthered knowledge of CBDCs by offering actionable insights and theoretical frameworks that might guide policymakers, practitioners, and researchers in shaping the future of digital finance.

5.7.3. Interpreting Ethical, Compliance, and Cybersecurity Dimensions in CBDCs

The implementation of CBDCs has brought to the fore a complex interplay of ethical considerations, compliance challenges, and cybersecurity demands. These dimensions are deeply intertwined and influence one another to shape the trajectory of CBDC adoption, acceptance, and effectiveness. Drawing on the synthesis of survey insights and interview data, this paper critically examines these interwoven facets in order to provide new contributions to knowledge.

i. *Ethical Dimensions: User Autonomy and Privacy First*

Results from the survey showed that **64.18%** of the respondents found user autonomy and privacy "important" or "very important," thus placing an ethical burden on how the protection of individual rights is ensured within a CBDC system. Interviews showed, however, that these often run counter to the operational imperatives thrown up by regulatory compliance. For example, while privacy-by-design principles, such as anonymization and selective data disclosure, offer solutions to protect user information, these features can complicate AML, CFT and CPF measures. Financial institutions and regulators are thus evaluating hybrid models with strong privacy guards that embed compliance capabilities in the process of seeking to mitigate such tensions. In this vein, respondents emphasized the transparency of data usage, where users are kept informed of their data collection, storage, and processing. Furthermore, decentralized systems that minimize data centralization were recommended to reduce the risks of unauthorized access and misuse.

This research underlines the duality of CBDC design, balancing user autonomy against compliance requirements. Privacy-enhancing technologies such as zero-knowledge proof embedded in a system and dispersed data storage enable the institutions to build trust while remaining compliant with regulatory requirements.

ii. Compliance Dimensions: Bridging Regulatory Gaps

The regulatory compliance concerns for CBDCs are multilayered. This is reflected by 37.94% of the respondents identifying integration with existing financial regulations as a "considerable" or "great challenge". It was revealed by the interview data that traditional regulatory frameworks, fitting for fiat-based systems, may not be sufficiently agile to keep up with special features of CBDCs.

The central theme was the harmonization of regulatory standards globally, with 75.00% of respondents promoting international collaboration. This will be important for cross-border transactions, particularly since the absence of uniform regulation increases interoperability risk and compliance danger. Evolving regulatory frameworks adapting to developing technological and operational landscapes were also preferred by respondents, as a means of maintaining CBDCs immune to emerging threats and challenges.

Research herein suggests a model of regulatory harmonization that elevates national standards to internationally accepted best practices without compromising local specificity. It can unite central banks, regulatory authorities, and international organizations to make a compliant yet responsive framework of laws for CBDCs with a template for coherence and flexibility.

iii. Cybersecurity Dimensions: Ensuring System Integrity and Resilience

Thus, cybersecurity became the top concern of CBDCs. Key risks in this area that were most relevant to CBDCs mentioned by 61.45% of respondents were related to data breaches, unauthorized access, and identity theft. From the interviews, it underlined that because of using legacy systems, there's an integral risk for multiple attacks, while at the same time stating the need for state-of-the-art cybersecurity features of the CBDC platform in order not to fall behind advanced cyber-attacks.

Multilayered cybersecurity architecture was pointed out by the respondents, which includes:

- **Advanced Encryption:** Methods include Elliptic Curve Cryptography and Homomorphic Encryption for cited reasons why sensitive information can be considered safe while at rest or in transit.
- **Continuous Monitoring and Real-time Threats Detection:** Through continuous monitoring through AI-powered tools, it is shown that threats not readily observable can be detected to mitigate against threats before their impacts are grave.
- **Zero-Trust Architecture:** These architectures reduce insider threats and the risks of unauthorized access by verifying users and systems continuously.

This also went on to demand proactive steps in line with this, like frequent security audits and penetration testing to identify the vulnerabilities. To this end, detailed incident response plans were proposed by the respondents, which can reduce the effect of a security breach and enable rapid recovery.

Combination of AI-powered cybersecurity solutions with the zero-trust fundamentals while developing CBDC systems is a novel method of constructing system resilience. The paper adds to the literature by suggesting a cybersecurity framework, founded on innovation in technologies and organizational readiness, that could assist in the protection of the ecosystems of CBDCs.

iv. Ethical Interplay, Compliance, and Cybersecurity Dimensions

The dimensions of ethics, compliance, and cybersecurity converge to make the landscape of CBDC implementation complex.

Though each dimension has its own issues, they are highly intertwined and call for a holistic approach to ensure the success of CBDC systems. For example, the technologies enhancing privacy support both ethical goals and compliance requirements by being able to share data securely while keeping user confidentiality. Correspondingly, robust cybersecurity can enhance compliance by ensuring transaction data integrity and inhibiting illicit activities. Through interviews, it was noted that stakeholder collaboration is key to mitigating these interdependencies. It means that, therefore, collaboration by central banks, financial institutions, technology providers, and regulators should result in integrated solutions whereby different priorities would balance out, while finally, according to respondents, open communication reassures the public and brings stakeholder alignment.

Convergent governance is yet another conceptual framework within which this approach to the combined ethics, compliance, and cybersecurity perspective would be understood in this model of nurturing collaboration or openness to lighten up the path amidst the CBDC complexity.

v. Practical Implications

Fairly, the ethical, compliance, and cybersecurity dimensions of CBDCs are entangled together rather than standing alone; they form integral parts of a more extensive ecosystem. This paper emphasizes the requirement for an equilibrious and integrated approach in handling such dimensions to make CBDCs secure, inclusive, and worthy of trust.

In this regard, the adoption of privacy-preserving technologies, harmonization of regulatory standards, and use of advanced cybersecurity measures would allow institutions to sort through the complexities of CBDC implementation without losing public trust or operational integrity. A new paradigm might be

developed around the concept of convergent governance, forming the base for sustainable CBDC adoption in these fast-changing times of financial development.

All in all, these ethical, compliance, and cybersecurity dimensions enhance the knowledge base on CBDCs, underpin with actionable insights, new frames that will consequently guide the shaping of a new future in digital finance by policymakers, practitioners, and scholars.

5.7.4. Thematic Convergence and Strategic Implications

The deployment of CBDCs is more than a technological change; it is a convergence of ethical consideration, compliance complexities, and cybersecurity imperatives. Each of these facets operates independently but intersects in such a way as to significantly influence the success of CBDCs. This section integrates findings from interview data and survey returns to examine the thematic convergence of these facets and extrapolates strategic implications.

i. Thematic Convergence: Ethical, Compliance, and Cybersecurity Dimensions

There needs to be a framework that integrates ethical aspects, compliance imperatives, and cybersecurity focus in the implementation of CBDCs. In support, majority of surveyed and interview participants identified a trade-off between privacy and compliance, as user autonomy should be preserved, while the compliance measures such as AML/CFT protocols very often involve far-reaching data monitoring. In a similar vein, interviews also demonstrated how these cybersecurity solutions must not only address technical vulnerabilities but must equally be required by ethical imperatives through data protection and user trust.

It is not an accident but a function of intrinsic complexity that characterizes digital currency ecosystems. For example, compliance operates in a wider context: regulatory frameworks requiring real-time monitoring of transactions have to address ethical issues related to user privacy and autonomy. Cybersecurity measures focused on ensuring operational resilience should be inclusive in respect to the compliance mechanism concerning money laundering and terrorism financing threats.

The paper develops “Convergence Frameworks” that integrate the ethical, compliance, and cybersecurity dimensions within the CBDC design. The framework provides a structured pathway to the policymakers and institutions on how to balance these interlinked priorities without compromising one for the other.

ii. Strategic Implications of Thematic Convergence

1) **Balancing Privacy and Compliance**

An important strategic implication of this thematic convergence is how to balance privacy with regulatory matters. Thus, designed-for-privacy principles emerged as a clear favourite approach by respondents; **25.00%** of interviewed advocated for features including the ability to anonymize transactions and store data in a decentralized manner. However, interview data indicated that a key operational challenge was how to integrate these features with requirements pertaining to AML/CFT/CPF, which require detailed transaction records.

Institutions have to adopt hybrid solutions to share data selectively. For instance, zero-knowledge proofs provide an opportunity to validate the transactions that took place while keeping sensitive user information private. Similarly, role-based access minimizes contact to authorized personnel, which reduces the possibility of misuse of data.

2) Strengthening Cybersecurity for Compliance and Trust

Not only are cybersecurity measures a solution in nature, but they also form the very base of compliance and user trust. In their responses, survey participants placed high values on continuous system monitoring at **56.25%**, and advanced encryption techniques at **58.64%** to reduce actual risks such as data breaches and unauthorized access. Further interviews made clear that such measures are crucial in ensuring the integrity of compliance systems themselves, which rely on secure transaction data for AML/CFT monitoring.

The strategic integration of predictive analytics with machine learning will position the institution to identify emerging threats in real-time. Proactive cybersecurity frameworks-like zero-trust architectures-naturally ensure that no user or system component is inherently trusted, enhancing operational security.

3) Collaborative Governance Models: A Cornerstone of Convergence

One of the strongest points arising from the interviews was emphasis on collaborative governance. As many as **75.00%** of the respondents believed in governance models that combine the skills of central banks, regulatory authorities, and private sector innovators in the realm of CBDCs. This collaborative approach meets the multifaceted challenges of CBDCs by drawing from various strengths.

These could be regulatory oversight by central banks and technological innovation by private fintech companies. In this respect, such collaboration will make sure that CBDC systems will equally be compliant, secure, user-friendly, and adaptable. The second important point is that transparency in governance processes of public consultations and feedback loops is critical for fostering trust among stakeholders.

Introducing “Collaborative Convergence Councils” is a unique solution to governance challenges through independent advisory bodies comprising central banks, private fintech firms, and consumer advocacy groups. Their role is to govern the CBDC systems regarding ethical, compliance, and cybersecurity aspects, assuring that they are aligned with the priorities of the general public and institutions.

iii. Technological Innovation: A Strategic Imperative

The new emerging technologies such as blockchain and AI in the CBDC ecosystem also have dual use. Blockchain architecture supports both decentralization for transparency and security, hence supports the requirements of compliance and cybersecurity. In contrast, interviews indicated a number of challenges- for instance, GDPR compliance, where immutable records of blockchain clash with data erasure.

On the other hand, AI strengthens both compliance and cybersecurity by allowing real-time transaction monitoring and threat detection. According to the respondents, AI algorithms could spot suspicious patterns perhaps overlooked by manual systems, further enhancing the efficiency of AML/CFT protocols. Yet, making sure that such algorithms are non-discriminatory and that their use is ethical, presents another challenge altogether.

The challenges listed above require investment in continuous research and development by institutions. Innovation hubs can simulate CBDC environments to test new technologies before full-scale deployment, ensuring they meet the threshold on ethical, compliance, and cybersecurity standards.

iv. Global and Regional Implications

Convergence of themes also has huge implications globally and regionally. It showed from the survey data the variance in the adoption rates of CBDCs, how advanced economies are able to implement them quicker due to robust digital infrastructures, while regions with sparse connectivity and limited financial literacy are experiencing slower adoptions, hence requiring tailored strategies.

These collaborative models of governance will help to achieve harmonization at the global level but still allow localized adaptations. For example, regions that have relatively low digital literacy can prioritize educative campaigns, whereas advanced economies are focused on scalability and interoperability across borders.

v. To Integrated CBDC Systems

The thematic convergence of ethical, compliance, and cybersecurity aspects highlights the complexity of CBDC implementation. Introducing the Convergence Framework and Collaborative Convergence Councils, this research provides actionable solutions to address these interdependent priorities.

By striking a balance between the demands of privacy and compliance, enhancing cybersecurity, shared governance, and leveraging technological innovation, CBDC systems can be secure, ethical, and efficient. Not only do these approaches address current challenges, but they set CBDCs up as the cornerstone of the future financial environment, resilient and evolutionary with the demands and technologies that will arise.

A coordinated approach will allow CBDCs to fulfill their revolutionary promise of public trust and regulatory probity on the path to sustainable, worldwide adoption.

5.7.5. Analytical Perspectives on Ethical and Security Frameworks for CBDCs

The implementation of CBDCs requires a strong integration of ethical and security frameworks to guarantee that digital currency systems are not just functional, but also fair, secure, and reliable. Based on interview evidence and survey data, this section critically examines the intersection of ethical concerns with security requirements and their implications for policy and practice. The analysis represents new contributions to knowledge through the proposal of integrated strategies that account for ethical considerations and advanced security mechanisms.

i. *Ethical Imperatives in CBDC Implementation*

The moral aspects of CBDC design concern privacy, inclusiveness, and end-user autonomy. As stipulated earlier, a great majority of survey takers prioritized privacy, naming it “important” or “extremely important,” reflecting broad concerns regarding the protection of data in digital currency systems. That said, the interviews made clear that privacy considerations tend to contradict compliance demands-in connection, for instance, to AML/CFT.

Hence, this tension operates to underscore the necessity of ethical requirements encompassing the elements of privacy-by-design. The participants highlighted the application of anonymization methods, targeted data sharing, and decentralized storage procedures. These procedures shield user information but enable required regulatory oversight: for example, zero-knowledge proofs can confirm transactions without revealing sensitive user information, thus effectively satisfying ethical and compliance requirements.

Further, inclusivity became a prominent ethical issue, with participants emphasizing the necessity of financial systems that serve underserved groups. User-friendliness and offline functionality were recommended by respondents to close the digital divide. Ethical structures must thus engrain accessibility as a fundamental tenet, enabling CBDCs to be inclusive and fair.

ii. Security as a Cornerstone of Trust

Security is paramount for the success of any CBDC initiative; any breach in security will lead to loss of user trust and, subsequently, damage to the system's credibility. For example, according to the survey data, majority of respondents named data breach and unauthorized access as critical cybersecurity risks. Additional concerns from the interview data revolved around system vulnerabilities and the scalability of security protocols with increased transaction volumes.

The issues highlighted herein are to be addressed with newer methods of encryption, multi-stage authentication, and real-time intrusion detection systems. For instance, it was opined that elliptic curve cryptography or AI-enabled intrusion detection systems would assist the CBDC platform in securing its operations effectively. These steps ensure not only the security of the users' information but also the functional integrity of the system.

The other very crucial recommendation was the implementation of zero-trust security models. Zero-trust models reduce the possibility of unauthorized access and enhance the system's overall security by demanding repeated authentication on each access request.

iii. The Intersection of Ethics and Security

The point of contact between ethical and security frameworks provides a dynamics so complex that the same needs to be balanced rather eloquently. While ethical parameters call for user autonomy and privacy, security imperatives need surveillance and analysis of transactional data with an eye on preventing fraud and compliance with regulatory prescriptions. This dual nature thereof creates a paradox which the institutions have to negotiate with accuracy.

The respondents presented a number of recommendations to balance the above conflicting priorities: embedding ethics in security controls was emphasized. For example, transactional data can be anonymized and feeding logs monitored for anomalous behavior, which will not invade people's privacy. Likewise, data is permitted to be disclosed to only authorized users using role-based access controls, thus minimizing misuse risks.

Transparency has been described as a panacea that would close the security-ethics divide. The collection, storage, and utilization of users' data must be led by transparency. Transparency regarding security controls and compliance needs creates trust and enables users to make fully informed decisions.

iv. Ethical-Security Integration Framework

This writing introduces the Ethical-Security Integration Framework (ESIF), a new approach to reconciling ethical concerns with security demands on CBDC systems. The framework rests on three pillars:

1) **Privacy-Preserving Security Protocols**
   - Incorporate advanced encryption and anonymization mechanisms.
   - Design AI algorithms to identify fraud without infringing upon users' privacy.

2) **Transparent Governance Structures**
   - Learn about data policies via transparent communication channels to be established for users.
   - Independent nature governing bodies provide accountability and thereby create transparency.

3) **Collaborative Ecosystems**
   - Foster cooperation between central banks, technology providers, and regulators to solve these challenges.
   - Standardize security and ethical best practices across borders for inter-operability.

The ESIF provides a structured framework to the intricate inter-play between ethics and security and thereby provides an applied guide to institutions while solving the challenges of CBDC implementation.

v. *Policy and Practical Implications*

Based on our findings, policymakers should take a holistic approach towards the governance of CBDCs. Ethical considerations cannot be prioritized over security imperatives; they have to become inherent to the core architecture of the system.

Regulators must make privacy-by-design concepts mandatory and to set out guidelines on ethical data handling.

Financial institutions: Financial institutions on the other hand, must invest in cutting-edge technologies that respond to ethics and security challenges. AI and machine learning can play a vital role in the quest for equilibrium in the face of real-time threat detection and user privacy considerations. At the operational level, periodic audits and stress tests in institutions to identify possible vulnerabilities and concerns for compliance with ethical standards should be done regularly.

Public awareness campaigns, training for the staff will also be important in building up awareness and competencies to manage the ethical and security dimensions of CBDCs.

vi. *Conclusion: Toward Ethical and Secure CBDC Systems*

The interplay between ethical and security frameworks in the implementation of CBDC therefore serves as a manifestation of the social values expected to be communicated through digital currency. A strong

emphasis on privacy, inclusiveness and user trust will put institutions on the path to creating a system that is not only secure but also ethical and fair.

This framework offers both a new method to prioritize them and a map for the sustainable and responsible introduction of CBDCs. Integration of ethical and security principles into the work of central banks, regulatory bodies, and technology providers as they jointly design the future of digital finance will be integral to building systems that inspire trust and facilitate global financial inclusion.

The survey data highlights the nuanced interplay between ethics, compliance, and cybersecurity in CBDC implementation.
The statistical findings reveal an urgent need to:
The survey data underlines the subtle interplay between ethics, compliance, and cybersecurity in CBDC implementation. The statistical findings hence depict an urgent need to :

1) **Ethical Priorities in CBDC Design**

- ✓ **User Privacy and Data Protection:** the protection of personal data is of paramount importance and 73.47% of respondents emphasized its importance. Privacy concerns are fundamentally linked to gaining users' trust in the CBDC.
- ✓ **Inclusivity:** 62.24% of respondents expressed the need for fair and equal access to CBDCs, reflecting the need to avoid financial exclusion in the process of implementing CBDCs.
- ✓ **Transparency and Accountability:** 65.31% of respondents emphasized that open and accountable governance of CBDC is important to gain public trust.

2) **Compliance and Regulatory Issues:**

- ✓ **Integration in Existing Frameworks:** 79.48% of respondents feel that integrating CBDCs with existing regulatory structures presents a moderate to significant challenge.
- ✓ **Urgency of Regulatory Updates:** A majority (82.99%) feel the need for regulation to evolve and meet new compliance needs arising from CBDCs.
- ✓ **International Alignment:** 69% of respondents indicated that it is difficult to harmonize CBDCs with international regulations, further highlighting the issue of global interoperability.

3) **Cybersecurity Concerns:**

- ✓ **Top Risks:** Unauthorized data access (38.02% rated it “Extremely Significant”).
- ✓ **Effective Measures:** System vulnerabilities (28.57% rated it as critical).
- ✓ Privacy-enhancing technologies, encryption and strong authentication mechanisms were rated as “Very Effective” or “Highly Effective” by more than 50% of respondents, indicating their importance in mitigating cybersecurity risks.

4) **Economic and Operational Impact:**

- ✓ **Traditional Banking:** 78.35% of respondents indicated that CBDC could have a somewhat or very positive economic impact on traditional banking activities.
- ✓ **Operational Challenges:** Operational challenges Focusing on resilience, respondents highlighted system fragility and operational risk as key concerns.

5) **AML-CFT-CFP Effectiveness:**

- ✓ 76.8% of respondents rated current CBDC systems as moderately effective in meeting Compliance standards, while only a small proportion (4.12%) rated them as very effective, indicating significant room for improvement.

6) **Balancing Ethical and Regulatory Tensions:**

- ✓ Another key issue is the conflict between protecting user privacy and meeting strict compliance and security requirements. This challenge highlights the need for solutions that combine innovations in privacy protection technologies.

By bringing these insights together, stakeholders in our workspace can overcome the complexities of CBDC implementation and ensure that these systems become tools for financial inclusion, security and innovation, rather than sources of risk and exclusion.

VI. CONCLUSIONS

6.1. Introduction

This final chapter brings together the key findings, implications, and reflections from a study on CBDCs. At every step of this research, there has been this undercurrent of interaction and interplay between the concerns of ethics, challenges for compliance, and risks with opportunities that emerge when discussing these critical dimensions.

This paper contributes to this bourgeoning discourse by examining these facets in detail for a sustainable and ethical implementation of CBDCs.

The findings have shown that although CBDCs hold the potential to transform financial systems globally, there are a lot of complications in their adoption. Key themes privacy, financial inclusivity, transparency, and operational resilience explore this report and present inherent contradictions between ethical imperatives, regulatory compliance, and technological security. It also places a strong emphasis on models of collaborative governance and strategies that look toward the future to negotiate through

these obstacles.

This last chapter revisits the main insights obtained through the analysis and discussions. It will also explore what implications these findings bear for policymakers, financial institutions, and technology developers. The chapter will lay out specific recommendations that can be put into practice to ensure that CBDCs are implemented and managed in a responsible manner while keeping a proper balance between innovation and regulation. It further reflects on the limitations of the study in an effort to establish a base for future research.

Lastly, this chapter highlights the original contributions that this research makes to the study of CBDCs, including conceptual frameworks combining ethical and security principles within the operational fabric of CBDCs and providing a roadmap for institutions looking to implement digital currencies responsibly. This could not be more timely for a world embracing digital transformation. It would also emphasize the critical need to reconcile technological advancement with ethical and regulatory standards to create a resilient, inclusive digital financial ecosystem resting on trust. This really is a culmination of our thorough investigation of challenges and opportunities presented by CBDCs and acts, so to speak, as one big call for continued cooperation and innovation.

6.2. Implications for Policy and Practice

6.2.1. Implications for policymakers and institutions

The benefits that will flow from CBDCs will go a long way in improving payment efficiency and fostering financial inclusion, thereby providing new tools to central banks for the execution of monetary policy. Integrating these brings multidimensional challenges, which will certainly need a highly comprehensive regulatory framework. How issues like transaction traceability, cross-border compliance, data protection, user privacy, financial inclusion, and cybersecurity are to be dealt with is what the regulatory bodies, policymakers, and financial institutions have to work out.

i. Transaction Traceability and Data Protection

Inherent in CBDCs is the detailed recording of transaction data, which may prove highly instrumental in combating such illicit activities as money laundering and tax evasion. On the other hand, though, that kind of transparency raises very serious concerns about user privacy and the potential for unwarranted surveillance. A centralized ledger with detailed transaction data could, for example, become a target for cybercriminals to compromise and execute mass surveillance, potentially infringing on individual freedoms.

ii. World Economic Forum

These risks can be mitigated by policy makers using privacy-preserving technologies in CBDC

architectures. Technologies like zero-knowledge proofs and differential privacy enable verification of transactions without revealing individual transaction information. For example, Sweden's central bank, Riksbank, has built in protection for privacy in the design of its e-krona CBDC pilot through the use of an open-source distributed ledger that allows shared information to be released to authorities and financial intermediaries on a need-to-know basis[84]. "This allows for a level of privacy that is akin to the two-tiered model used by central banks today," the World Economic Forum Digital Currency Governance Consortium White Paper Series says.

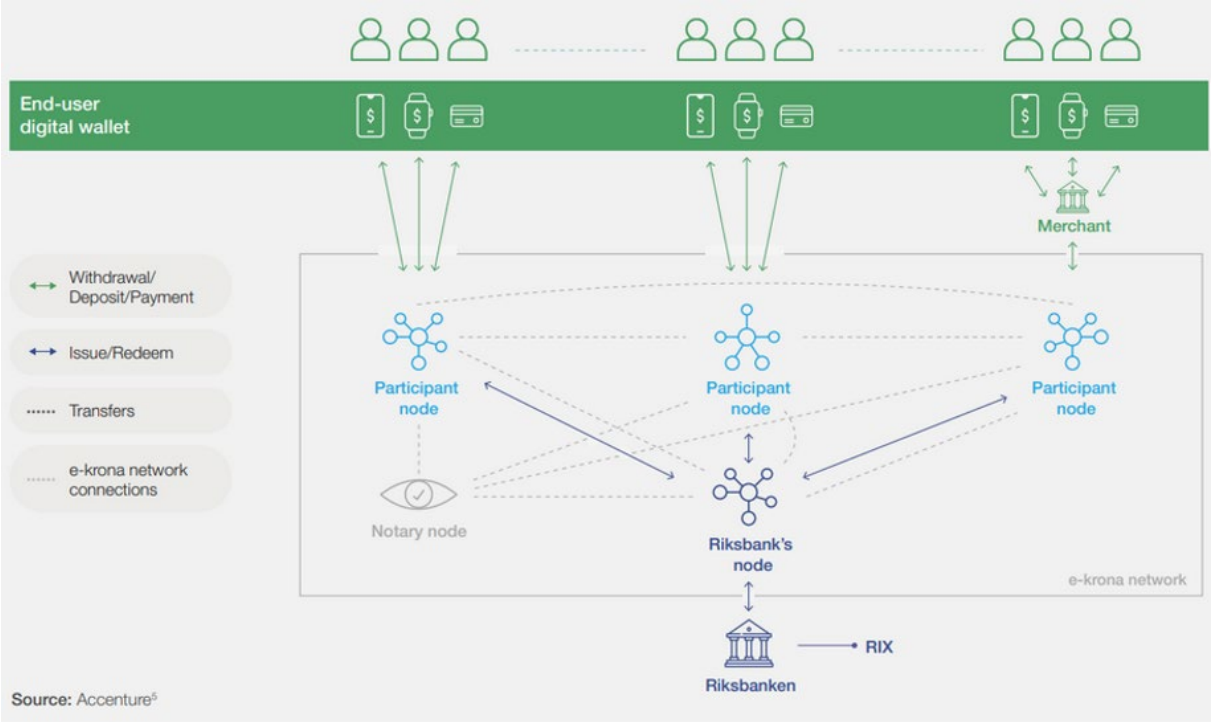


Figure 31: Conceptual architecture for the e-krona pilot

iii. Cross-Border Compliance and Interoperability

While financial transactions have been international in nature, CBDCs therefore have to be designed with cross-border functionality in mind. On the other hand, different regulatory standards across different jurisdictions provide a big challenge. The BIS explains that the issues related to cross-border payments include differences in both regulatory standards and technological systems, which may cause frictions in transactions.

It will also be important to address these issues through international cooperation. There should be

[84] https://www.weforum.org/stories/2023/11/privacy-concerns-around-cbdcs/
https://www.riksbank.se/en-gb/payments--cash/e-krona/

harmonization of regulatory standards and interoperable systems that will enable seamless cross-border CBDC transactions by policymakers. Such efforts in this direction are represented by the BIS Project Dunbar, which investigates the development of shared platforms for cross-border CBDC payments, aiming at unified frameworks for international transactions.

iv. Financial Inclusion

Financial inclusion One of the key drivers of CBDC issuance is financial inclusion, including providing access to digital financial services for the unbanked and underbanked. However, the nature of the digitalization of CBDCs risks excluding those without access to digital infrastructure or literacy. For instance, in Nigeria, although the e-Naira has been launched, uptake remains slow at 13 million wallets for a population of 233 million, hence showing how difficult it is to achieve the goal of reaching the unbanked[85].

In designing CBDC implementation, policymakers have to make sure that the measures to be taken for bridging the digital divide are contained in the plan: investment in digital infrastructure, promotion of digital literacy, and accessibility and usability of CBDC platforms. It should also consider offline functionalities to accommodate users in areas with limited internet connectivity.

v. Cybersecurity Threats

The digitization of currencies makes them vulnerable to cyber threats such as hacking, fraud and technical failures; a successful cyber attack on CBDC systems could undermine confidence in the financial system and have far-reaching economic consequences. The IMF has noted that CBDC vulnerabilities might be leveraged to compromise a nation's financial system and has placed an emphasis on strong cybersecurity measures[86].

This is an area to which all these institutions have to invest in advanced cybersecurity infrastructure. Some of the measures will include real-time monitoring systems, periodic security audits, and incident response protocols. The integrity of the CBDC systems also depends upon collaboration with experts in cybersecurity and following international standards of security.

vi. Balancing Innovation with Compliance

The emergence of CBDCs offers attractive opportunities for financial sector innovation, modern payment methods and improved monetary policy. However, all these need to be fully compatible with the existing financial regulatory framework. Such a balance is highly relevant to prevent abuses, support

[85] https://www.eos-intelligence.com/perspectives/technology/enaira-is-it-here-to-stay-or-are-Nigerians-going-to-say-nay/
[86] https://www.imf.org/en/Publications/fandd/issues/2022/09/Central-bankers-new-cybersecurity-challenge-Fanti-Lipsky-Moehr

financial stability, and build trust in the system.

Consider, for example, the Bahamas, which launched the Sand Dollar, a CBDC, in 2020[87]. After launching the Sand Dollar in late 2020, **Mr Porter** revealed that the current amount in circulation is $2.1 million, representing less than 0.5% of cash in circulation. (The Bahamian dollar is pegged to the U.S. dollar). To facilitate widespread adoption, regulators are developing policies that will force commercial banks to access this digital currency. This effort highlights the importance of a regulatory framework that not only ensures the integration of CBDCs but also ensures compliance with financial legislation and consumer protection legislation.

1) A Regulatory Framework That Supports Innovation

CBDCs introduce new issues which are not fully covered under current financial law. Policymakers thus must create comprehensive regulatory frameworks that address the different nature of the digital currencies with heightened compliance expectations. These include:

AML/CFT Regulation Revisions: Since CBDCs are digital, regulation of AML and combating the financing of terrorism will need to adapt. Advanced transaction monitoring, authentication, and fraud detection are important for risk management. Consumer protection in the digital environment: The security, transparency, and fairness of digital transactions are important to maintain public trust. Regulators need to extend existing consumer protection legislation to CBDC-related transactions.

Coordination with Important Stakeholders: Regulations cannot be framed in a vacuum. Banks, fintech players, and even the general public need to be included in policy-making to promote innovation while protecting compliance.

2) How Financial Institutions Have to Change

The preparedness of financial institutions will have a significant part to play in the seamless integration of CBDCs. Banks and financial service providers will have to make changes to their infrastructure, invest in technology upgrades, and offer training to their personnel to be able to handle digital currency transactions efficiently.

Some of the key areas of change are:

- **Strengthening Cybersecurity Controls:** With new forms of digital transactions that CBDCs introduce, banks must strengthen data protection measures and defend against cyber attacks.

[87] https://www.ledgerinsights.com/bahamas-sand-dollar-cbdc-has-2-1m-in-circulation-after-3-years/

- **Dealing with Increased Compliance Needs:** Reporting to regulators and monitoring transactions will require more sophisticated data management systems to meet new AML/CFT compliance regulations.
- **Continued Regulatory Collaboration:** Banks need to work closely with regulators in an ongoing manner to map their practices against evolving legal systems. Pilot initiatives and regulatory sandboxes can help gain useful experience to facilitate the transition towards the adoption of CBDC.

CBDCs have the potential to transform the financial landscape, but their implementation needs to be carefully calibrated, weighing innovation and compliance. Policymakers and financial institutions should work together to create clear regulations that promote financial inclusion while addressing key issues such as transaction traceability, cross-border compliance, data privacy and cybersecurity. Through active collaboration between stakeholders, CBDC can be part of a flexible, secure and inclusive digital currency ecosystem that benefits the economy and people.

6.2.1. Adaptations of Regional Policy for Africa

Central Banks Digital currencies can offer an opportunity to transform financial systems in the African region, particularly in countries such as Mali, Burkina Faso and Nigeria. However, successful implementation will require policies that address the infrastructure, education and socio-economic challenges facing the region. This section discusses the specific adaptations needed to overcome such obstacles, taking advantage of opportunities for alignment with CBDC global standards.

i. Overcoming Regional Infrastructural Challenges

Full deployment of CBDCs across Africa depends to a large degree on the availability and reliability of the infrastructure. For countries in Mali and Burkina Faso, the deficiency in digital infrastructures has remained among the greatest impediments to wider adaptation of CBDC. The poor internet connectivity has locked most rural communities out of reaching the digital platforms offering online payments. While Nigeria has relatively better digital infrastructure, issues of network congestion and inconsistent service delivery still persist, especially in remote areas.

The development of digital infrastructure, such as internet connectivity, mobile networks, and electricity supply, should be at the heart of policy adaptations, especially in underrepresented rural areas. Governments and central banks might work with telecom companies and technology providers to ensure a reasonable price for and reliability of internet access. Another approach is the introduction of the offline functionality of CBDCs. An offline CBDC would bridge the gap and make transactions inclusive, at least in areas where digitalization is poor.

Interoperability between CBDC systems and existing mobile money systems such as Orange Money and MTN Mobile Money in Burkina Faso and Mali will also facilitate adoption. Policies need to enable cooperation between mobile money operators and central banks and guarantee the realization of an environment that makes it easy for people to switch back and forth from CBDC to existing payment means for goods and services.

ii. Gap in Financial Literacy

Financial literacy is still one of the main barriers to the adoption of CBDCs in Africa. In Burkina Faso and Mali, much of the population-even less so for those in rural areas, has never had experience with formal financial systems. Most of the population lacks basic knowledge necessary for understanding and embracing digital financial tools. While Nigeria is relatively more financially literate, there are still significant gaps in this respect, especially among older and less-educated populations.

More precisely, intervention through policy should be further tuned to context-specific financial literacy programs. Central banks and governments should liaison with various educational institutes, NGOs, and local organizations for conducting various workshops and training programs. The programs can demystify the CBDCs, and explain in clear, simple terms how they will work, what are their benefits, functionalities, and security measures. Speaking in the local language and using culturally appropriate metaphors can foster comprehension and generate confidence among diverse demographic constituencies.

In addition, economic education programs need to be mixed with digital literacy programs to enable users to utilize digital platforms confidently. For instance, in Nigeria, where relatively high smartphone penetration allows for it, policy can include incentives for the purchase of affordable smartphones or devices to use on CBDC platforms. In Mali and Burkina Faso, affordable access to digital kiosks or community access points where users can access CBDC services and receive support may be a game-changer.

iii. Addressing Socioeconomic Inequalities

Socioeconomic disparities are a longstanding issue in Africa and directly impact the inclusivity of CBDC systems. A significant portion of the population in Mali and Burkina Faso falls under the poverty line with limited access to financial services. Women, specifically, are vulnerable to being victimized by systemic obstacles that push them out of formal financial networks. Nigeria, though more economically varied, still suffers from regional disparities that deter financial inclusion.

Policies must be skewed towards the design aspects of CBDCs to mitigate such imbalances. Design features like tiered KYC requirements would enable the integration of poor classes into the formal

economy fold. For instance, enabling basic CBDC functionality with minimal identification could help lower barriers for those who lack formal documentation. As users establish a transactional history, they can progressively access upper-tier services.

Subsidization of the transaction cost of the poor and, simultaneously, welfare distribution by the governments via the CBDC platform will render them even more inclusive. Mali and Burkina Faso, as remittance recipients, are part of required household incomes, and the introduction of CBDC in cross-border remittances will allow them to have cheaper and secure transfer.

Targeting gender inequalities through inclusive policy is another key area. Indeed, governments may encourage women to participate in the CBDC systems by advertising campaigns as well as other incentives, such as issuing grants or microloans via CBDCs. For this reason, empowering them economically may lead to economic growth and social development more extensively.

iv. Smoothening National Policies to Global Standards

On regional issues, African countries should align their policies on CBDFs with international standards in the search for interoperability and the building of global trust. The international standards are set by the FATF through directions on compliance aspects related to AML/CFT, data protection, and cybersecurity. For those standards to be aligned to the African setting, very substantial policy adjustment would be required.

The eNaira has already shown an attempt to meet international standards while serving local needs in Nigeria. Lessons from the Nigerian experience can inform Mali and Burkina Faso in developing policies that reconcile global requirements with local realities. The use of privacy-preserving technologies, like zero-knowledge proofs, might satisfy global data protection requirements without undermining user privacy.

Collaborative policymaking is critical to harmonizing national policies. African nations should engage in regional dialogues, such as through the West African Economic and Monetary Union (WAEMU) and the African Continental Free Trade Area (AfCFTA), to develop standardized frameworks for CBDC implementation. These frameworks can address cross-border interoperability, enabling seamless transactions between neighboring countries and fostering regional economic integration.

v. Opportunities for Technological Leapfrogging

African countries, for the first time in history, have a real chance to leapfrog the traditional financial systems by embracing leading-edge digital technologies. In this vein, policies should support innovation through a regulatory sandbox that lets fintech companies and startups test CBDC-related solutions. It enables new technologies to be deployed in a controlled environment, therefore fostering innovation at

lower risk.

Governments should also invest in studies and development to research new technologies like blockchain and Artificial Intelligence that can help further develop capacity and security. Partnerships and investments that would further accelerate globalization, with African countries putting themselves on the frontline in innovating about CBDCs.

vi. The Way Forward

This success will require a multilateral policy initiative to surmount regional issues and capitalize on the specific opportunities available. For nations such as Mali, Burkina Faso, and Nigeria, this includes investing in infrastructure, financial and digital literacy, and fighting socioeconomic inequalities. In the meantime, adherence to international standards coupled with supporting innovation will make these nations remain competitive in the expanding digital economy.

By adopting such regional policy innovations, African nations can be at the forefront of the inclusive and sustainable deployment of CBDCs. This will not only result in better financial systems but also in more extensive socio-economic progress, building a platform for a richer and more inclusive tomorrow.

6.2.2. Ethical and security frameworks for CBDCs

CBDCs will be transformational in the financial sector, bringing much-needed efficiency and inclusiveness. However, their implementation gives rise to many ethical and security concerns, which have to be treaded carefully in order to preserve public trust in the system and the integrity of the system.

i. Ethical Consideration in CBDC Implementation

1) Data Privacy

By their very nature, CBDCs digitize currency and, therefore, are a magnet for the collection and storage of huge reams of transactional data. That creates the potential for surveillance and other forms of misuse of personal financial information. The World Economic Forum makes a point of the fact that central banks are acutely aware of these privacy concerns and are actively working to address them through protective measures and public education.

2) Inclusivity

Among the most important goals that CBDCs should pursue is to further financial inclusion by enabling unbanked and underbanked people to access digital financial services. On the other hand, in the case of a poorly designed CBDC, it could contribute to the perpetuation of the same inequalities if some groups do not have access to either the basic digital infrastructure or literacy in such platforms. The accessibility of CBDCs has to be guaranteed at all levels of society to avoid further digital division.

3) User Autonomy

CBDC design should respect user autonomy, allowing individuals to take control of monetary transactions without undue hindrance. That would include protections against government overreach in forms of unwarranted surveillance or restrictions on how individuals may use their funds. Proper weighting of the necessity for regulation with the freedoms for individual citizens is important here.

ii. *Ethical frameworks for CBDCs*

1) Transparency in every transaction process.

In addition, the CBDCs should have a clear process of transactions in order to implement transparency, which would increase public trust. More open communication on how transactions are monitored, data is used, and privacy is safeguarded can dissipate concerns about surveillance and misuse of information. Transparency ensures that users are well-informed and can trust the system.

2) Equitable Access to Financial System

In the development of CBDCs, financial inclusion should be pursued to ensure equal access for all, regardless of socio-economic status or technological capability. This requires easy-to-use platforms that are accessible to all, as well as support for those with access challenges, such as the elderly and people in rural areas.

3) Equitable Treatment of Underserved Populations

Particular care is necessary to address underserved communities, so they do not fall back during the transition to digital currencies. This is having policies and programs in place that address some of the particular issues these communities are going to face, such as fewer digital devices or internet connections.

iii. *Safety Architectures for CBDCs*

1) Real-Time Threat Detection

Given the critical nature of CBDC systems, threat-detection mechanisms in real time are needed, which can flag and mitigate cyber threats without delay. According to the Bank for International Settlements, this is of the highest importance in terms of ensuring security and resilience for CBDC systems.

2) Advanced Encryption Techniques

Advanced encryption is important for transactional data protection against unauthorized access and to keep the integrity of the data. With the development of quantum computing, it will be important to adopt an encryption method that can outsmart future technological development to protect CBDC systems from possible threats.

3) **World Economic Forum**

Collaborative Governance in all CBDC systems, it would be a requirement to develop a collaborative governance framework with central banks, financial institutions, technology providers, and other stakeholders in the ecosystem. This collaboration will ensure that security protocols are going to be holistic, including a coordinated response to possible threats.

iv. Balancing Ethical and Security Considerations

It is most crucial to find a balance between security demands and ethical considerations when designing and building CBDCs, where data privacy and control by the user do not compromise system security and where robust security mechanisms do not intrude upon human rights; only with an end-to-end approach that integrates ethical frameworks into security measures do we ensure putting CBDCs into operation effectively as much as securely.

While the implementation of CBDCs is highly promising, it also gives rise to very complex ethical and security issues. In designing CBDC systems that are secure and ethically sound, central banks should consider a framework that focuses on data privacy, inclusivity, and user autonomy, along with strong measures such as real-time threat detection and advanced encryption. Integrating CBDCs into the financial system through collaborative governance and transparency is the only way to ensure the public's trust.

6.2.3. Ethical Considerations of CBDC for Mali, Burkina Faso, and Nigeria

Success will depend not only on the readiness of the technology but also on the aligment of ethical frameworks with local contexts as CBDCs gain traction around the world. In Mali, Burkina Faso, and Nigeria, there are specific challenges and opportunities regarding the actualization of ethical principles of CBDC systems within their respective cultural, economic, and technological environments. This section considers how the principles of inclusivity, data protection, and autonomy can be tailored to each of these regions in ways that promote ethical and effective adoption.

The three countries Mali, Burkina Faso, and Nigeria have been facing **financial inclusion** challenges because of the huge portion of unbanked and underbanked segments of their populations. In Mali and Burkina Faso, there is a predominance of rural communities where lack of access to formal banking and digital literacy is a very strong barrier. Women are also more likely to be financially excluded due to cultural and socioeconomic constraints. While more advanced in terms of financial inclusion, Nigeria still grapples with regional disparities, particularly in the northern regions.

The design of such national ethical frameworks must guarantee inclusivity in access to CBDC systems

irrespective of socio-economic and geographical situations. For instance, a tiered KYC expectation enables the unbanked to enjoy lower-level access to the digital economy while generating transaction records for higher-level access. The ability to perform transactions offline, particularly where internet connectivity is not stable, is essential to bridge the connectivity gap. The enforcement of certain policies, like subsidizing the cost of transactions for impoverished users and promoting financial education initiatives, is necessary. For Mali and Burkina Faso, it is essential that these be done in local languages and in a culturally sensitive manner to derive optimum response from the population. In Nigeria, the CBDC system can be scaled up using current mobile money networks and collaborating with fintech firms.

i. *Data Protection: Securing Privacy in the Digital Era*

With the CBDCs implementation, one of the critical ethical considerations is data protection, especially in regions where data privacy laws are still developing. The lack of wide-based data protection frameworks gives rise to concerns about possible misuse of personal and financial information in Mali and Burkina Faso. This makes Nigeria with more developed data protection laws, that is, the Nigeria Data Protection Regulation (NDPR) a case study for balancing innovation with user privacy.

Ethical frameworks for CBDCs in these countries would need to strongly emphasize the principle of privacy by design, ensuring that users' data is protected throughout the whole transaction life cycle. This can be achieved through technologies such as encryption, anonymization and distributed data storage. Zero-knowledge proofing, for example, allows transactions to be verified without revealing sensitive information, thus ensuring a balance between confidentiality and regulatory compliance. Similarly, clear data governance policies should be put in place. This means defining when and how user data will be collected, stored and shared. In countries where institutional trust is low, such as Mali and Burkina Faso, communicating data policies can help build public trust in CBDCs. Nigeria's regulatory experience can provide guidance for establishing similar frameworks in neighboring countries in West Africa and harmonizing data protection across the region.

ii. *Autonomy: Empowering Users in Digital Financial Systems*

A standard of ethical CBDC implementation, user autonomy is the philosophy that individuals must be in charge of their monetary information and decisions. But in countries with low digital literacy rates, such as Mali and Burkina Faso, the possibility of users becoming overly dependent on intermediaries or even being exploited is very real. Nigeria has a higher level of digital engagement, but there is still a long way to go to help users from different social and economic backgrounds.

Ethical design can benefit users by empowering them with the ability to make smart choices. For example, users can have greater control over their information with tools like variable privacy controls

or permission-based sharing of personal data. Additionally, easy-to-use interfaces that are sensitive to local cultures could enhance access and facilitate autonomy among less technologically skilled individuals.

Financial education is key to autonomy. In introducing CBDC, there must be programs that inform people on how to utilize digital channels and reject fraud. This can be expanded with the help of fintech companies and Nigeria's community organizations, and in Mali and Burkina Faso, with NGOs and local leaders taking the lead.

iii. *Harmonizing Ethical Frameworks with Local Realities*

The cultural diversity and socio-economic conditions in Mali, Burkina Faso, and Nigeria demand ethical frameworks that are both flexible and context-specific. For instance, community-based governance models, where local leaders are involved in overseeing CBDC operations, can enhance trust and acceptance in rural areas. In Nigeria, with the financial ecosystem more developed, the ethical frameworks may focus on integrating the CBDCs with existing digital payment systems while addressing emerging challenges related to algorithmic bias in AI-driven compliance tools.

Development and implementation of such frameworks are sine qua non for collaboration among stakeholders. This would, therefore, make central banks, regulators, technology providers, and community representatives work together to ensure that ethical principles are aligned with local realities. In this respect, regional organizations like the Economic Community of West African States (ECOWAS) can play a leading role in harmonizing ethical standards across these countries to ensure interoperability and trust across borders.

iv. *Balancing Ethics with Compliance and Security*

Ethics models will have to resolve how ethics, security, and compliance intersect to deal with issues of inclusivity, data privacy, and autonomy. This is particularly sensitive in those jurisdictions where institutional capacity may be weak for example, in Mali or Burkina Faso where achieving AML/CFT compliance without infringing on user privacy may be extremely challenging. The example of Nigeria's eNaira ideally demonstrates the necessity of incorporating ethical concerns in the regulatory framework and provides enlightening lessons to neighboring countries.

Such technologies, such as real-time transaction monitoring via AI, would be capable of helping CBDC systems enhance the goal of maintaining ethical standards; blockchain technology would provide secure and transparent record-keeping. Policymakers would need to guarantee that the framework is sufficiently agile to improve on an iterative basis as new opportunities and challenges become apparent.

The possibility of launching CBDCs in Mali, Burkina Faso offers a unique opportunity to reconstruct

financial systems that are equitable and ethical. They can start by taking inspiration from the e-Naira model in relation to the links between these countries on the same continent thanks to their proximity. Solving local problems and leveraging regional capabilities can also set an example for African countries in the adoption of CBDCs that is ethical. Tailored ethical standards addressing the elements of inclusiveness, data privacy, and autonomy will not only give confidence to public trust but also act as a guarantee that CBDCs foster wider socio-economic development. Mali, Burkina Faso, and Nigeria can be a trailblazing success in creating an ethical, secure, and effective digital financial system through partnership and innovation.

6.3. Recommendations for Future CBDC Implementation

6.3.1. Actionable strategies to address

The rollout of CBDCs is fraught with challenges and opportunities. In order for them to be effectively adapted and adopted in the financial system, the following are some pragmatic steps:

i. Implement Educational Campaigns to Increase Digital Literacy and Trust in CBDCs

Among the significant factors underlying opposition to introducing CBDCs is that insufficient knowledge about digital currencies by the public exists, let alone other technologies whose delivery of CBDCs is feasible. This information vacuum has a potential consequence of mistrust, further discouraging individuals from dealing with CBDCs. Institutions should, in turn:

Develop Extensive Education Programs: Such projects that outline the principles under which CBDCs operate, their benefits to be derived, and the functionalities around them. Target different demographics with specially prepared curricula. Collaboration with private sector players could amplify these efforts, as they would utilize their platforms to disseminate information down the line effectively. The World Economic Forum adds that without proper education and awareness, CBDC implementation may not achieve what it is set out to do and could introduce unintended risks.

Promote Digital and Financial Literacy: More than understanding CBDC, the general public needs to understand digital financial services. It is here that institutions should invest in programs for improving digital skills and financial literacy, especially among the most marginalized populations, who are more vulnerable to exclusion because of their low digital proficiency. According to the Payments Association, the low level of digital literacy among marginalized groups impairs the effective use of CBDCs.

Engage in Transparent Communication: Building trust requires transparency. Institutions should openly communicate the security measures in place, data privacy protocols, and the steps taken to protect users. This transparency can alleviate concerns and foster confidence in the new digital currency system.

ii. Develop Interoperable Systems for Seamless Integration Across Borders

The global nature of commerce means CBDCs should be operable across borders. Thus, institutions

should:

Implement Common Standards: Integrate at the global level on common technical and regulatory standards that facilitate interoperability. In this way, one can avoid the risk of "digital islands" and ensure CBDCs work seamlessly across borders. According to the Payments Association, interoperability between cross-border payments remains a big challenge in avoiding fragmentation of the global financial system.

Payments Association: Engage in International Collaborative Work: Participate in initiatives such as Project mBridge by BIS on cross-border transactions of CBDCs. That would provide an opportunity not only to be at the forefront but to also develop interoperable solutions. A recent development involves Saudi Arabia joining Project mBridge for scaling up CBDC settlements across borders.

Ensure Regulatory Harmonization: Cooperate with foreign regulatory bodies on the harmonization of laws and regulations on CBDCs. This alignment will help in facilitating cross-border transactions and compliance for various jurisdictions. According to BIS, the design of CBDCs must be capable of cross-border operations at the design stage itself. Further, international cooperation at that initial stage is essential.

iii. *Leveraging Artificial Intelligence for Real-Time Monitoring and Anomaly Detection in Compliance Systems*

The digital form of CBDCs makes it challenging to track transactions and maintain compliance. AI, in this regard, can perform the following:

AI-Driven Monitoring Tools: Employ AI to analyze large amounts of transaction data in real time and alert on potentially fraudulent suspicious activity instantly. This proactive measure adds an additional layer of security and integrity to the CBDC system. Industry leaders have discussed at conferences like Money20/20 USA 2024 how data and AI are converging in the creation of resilient financial networks.

Enhance Regulatory Compliance: AI can be utilized in making transactions AML/CFT compliant by identifying patterns of illicit activities. This is critical in upholding the integrity of the financial system.

Adaptive Learning: The AI systems can learn and evolve with new threats emerging so that the compliance mechanisms are effective. This is an essential part of the dynamic digital environment.

By adopting these measures, institutions can minimize the issues associated with CBDC implementation and foster an efficient, inclusive, and secure digital currency environment. Innovation in technology, public-private partnerships, and ongoing education are essential for successful implementation.

6.3.1. Balance privacy, security, and compliance

The implementation of CBDCs requires a fine balance between the protection of user privacy with high security and regulatory compliance. Such a balance is critical to fostering public trust in the use of the new digital currency and to maintaining integrity in the financial system. Advanced cryptography such

as zero-knowledge proofs and secure multiparty computing are at the heart of this effort:

i. Zero-Knowledge Proofs (ZKPs): Enabling Privacy and Security

Achieving privacy and security ZKP is a type of cryptographic protocol in which one party, called the prover, convinces another party, called the verifier, of the truth of a statement other than its validity. Here are the uses of ZKP by the CBDC:

Verification of transactions: ZKP allows transactions to be verified without the need to disclose personal information, such as who the parties involved are or how much the transaction is. This ensures the legitimacy of the transaction. This ensures the legitimacy of the transaction but protects the user's privacy. An example could be the application of ZKP cryptography that will enable “trustless privacy” in CBDCs and solve some very critical concerns related to state-backed digital currencies.

Regulatory Compliance: With ZKPs, financial institutions can prove regulatory requirements, including AML and CFT, without actually exposing information on the underlying customers. This will further help compliance officers verify that the transactions meet the legal threshold without access to confidential information.

ii. Secure Multi-Party Computation (SMPC): Collaborative Privacy Preservation

Secure multi-party computation enables several parties to compute jointly a function of their input without revealing their own input privately. In CBDC, SMPC can be applied as follows:

Distributed Transaction Processing: SMPC enables the processing of a transaction over multiple nodes without any node observing the details of all transactions. Decentralization in this manner improves security and lessens the scope of data leakage. Example: Incorporation of SMPC protocols in blockchain architectures provides transaction privacy security without any expense to computational efficiency.

Privacy-Preserving Analytics: Regulators can perform some analysis on the aggregated level of transactions data to represent fraud detection or systemic risk without ever viewing the transaction data of an individual, thereby ensuring user privacy.

iii. Balancing Privacy with Security and Compliance

ZKP and SMPC are powerful methods of privacy protection, but we need to make sure that their application does not compromise information security or regulatory compliance. This can be ensured by:

Selective disclosure: where users can reveal only the information necessary for a particular purpose. For instance, users can verify that their age is over a specific limit without revealing their actual date of birth. This demonstrates one of the key concepts of privacy-preserving digital identity systems.

Hierarchical access control systems: These rights enable controlled access to specific data, safeguarding confidential information while allowing required oversight. Round-the-clock monitoring

and assessment: There is a need to embrace an artificial intelligence-powered framework that can keep an eye on the system's functionality in real time and identify abnormal activity at the earliest opportunity. The procedure must prioritize the confidentiality of users and aim for transaction details rather than users' personal details.

iv. CBDC Implementation of Privacy Enhancing Technologies

Practically, the application in real life of ZKP and SMPC within a CBDC would include embedding the protocols of ZKP and SMPC into CBDCs to make privacy preservation natively part of the very design of the system, considering careful implementation so that system efficiency and scalability are upheld.

Regulatory Alignment: Active engagement with regulators for the deployment of cryptographic techniques in a manner to complement and support legal frameworks while allowing a compliance pathway with no compromise on user privacy.

Public Engagement: Educating stakeholders, the public, and financial institutions on how the technology works will help foster trust in these technologies' operation, which is important to increasing adoption.

v. Challenges and Considerations

ZKP and SMPC are computationally intensive and less scalable, thus challenging to implement in CBDCs. Besides, there is a strong need for standardization. All these challenges require continuous research and development activities targeting practical, efficient, and secure solutions.

There exists a sweet balance between the implementation of CBDC, ensuring that privacy, security, and compliance are appropriately considered. It is definitely possible to construct a digital currency system that safeguards user privacy, ensures sound security, and complies with regulatory requirements by leveraging state-of-the-art cryptographic techniques like zero-knowledge proofs and secure multi-party computation. A proper balance between the issues at hand will be extremely important in the successful use and sustainability of CBDCs within the ever-changing financial ecosystem.

6.4. Limitations of the Study

6.4.1. Scope and methodological constraints

Regional and stakeholder group scope constrained the study. Survey and interview data biases the study in the sense of not representing the entire global CBDC ecosystem. With a targeted regional and stakeholder group scope, this study has some limitations that affect the comprehensiveness and generalizability of the results.

i. Regional Focus

Focusing on Mali, Burkina Faso, and Nigeria, with greater emphasis on Mali and Burkina Faso, limits the scope of this presentation, as the global nature of CBDCs requires a broader perspective. The

implementation of CBDCs varies significantly across countries, depending on economic conditions, technological infrastructures, and regulatory frameworks. While some nations, such as China, have made significant progress with their digital yuan, others are still in the exploratory phase. As the International Monetary Fund highlights:

"*Interest in developing retail and wholesale CBDCs remains high worldwide, and the pace of development varies*".

ii. Stakeholder Group Selection

The research is based on evidence from particular stakeholder groups, i.e., consumers, financial institutions, or policymakers, and can be biased. Every group has varying insights and interests in CBDC introduction. Central banks, for instance, would have an interest in monetary policy implications of CBDCs, whereas consumers have an interest in usability and privacy. Partial participation results in limited understanding of multifaceted opportunities and challenges associated with CBDCs.

iii. Methodological Constraints

Data from Survey and Interview: When surveys and interviews become the key source for the data, the answers to the questions can be infected by social desirability biases or selective memories. They may give answers perceived to be expected or not remember internal information correctly, hence a shallower dataset that does not express the full complexity of CBDC adoption.

The rapidly changing nature of digital currencies is such that data collected over a certain period of time may very well become outdated rapidly. Technological changes and regulatory changes can change the landscape of CBDCs, which might render the earlier findings less relevant.

iv. Recommendations for Future Research

Include a diverse range of countries in various stages of CBDC development in order to give a more global view. Technologists, legal experts, and end-users must all be engaged in consultations to ensure that the CBDC implications are captured holistically. Quantitative data should be combined with insights from qualitative analysis to enhance the robustness and depth of analysis. By acknowledging these limitations, future research can make more constructive contributions to the discourse on CBDC implementation and broader economic and societal impacts.

6.4.2. Impact on findings interpretation

Although the findings have valuable implications, their applicability is bound to differ across different regulatory environments and technological infrastructures. Future studies would have to consider a broader dimension to validate such conclusions.

Emphasis on specific areas and stakeholder groups sacrifices generality to a great degree to different regulatory environments and technological infrastructures.

i. *Different Regulatory Environments*

Most regulatory environments differ significantly from state to state regarding CBDCs. This is due to the fact that there are certain countries with highly regarded and well-established legal systems that embrace these digital currencies, whereas others have just started their journey towards regulation. This can actually have a significant effect on the rollout and the adoption of CBDCs. Bank for International Settlements studies demonstrate how legal issues are one of the most critical issues in relation to the implementation of CBDCs due to the speed with which innovation occurs within the space, rendering any existing legislation and regulations liable to ongoing amendments.

ii. *Bank for International Settlements: Technological Infrastructure Differences*

The technological readiness of the nation is one of the most essential elements in the effective launch of CBDCs. For instance, the majority of developed countries have improved digital infrastructure like high internet coverage and strong cybersecurity, hence largely favoring the implementation of CBDCs. Poorer countries may have very limited digital infrastructure and lower levels of digital literacy, which might constitute a barrier to the effective adoption of CBDCs. For instance, most countries in Africa face challenges while trying to develop effective legal and regulatory frameworks for CBDCs; it is mostly attributed to inadequate capacity as well as experience in issues related to regulating financial technology and digital currency.

iii. *Implications for Interpretation of Findings*

Given these differences, the general applicability of the conclusions of this study might be limited. Policies that have been successful in areas where technological infrastructure is highly developed and regulatory environments are permissive may not have similar effects in other places without such advantages. Thus, although the study is insightful, its applicability in different contexts is limited.

6.4.3. Context-Dependent Restrictions

Interpretations of findings on the introduction of CBDCs in Africa, therefore, in the cases of Mali, Burkina Faso, and Nigeria, should be done with a due consideration of the peculiar set of socio-economic and technological conditions obtaining in each context. Those contextual factors sculpt not only the feasibility of the adoption of CBDC but also how findings from this study can be applied and understood.

i. *Socio-Economic Variations and Their Impacts*

One major limitation is the socio-economic disparity among the countries: while Nigeria is ranked as the biggest economy in Africa with a much-developed financial sector, Mali and Burkina Faso have more pronounced poverty and less strong financial infrastructures. Those disparities imply that findings might be interpreted in very distinct ways within each of those contexts most notably with regard to issues of the scalability and accessibility of CBDCs. For example:

Financial Exclusion: Most of the population in Mali and Burkina Faso is unbanked, which will make

it very hard to gauge how ready these regions might be to adopt CBDCs. Results underlining digital inclusion would have even more resonance in these settings, though they also shed light on the challenge of overcoming gaps in infrastructure and literacy.

Income Inequality: The uneven distribution of income and wealth in the three countries means that early CBDC use might skew to higher-income, urban populations at the expense of poorer segments of society. That could result in the research overestimating CBDC adoption potential and underestimating rural and low-income challenges.

ii. Technological Readiness

Another limitation is the technological gap among the three countries: whereas Nigeria has achieved some level of mobile money adoption and fintech innovation, Mali and Burkina Faso are far behind with respect to internet and mobile connectivity. These technological disparities have implications for almost all major aspects of CBDC implementation, including

In the case of Mali and Burkina Faso, poor Internet access makes this even more relevant, but the findings on the feasibility of offline CBDC transactions suggest that the lack of technological infrastructure in these countries may have overstated the difficulties while understating the solutions available through innovative offline technologies. High mobile penetration in Nigeria provides a strong base for CBDC adoption. However, findings that depend on mobile accessibility will apply less to Mali and Burkina Faso, where access to mobile devices is more constrained.

iii. Cultural and Institutional Differences

The institutional and cultural dimensions also come to the forefront when interpreting findings. The fate of any adoption of CBDCs will be dependent on the character of a country's regulatory regime, its government structure, as well as confidence in financial institutions by the populace.

Regulatory Framework: The case of Nigeria has more detailed regulatory frameworks in digital financial services compared to those of Mali and Burkina Faso. Such a difference calls for an interpretation of findings in respect to compliance and regulation in their specific institutional contexts in these countries.

Public Trust: The findings related to user adoption of CBDCs in Mali and Burkina Faso have to consider these trust deficits in formal financial institutions and government initiatives. For example, recommendations related to transparency and stakeholder engagement would carry more weight in those countries.

iv. Influence of Political Stability

The nations' political stability also impacts interpretation of results. While Nigeria has localized unrest, Mali and Burkina Faso have faced large-scale political crises, including coups and insurgencies. These are variables which impact implementation and trust-building for CBDCs:

Security Concerns: Political instability can also deflect investment away from technological advancement and public sensitization campaigns, making implementation of inclusivity and accessibility results more challenging.

Stakeholder Coordination: The fragmented governance structures in both Mali and Burkina Faso complicate efforts to align CBDC initiatives with global standards and local needs, limiting the applicability of recommendations for coordinated policymaking.

v. Generalization of Findings Challenges in

Given such different socio-economic and technological landscapes, generalizing findings across the three countries is very challenging. For example:

Economic Ecosystems: Findings emphasizing the role of fintech partnerships in driving CBDC adoption or improvement may be highly relevant in Nigeria, where such partnerships are strong, but less so in Mali and Burkina Faso, where the fintech sector is still nascent.

Adoption Rates: Projections of CBDC adoption or improvement rates based on the relatively advanced digital ecosystem of Nigeria may not reflect the slower pace that can be expected in Mali and Burkina Faso.

vi. Data Gaps and Their Implications

Availability and quality of data from these regions is another limitation. Inconsistent or incomplete data on financial inclusion, digital literacy, and technological adoption rates in Mali and Burkina Faso may introduce biases in interpreting findings. For example: Results from surveys may overrepresent urban and digital literates at the cost of rural and marginalized populations.

At the same time, poor data granularity on regional variation within each country makes it difficult to adapt findings to specific local contexts, whether rural versus urban or related to socio-economic groups. Implications for Interpretation These contextual boundaries served to bring perspective to the need for caution in interpretation of the findings within the African context. Although the overall themes of inclusivity, accessibility, and ethical implementation are most applicable, their implementation must be sensitive to the unique challenges and possibilities of each country. For instance: It would be more an issue of constructing basic infrastructure, establishing digital literacy, and acquiring the trust of locals via local outreach campaigns in Mali and Burkina Faso. In Nigeria, it would be an issue of scaling up current digital environments, interoperating the CBDCs with mobile money platforms, and handling more sophisticated compliance and cybersecurity issues. Conclusion These are underscored by the socio-economic, technological, and institutional differences between Mali, Burkina Faso, and Nigeria. Noting these limitations is very instrumental for policymakers, financial institutions, and researchers in each country to implement policies to tailor CBDC implementation strategies to the peculiar needs and

challenges of the specific countries. This is only done when context is taken into consideration; otherwise, the full potential of CBDCs in fostering financial inclusion, economic growth, and technological innovation in Africa would be a fallacy.

6.5. Directions for Future Research:

Because CBDC is a rapidly evolving field of study, there are many aspects that require additional research to bridge the gap between essential knowledge and practice. This paper establishes a foundation for the ethical, compliance, and cybersecurity aspects of CBDC implementation, but at the same time reflects the complexity and interdependence of the field, which is an ongoing topic of research. The following have been highlighted as key areas of further understanding to ensure that CBDCs are effective, inclusive, and secure.

6.5.1. Suggest areas for further investigation:

CBDCs exist at the intersection of financial technology, governance, and socio-economic systems. The nature of their implementation and effects is influenced by factors that range from regulatory frameworks to cultural perceptions of digital financial systems. More critically, future research should unpack these factors for their nuances and implications to provide actionable strategies for central banks, policymakers, and financial institutions. Three areas have emerged as important: regional differences in adoption, the impact of socio-economic factors on less privileged groups, and the question of the sustainability of privacy-preserving technologies.

6.5.2. Regional variations in adoption

The adoption and success of CBDCs are not the same across regions, since the diffusion is deeply influenced by the different socio-political, economic, and infrastructural characteristics. It is important for future research to look into the way such factors mold the implementation and acceptance of the CBDC in various parts of the world.

- ***Socio-Political Factors***

Regional variation in the pace of CBDC adoption has been undergirded by unequal degrees of government support, public trust, and regulatory preparedness. CBDCs will take off quicker in those parts of the world that enjoy high levels of political stability and institutional trust, like parts of Europe and East Asia. Conversely, regions characterized by unsteady governance structures or low public trust in the central institution may witness CBDC adoption at a much more sluggish and laborious pace. Future studies should examine how governments can cultivate trust and enabling environments for the implementation of CBDCs.

- ***Economic Factors***

Besides the many factors identified above, economic factors also play a very key role in shaping CBDC adoption. For instance, developed economies with robust financial systems and high smartphone penetration, such as those of North America and Europe, will have an easier time integrating CBDCs into their payment infrastructures. Conversely, developing economies are hampered by spotty digital infrastructure, a lack of financial literacy among a large part of the population, and high levels of informal economic activity. It is also important that research will be directed at identifying tailored approaches to CBDC design and implementation which could mitigate these economic disparities. Technological Infrastructure The availability and quality of digital infrastructure, including internet access and mobile penetration, are critical determinants of CBDC adoption.

Regions with advanced technological ecosystems, such as South Korea and Singapore, can leverage their existing infrastructure to support CBDC deployment.
On the other hand, regions like Sub-Saharan Africa have underdeveloped infrastructure and need huge investments in digital connectivity and mobile access. Research should focus on strategies that will help bridge these technological gaps and assure equitable access to CBDCs across regions. Cultural and Behavioural Factors Not surprisingly, cultural attitudes toward digital currencies and the trust in technologies widely differ across regions. For example, the push for digital payments by the government has meant that digital financial systems have gained wide acceptance in China. On the other hand, in places where cash remains the dominant mode of transaction, it is very likely to find CBDCs getting less acceptance. Future studies need to examine how cultural and behavioral factors influence user acceptance and adoption of CBDCs. These regional differences will, therefore, give researchers valuable insights into the contextual drivers of CBDC adoption and provide recommendations on how to best adjust the implementation strategies to the unique regional needs.

6.5.3. Socio-economic impacts on underserved groups

One of the most potential uses of CBDCs, in fact, is the hope of providing enhanced financial inclusion by digital access to financial services for excluded communities. Yet, to fulfill this hope, much more needs to be understood about the probable socio-economic effects of CBDCs on these very communities.

i. Financial Exclusion

Many underserved communities, especially in developing countries, face barriers to accessing traditional financial services, such as high fees, lack of identification documents and limited access to physical banking services. CBDCs provide low-cost, accessible digital payment systems to address these barriers. Future research should assess how CBDCs can be built to meet the specific needs of underserved communities, such as rural and deprived areas.

ii. *Economic Inequality*

Though CBDCs can potentially reduce economic inequality, if poorly designed, they can enhance it. For example, solutions that require smartphones or reliable internet access could disenfranchise those without them. Studies should examine ways to counter such risks and render CBDC systems inclusive and equitable.

iii. *Digital Literacy*

Digital literacy has a specific enabling role to play in the successful utilization of CBDCs. Absent sufficient awareness and proficiency, certain segments of the population are not able to comprehend, or will not be in a position to use and engage with, such types of digital financial infrastructure and associated applications. Additional research must capture the function of education and training programs to realize heightened digital literacy in empowering underprivileged populations.

iv. *Gender Disparities*

Gender disparities in access to financial services are well-documented, with women facing more significant barriers to financial inclusion compared with men in many regions. CBDCs can help close such gaps by giving women greater control over their money and less reliance on intermediaries. Issues that researchers should study include the gender-specific impact of CBDCs and the ways in which gender equity might be improved in digital financial systems.

By studying such socio-economic impacts that the CBDCs have, especially on less represented communities, researchers are best equipped to avail valuable insights for ensuring that any digital currency that may be used in the interest of financial inclusion succeeds in cutting disparities.

6.5.4. Ethical Adoption for Africa

Any introduction of CBDCs into Africa in general, and Mali, Burkina Faso in particular, requires a prior profound analysis of the regional political stability, economic arrangements, and cultural habits that would affect its usage and adoption. The present study gives some tentative insights into these dynamics; more research is required to outline in detail the manner in which such factors will complicate the process of CBDC adoption in different African contexts.

1) Political Stability and CBDC Adoption

The major determinant of CBDC adoption in Africa is political stability. The past few years have seen large political upheavals rocking countries like Mali and Burkina Faso with coups, insurgencies, and governance challenges. Such conditions give way to an environment of uncertainty that may be unfavorable for the trust required for successful CBDC rollouts. This is true for the case:

Maly and Burkina Faso: Political instability in these countries may delay the development and deployment of CBDC infrastructure. More research is needed to explore how periods of instability affect

stakeholder collaboration, public awareness campaigns, and regulatory coordination necessary for CBDC implementation.

Nigeria: Despite Nigeria's relative political stability, local conflicts in certain areas could potentially inhibit the improvement of the e-Naira. Future research should explore the effects of localized instability on the adoption and trust of digital financial systems.

The relationship between political stability and the adoption of CBDCs would assist policymakers and institutions in designing stable strategies that could survive the tests of time amidst seasons of political instability, while not derailing progress towards digital financial inclusion.

2) **Economic Frameworks and Regional Flexibility**

These varied African economic structures pose both opportunities and challenges for CBDC adoption. Nigeria, Africa's largest economy, has a more evolved financial system and greater fintech innovation relative to Mali and Burkina Faso, economies that are more agrarian- and informal trade-based economies. These structural differences require special means:

For Nigeria: The prevailing state of fintech in Nigeria already situates the country at the forefront of CBDC adoption. Researchers should try to see how prevailing fintech partnerships and mobile payment platforms can be integrated further with CBDC initiatives in order to achieve scale.

For Mali and Burkina Faso: These economies are confronted with such constraints as restricted access to banking and high informality. Future work will consider the potential of CBDC design to accommodate informal trade networks and bring access to digital financial services to excluded groups.

In addition, research should be done on how CBDC usage patterns may diverge with respect to economic disparities: for example, whether urban elites are more likely to use CBDCs than rural communities. That would shed light on whether CBDCs bridge economic divides or exacerbate them.

i. *Cultural Norms and Societal Confidence*

The cultural norms of each society play a very big role in the reception of new technologies, including CBDCs. In many African countries, traditional reliance on cash and suspicion of formal banking systems are large impediments to the adoption of digital currencies. There is a need to explore such cultural dynamics in order to understand public trust and behavioral readiness for CBDCs.

Trust in financial institutions: In general, there is low trust in financial institutions in both Mali and Burkina Faso, partly as a result of past experiences with corruption and inefficiency. Future research should show how CBDC initiatives might embed transparency and community engagement to help re-establish this trust.

Technological Familiarity: The cultural acceptance of mobile money systems in Nigeria, such as Paga

and M-Pesa, suggests a pathway for CBDC adoption. What implications these cultural precedents can have for CBDC design and implementation strategies in similar contexts should be investigated.

Cross-border Cooperation and Regional Cohesion: The implementation of CBDCs in Africa raises issues related to regional integration and cross-border cooperation. In the case of the West African Economic and Monetary Union (WAEMU), Mali and Burkina Faso share a common currency, the CFA franc, and a common regulatory framework, while Nigeria is independent with its own currency, the naira. This divergence brings along certain challenges but also opportunities: WAEMU Countries: Future research will be directed to explain how regional monetary unions, like WAEMU, could support CBDC adoption with common infrastructure and harmonized policies; that is, to research the feasibility of a regional CBDC that complements the CFA franc to foster financial integration.

Nigeria Further research is needed to ascertain how Nigeria's independent monetary policy affects its ability to cooperate with its neighbors in cross-border CBDC efforts. Knowledge of these dynamics could help devise instruments to promote regional interoperability and cooperation.

ii. *Policy and Governance Implications*

Effective governance and policy frameworks are essential for CBDC adoption, particularly in regions with diverse regulatory environments. Mali and Burkina Faso may face challenges in establishing the necessary regulatory infrastructure, while Nigeria’s more advanced regulatory framework provides a model for other countries in the region. Future research should focus on:

Nigeria's regulatory framework has also offered a glimpse into systems that can further be used in less developed environments. Analyzing how global standards for CBDCs can be mapped to local governance systems to facilitate compliance and operational effectiveness. Conclusion The political, economic, and cultural situations of Mali, Burkina Faso, and Nigeria highlight the intricacies of CBDC adoption in Africa. This thesis has revealed some of the main opportunities and challenges, but further research is necessary in order to get into greater detail on these regional variations and provide recommendations for policymakers, financial institutions, and technology providers that can be implemented. In doing so, such research can assist in creating CBDCs that are efficient, fair, and inclusive, hence their certain success in the diversified African financial ecosystems.

6.5.5. Sustainability of privacy-preserving technologies

Privacy-preserving technologies are a given requirement for the security and trust of CBDC systems. However, substantial challenges remain regarding their long-term sustainability and scalability, which calls for further investigation.

i. *Technological Feasibility*

Of these, homomorphic encryption and zero-knowledge proofs are emerging technologies that could be a solution to user privacy in CBDC systems. Those technologies, however, are extremely computationally intensive and might not be feasible on a large scale. Future research must be directed to whatever advancements are achieved in those technologies that would make them efficient and scalable.

ii. *Regulatory Compatibility*

Adherence to regulatory stipulations, such as AML/CFT/CPF, must be ensured while privacy is maintained. How to implement privacy-enhancing technologies within CBDC systems is an issue that research needs to contend with to achieve a compromise between regulators and users.

iii. *Cost-Effectiveness*

The majority of privacy-enhancing technologies are costly to adopt, particularly in emerging economies. Future research should therefore emphasize economically viable methods through which such technologies can be adopted, as well as other strategies that provide sufficient protection at little cost.

iv. *User Trust and Adoption*

Success in privacy-preserving technologies relies on users' trust and uptake. When users find the technologies to be opaque or incomprehensible, they will hesitate to utilize CBDC systems. Studies need to focus on determining how to ensure that privacy-preserving technologies are easy to use and transparent to generate trust and confidence among users.

v. *Sustainability and Environmental Impact*

The computational requirements of these privacy preserving technologies have severe environmental implications. Assuming that a CBDC gets close to a mass market, the energy consumed by these systems could be substantial. Sustainable means of deployment of these privacy-enabling technologies-a means either to harness renewable resources or to make new, energy-efficient algorithms-should be studied.
By addressing these challenges, researchers can contribute to the development of sustainable, scalable, and user-friendly privacy-enhancing technologies that will facilitate the long-term viability of CBDCs.

Future studies on regional disparities in CBDC adoption, socio-economic effects on underserved communities, and the viability of privacy-preserving technologies will be important to address the challenges and fully harness the potential of CBDCs. In these domains, researchers can make valuable contributions by providing critical insights and feasible solutions for the ethical, secure, and inclusive deployment of CBDCs, and hence reshape the world financial landscape.

6.6. Contributions to Knowledge

6.6.1. Highlight unique contributions to CBDC research

This thesis presents a novel Ethical-Security Integration Framework (ESIF) that fills the gap between regulatory compliance issues and cybersecurity practice in CBDC deployment.

In modern days, CBDCs introduced within the realm of FinTech can be viewed as nothing but a revolution. However, the deployment of CBDC can be materialized only if large insight about different ethical issues is obtained relating to compliance and cybersecurity matters. Additionally, it develops fresh new frameworks that allow providing operational tools to catch certain key problems within CBDC studies. Results obtained from this work will fill in the knowledge gap that exists but also provide further opportunities for both investigation and implementation.

i. Highlight Unique Contributions to CBDC Research

The main contributions of the thesis relate to the formulation of the ESIF, which is new in tackling the twin imperatives of ethical considerations and cybersecurity practices regarding the implementation of CBDCs. The ESIF is new because it brings together areas usually treated in isolation, putting together an integrated perspective necessary for CBDC systems that are complicated and multifaceted.

ii. Bridging Ethics and Cybersecurity

ESIF was well-placed to combine ethical factors, including privacy, inclusivity, and transparency, with strong cybersecurity measures. As a framework, it incorporated ethical factors into the underlying design of CBDC systems to ensure that user rights would be prioritized without undermining security or operational integrity.

iii. Balancing Privacy and Compliance

The model addresses one of the most salient conflicts surrounding CBDCs - finding a middle ground between user privacy and regulatory requirements ESIF has demonstrated how financial institutions can meet regulatory requirements without compromising user trust by incorporating real-time monitoring capabilities for AML/CFT/CPF compliance, and by incorporating privacy-enhancing technologies, including zero-knowledge proofing and anonymization techniques, ESIF has demonstrated how financial institutions can meet regulatory requirements without compromising user trust.

iv. Adaptability Across Contexts

ESIF is designed to be adaptable in various socio-political and technological environments. As its modular design enables it to be adjusted to diverse regional and institutional requirements, it can operate very effectively in a diverse range of setups for financial institutions and central banks.

v. Advancing Academic Discourse

This thesis thus provides novel contributions by integrating different threads of literature sourced from ethical philosophy, best cybersecurity practices, and the financial regulations' field that lead to an extension of academic scholarship in this area. It hence provides a theoretical foundation for continued

research work on ethical and security matters linked to digital financial systems.

6.6.1. Emphasize practical relevance of developed models

It therefore provides regulators and financial institutions with practical insights into how to surmount some of the ethical and compliance challenges of CBDCs. Theoretically, this paper contributes, and frameworks and strategies that can provide positive answers might be given to regulators, financial institutions, and technology providers. These models have been designed in such a way that they mitigate ethical, compliance, and operational challenges that come with the implementation of CBDCs.

i. Regulatory Guidance

These recommended pathways introduce some of the ways that policymakers can introduce balanced regulatory frameworks for innovation and oversight. The coherence in domestic and global regulations certainly addresses issues with inconsistency and interoperability standing in the way of CBDC cross-border transactions. It also describes how regulators might introduce AML/CFT/CPF protocols without injury to user privacy.

ii. Institutional Preparedness

The dissertation provides a raft of holistic financial plans that will further the level of preparedness on an institutional scale by leveraging both sequenced rollout approaches, which are coupled with necessary investments for renovating legacies, incorporating newer technologies using AI-driven fraud detection, blockchain-driven transparency among others.

iii. Privacy-Preserving Technologies

Witnessing the important function of privacy in facilitating users to trust, this thesis shifts gear to the practicality of using privacy-enhancing technologies. The models suggested herein give the perspective of how such technologies, such as homomorphic encryption and decentralized storage networks, would be utilized by any institution in protecting user data in meeting the demands of the regulators.

iv. Financial Inclusion

The study highlights actionable recommendations for the use of CBDCs for financial inclusion, especially for underserved communities: from creating user-friendly interfaces for areas with low internet penetration, to offline capabilities and improving digital literacy, to education campaigns.

v. Stakeholder Collaboration

This paper highlights the feasibility of a collaborative governance framework between central banks, regulators, private sector experts and end-users. Through participatory decision-making, the proposed framework will help ensure that the design and management of the CBDC system is optimally structured to meet the requirements of a wide range of stakeholders.

vi. Future-Proofing CBDC Systems

The proposed framework takes into account the evolving technological and regulatory environment, which is intended to adapt and evolve as CBDC systems develop. This includes the integration of new technologies such as artificial intelligence and quantum computing, as well as the adoption of environmentally friendly and sustainability-oriented practices.

In general, this thesis presents a double contribution to CBDC research. The Ethical-Security Integration Framework (ESIF) is a new theoretical contribution, delivering a comprehensive approach to mapping ethicality onto cybersecurity. Meanwhile, the real-life applicability of the proposed models ensures their direct application in addressing CBDC implementation challenges. These contributions build on the existing knowledge of CBDCs and establish a robust basis for research and practice going forward in a manner that will help achieve an ethical, secure, and inclusive digital financial system.

6.7. Closing Remarks

6.7.1. Reflect on CBDCs' role in global finance

CBDCs will surely change the game in global finance and present a paradigm shift as far as the interaction between governments, institutions, and individuals in the financial ecosystem goes. Being a means to digitize fiat currencies, CBDC has great prospects to enhance transparency, operational efficiency, and financial inclusion with regard to some of the most knotty economic systems problems facing the present century.

Above all, CBDCs promise modernization of financial systems by minimizing dependence on the conventional banking infrastructure and thus allow for seamless and cost-effective methods of payments. This would immensely raise international trade because it enables practically instantaneous cross-border transactions with a minimum barrier to the transactions in comparison to existing settlement mechanisms. Further, traceability of the transactions provided through CBDCs institutes unprecedented transparency in money flows, which has become so handy in combat money laundering, financing terrorism, and other crimes.

However, there is a number of challenges to be faced regarding CBDCs. This thesis demonstrated how ethical dilemmas with regard to privacy, autonomy, and user control are at risk if not handled in such a manner as to prevent unintended consequences-such as increased surveillance or financial exclusion. Similarly, robust cybersecurity frameworks will be required to defend against the increasingly complex threats in digital fraud, hacking, and system vulnerabilities.

However, CBDC is not only a technological innovation, but also a strategic opportunity for central banks to reaffirm their relevance in an increasingly digitalized economy. If CBDCs can overcome various

ethical, compliance and security challenges, they can serve as an important tool in reshaping the global financial landscape for stability, inclusion and innovation.

6.7.2. Distinctive Contributions to CBDC Research in Africa

This research contributes meaningfully to the understanding of CBDC deployment in the African context, which has special emphasis on challenges peculiar to Mali, Burkina Faso, and Nigeria. This study offers new insights into the design, implementation, and administration of CBDCs tailor-made for an African economy in consideration of the socio-political, economic, and technological environment of these countries.

i. Regional Issues and Concerns in CBDC Implementation

This thus is an important paper, shedding light on the regional-specific challenges that impinge on CBDC adoption in Africa. This study presents how, for Mali and Burkina Faso, infrastructural deficits such as limited access to digital connectivity and underdeveloped financial systems act as barriers to CBDC deployment. The identified barriers show the need for solutions including offline functionality, low-cost mobile platforms, and simplified user interfaces for use in low-tech environments.

One also looks at the more developed Fintech ecosystem in Nigeria to understand how existing mobile money platforms and widespread smartphone penetration can act as a springboard for CBDC adoption. It also brings to the fore the challenges of low trust in government-led financial initiatives and regional disparities in digital literacy, which have to be addressed to make access equitable.

ii. Ethical Aspects Customized for African Contexts

Such a thesis would go a long way in contributing to the international discourse on CBDCs by bringing ethical considerations, normally at the margin of discussions in African contexts, to the fore. It explores topics of financial exclusion, privacy rights, and user autonomy under specific regional cultural and economic conditions.

For instance, the research underlines the critical need for protecting individual privacy while at the same time ensuring enough transaction traceability in order to comply with the obligations related to AML/CFT/CPF regulations.

This paper responds to the call for the development of an Ethical-Security Integration Framework (ESIF) that provides a structured approach to balancing these competing priorities. The framework is particularly relevant in regions like Africa, where there is a huge variation in regulatory capacities and cultural norms that reinforce community trust and informal financial systems.

iii. Framework for Financial Inclusion

One of the most striking contributions this research makes is the emphasis on financial inclusivity as

one of the core objectives of CBDC implementation in Africa. This study, through its research, identifies ways in which the gap between digital finance and underserved communities without access to traditional banking systems in many populations of Mali, Burkina Faso, and Nigeria can be bridged.
It affirms, through the CBDC advocacy, multilingual interfaces, and very low transaction fees, the foundation that will make CBDCs accessible to very marginalized groups, especially those in rural areas and women. This could also underline the potential of CBDCs in integrating informal economies into the formal financial system especially a must for countries like Mali and Burkina Faso. This will help bring more stability to the economy, better collection of revenues by way of taxation, and financial security to citizens.

iv. Regional cooperation – moving the dialogue forward

One of the most relevant contributions that this work makes is in the focus of regional cooperation in the implementation of CBDCs. More precisely, for countries belonging to the West African Economic and Monetary Union WAEMU that is, Mali and Burkina Faso the study analyzes the feasibility of creating a regional, homogeneous CBDC that would complement the CFA franc.

This research provides the foundation for a number of discussions on regional financial integration through its examination of the benefits and challenges involved. On the other hand, it discusses how the independent monetary policies of Nigeria may be relevant to affect its capacity in engaging with cross-border CBDCs. The insights are valuable for policymakers and central banks working toward harmonizing the digital currency framework across very different regulatory environments.

This research further enriches the technological dialogue surrounding CBDCs by examining the potential adaptation of innovations such as blockchain, artificial intelligence (AI), and privacy-preserving technologies within African settings. With a focus on the scalability and flexibility of CBDC frameworks, this study offers practical suggestions for the development of robust infrastructures capable of evolving in tandem with technological progress and regulatory transformations.

These findings underline the requirement for low-bandwidth solutions and secure, lightweight mobile applications features especially critical for rural areas in Mali and Burkina Faso. This study has found that this can be used in Nigeria to improve CBDC at scale using existing fintech platforms.

v. Practical Policy Recommendations

In conclusion, this study does indeed make a unique contribution in that it provides policy recommendations tailored to the African context.

Establishing collaborative governance arrangements including fintech innovators and local communities, besides the traditional central banks. Develop regulatory guidance balancing compliance

with inclusivity and privacy considerations. Implementing capacity-building programs to enhance financial literacy and digital skills for underserved populations. These recommendations not only address the short-term challenges of implementation but also lay the foundation for sustainable CBDC ecosystems in Africa. Conclusion This, therefore, is a big contribution to the global discourse on CBDCs in light of unique challenges and opportunities in Africa. A more generalized road map toward CBDC implementation within Africa could take into consideration the very divergent contexts faced in such places as infrastructural, ethical, and regulatory issues specific to Mali, Burkina Faso, and Nigeria. The presented frameworks and strategies are relevant not just to the countries chosen for their analysis but are actually highly applicable to many of the other developing regions and situate this work, in this way, within the notable contributions of work at the level of digital financial systems.

Bibliography

Ahnert, T., Assenmacher, K., Hoffmann, P., Leonello, A., Monnet, C., & Porcellacchia, D. (2022). The economics of central bank digital currency (ECB Working Paper Series No. 2713). European Central Bank.

Agrawal, R., & Gupta, N. (2021). Transforming cybersecurity solutions using blockchain. Springer Nature Singapore Pte Ltd. https://doi.org/10.1007/978-981-33-6858-3

Ashfaq, M., Hasan, R., & Mercon, J. (2023). *Central bank digital currencies and the global financial system: Theory and practice*. Walter de Gruyter GmbH. https://doi.org/10.1515/9783110982398

Ashurst, S., Tempesta, S., & Kampakis, S. (2022). *Blockchain applied: Practical technology and use cases of enterprise blockchain for the real world*. Routledge. https://doi.org/10.4324/9781003132592

Bello, A. U. (2016). *Improving anti-money laundering compliance: Self-protecting theory and money laundering reporting officers*. Palgrave Macmillan. https://doi.org/10.1007/978-3-319-43264-9

Bilotta, N., & Botti, F. (2021). *The (near) future of central bank digital currencies: Risks and opportunities for the global economy and society*. Peter Lang AG, International Academic Publishers.

Bilotta, N., & Botti, F. (2024). *The (near) future of CBDCs: Risks and opportunities for the global economy and society* (Vol. 7). Peter Lang GmbH. https://doi.org/10.3726/b18087

Bindseil, U., & Fotia, A. (2021). *Introduction to central banking*. Springer International Publishing AG.

Bhatia, N. (2021). Layered money: From gold and dollars to Bitcoin and central bank digital currencies. Nik Bhatia.

Biersteker, T. J., & Eckert, S. E. (Eds.). (2008). Countering the financing of terrorism. Routledge, Taylor & Francis Group.

Bordo, M. D., & Levin, A. T. (2017). Central bank digital currency and the future of monetary policy (Working Paper 23711). National Bureau of Economic Research. http://www.nber.org/papers/w23711

Brink News. (2021, August 9). *1.7 billion people don't have a bank account but mobile banking could change their lives*. https://www.brinknews.com/bridging-the-digital-divide-to-widen-financial-services-in-central-asia/

Cox, D. (2014). Handbook of anti-money laundering. John Wiley & Sons, Ltd.

Creswell, J. W. (2009). *Research design: Qualitative, quantitative, and mixed methods approaches* (3rd ed.). SAGE Publications.

Daymon, C., & Holloway, I. (2002). Qualitative research methods in public relations and marketing communications. Routledge.

Fetiniuc, V., & Luchian, I. (2014). *Banking ethics: Main conceptions and problems*. *Annals of the University of Petroşani, Economics, 14*. https://www.upet.ro/annals/economics/pdf/2014/part1/Fetiniuc-Luchian.pdf

Heckel, M., & Waldenberger, F. (2022). *The future of financial systems in the digital age: Perspectives from Europe and Japan*. Springer. https://doi.org/10.1007/978-981-16-7830-1

International Bank for Reconstruction and Development / The World Bank. (2009). [Publication information not provided]. World Bank. https://www.worldbank.org

Johnson, R. B., & Christensen, L. (2020). *Educational research: Quantitative, qualitative, and mixed approaches* (7th ed.). SAGE Publications.

Kuada, J. (2012). *Research methodology: A project guide for university students*. Samfundslitteratur.

Leavy, P. (2017). Research design: Quantitative, qualitative, mixed methods, arts-based, and community-based participatory research approaches. The Guilford Press.

Leedy, P. D., Ormrod, J. E., & Johnson, L. R. (2019). *Practical research: Planning and design* (12th ed.). Pearson.

Lilley, P. (2006). Dirty dealing: The untold truth about global money laundering, international crime and terrorism (3rd ed.). Kogan Page.

Maguire, M., & Delahunt, B. (2017). *Doing a thematic analysis: A practical, step-by-step guide for learning and teaching scholars*. *AISHE-J, 8*(3). https://ojs.aishe.org/index.php/aishe-j/article/download/335/553/1557

Mendo Antunez, M. (2023). *Understanding CBDC: Money and blockchain*. BoD – Books on Demand GmbH.

Miles, M. B., & Huberman, A. M. (1994). *Qualitative data analysis: An expanded sourcebook* (2nd ed.). SAGE Publications.

Nakamoto, S. (2008). *Bitcoin: A peer-to-peer electronic cash system*. Retrieved from https://www.sec.gov/comments/s7-04-23/s70423-290181-707862.pdf

Niepelt, D. (Ed.). (2021). *Central bank digital currency: Considerations, projects, outlook*. Centre for Economic Policy Research. https://www.cepr.org

Prastyanti, R. A., Rezi, & Rahayu, I. (n.d.). Ethical fintech is a new way of banking. Universitas Duta Bangsa Surakarta, Indonesia. https://doi.org/10.56457/jimk.v11i1.353

Ratten, V. (2023). *Research methodologies for business management* (1st ed.). Routledge.

Rebé, N. (Ed.). (2023). *Cyber-laundering: International policies and practices*. World Scientific Publishing Europe Ltd.

Rovera, C. (2024). Ethics in banking - Is it possible? Springer Nature. https://doi.org/10.1007/978-3-031-22148-4

Saunders, M. N. K., Lewis, P., & Thornhill, A. (2023). *Research methods for business students* (9th ed.). Pearson Education Limited.

Schoonenboom, J., & Johnson, R. B. (2017). *How to construct a mixed methods research design*. *Kölner Zeitschrift für Soziologie und Sozialpsychologie, 69*, 107–131. https://pubmed.ncbi.nlm.nih.gov/28989188/

Sylla, M. (2023). *Banking compliance in Senegal and in the UMOA zone: How can Senegalese banks and those in the UMOA zone establish and implement a compliance framework?* Publishroom Factory.

Tadis, G. (2019). *An investigation of business ethics practice and its performance in the case of Lion International Bank (LIB) S.C.* [Master's thesis, St. Mary's University]. St. Mary's University Repository. http://www.repository.smuc.edu.et/bitstream/123456789/4818/1/Final%20Thesis%20Print.pdf

V. S., A., Asharaf, S., Goldston, J., & Williams, S. (Eds.). (2023). Blockchain for Industry 4.0 - Emergence, challenges, and opportunities. CRC Press.

Van Cleeff, A. (2015). *Physical and digital security mechanisms: Properties, combinations and trade-offs* (Doctoral dissertation). University of Twente. https://doi.org/10.3990/1.9789036538848

Walker, T., & Morris, L. (2021). The handbook of banking technology. John Wiley & Sons Ltd.

Wilson, E. (2017). *School-based research: A guide for education students* (3rd ed.). SAGE Publications Ltd.

Yamaoka, H. (2019). The future of central banking. *Accounting, Economics, and Law: A Convivium*. Advance

online publication. https://doi.org/10.1515/ael-2019-0003

Yanagawa, N., & Yamaoka, H. (2019). *Digital innovation, data revolution, and central bank digital currency* (Bank of Japan Working Paper No. 19-E-2). Bank of Japan. https://www.boj.or.jp/en/research/wps_rev/wps_2019/data/wp19e02.pdf

Literature and Academic Journals

Academic Journals				
SN	**Document**	**Link**	**Published**	**Key Insight**
1	Technology Effects on Emerging Economies'	Selinus Library	Amr Aboelenein – Selinus University, 2023	This dissertation analyzes the role of fintech and digital transformation in advancing financial services and economic development

Academic Journals				
SN	**Document**	**Link**	**Published**	**Key Insight**
	Financial Services and Economic Development: The case of Egypt and India			in Egypt and India. It highlights how digital financial inclusion, mobile banking, and AI-driven financial services foster economic growth, while pointing out the challenges of regulatory frameworks and digital infrastructure in both nations.
2	Impact of CBDC Implementation on Emerging Markets	Selinus Library	Jamilu Muhammad Aliyu – Selinus University, 2023	This dissertation provides insights into the implementation of Central Bank Digital Currency in emerging markets. It emphasizes how CBDC adoption can enhance financial inclusion and stability while addressing potential economic risks, regulatory challenges, and technological barriers.
3	A Comparative Study of Electronic Money's Privacy Policies and Privacy Laws	Selinus Library	Guanru Liu – Queen's University, 2011	This thesis provides a comparative analysis of electronic money privacy policies, focusing on privacy laws in Canada and the European Union. It evaluates the privacy policies of PayPal, MasterCard, and Octopus Card against existing privacy regulations, highlighting the risks associated with personal information in e-money transactions.
4	The Limits of Money Laundering Laws and Risk Control Measures	Selinus Library	Ehi Eric Esoimeme – Selinus University, 2022	This dissertation provides a comparative analysis of approaches to implementing the Financial Action Task Force (FATF) recommendations. It focuses on Nigeria, the United States, and the United Kingdom, highlighting the need for legal reforms in Nigeria to strengthen AML/CFT measures, particularly with the use of AI for customer due diligence and account monitoring.
5	Central Bank Digital Currency (CBDC) as a Third Form of Money: Key Risks and Development Directions	DOI link	Anatoliy Guley, Alexey (Oleksii) Aleksandrov – Baltic Journal of Legal and Social Sciences, 2024	This paper explores the potential of CBDCs to transform the global economy by reducing costs and enhancing access to financial services. It emphasizes the need for proper regulation, cybersecurity measures, and a gradual transition to CBDCs to maintain macroeconomic stability while managing risks associated with private digital currencies and decentralized finance.
6	Central Bank Digital Currency (CBDC) as a Third Form of Money: Key Risks and Development Directions	DOI link	Anatoliy Guley, Alexey (Oleksii) Aleksandrov – Baltic Journal of Legal and Social Sciences, 2024	This paper explores the potential of CBDCs to transform the global economy by reducing costs and enhancing access to financial services. It emphasizes the need for proper regulation, cybersecurity measures, and a gradual transition to CBDCs to maintain macroeconomic stability while managing risks associated with private digital currencies and decentralized finance.
7	The Optimal Quantity of CBDC in a Bank-Based Economy	DOI link	Lorenzo Burlon, Carlos Montes-Galdón, Manuel A. Muñoz, Frank Smets – ECB Working Paper, 2022	This paper examines the trade-offs of issuing CBDCs in a bank-based economy. It explores the potential effects on bank intermediation, welfare gains, and the optimal CBDC quantity for stability. The study suggests an optimal range of 15% to 45% of quarterly GDP for CBDC circulation to mitigate the risk of bank disintermediation and promote economic stability.
8	Blockchain Application for Central Banks: A Systematic	DOI link	Natalia Dashkevich, Steve Counsell, Giuseppe Destefanis – IEEE Access, 2020	This paper presents a thematic review of blockchain use cases for central banks, focusing on areas such as Central Bank Digital Currencies (CBDCs), payment clearing and

Academic Journals				
SN	**Document**	**Link**	**Published**	**Key Insight**
	Mapping Study			settlement systems, regulatory compliance, and audit trails. The study identifies gaps and opportunities for further exploration in the adaptation of Distributed Ledger Technology (DLT) for central bank operations.
9	AML by Design: Designing a Central Bank Digital Currency to Stifle Money Laundering	DOI link	Robert Z. Mahari, Thomas Hardjono, Alex Pentland – MIT Science Policy Review, 2022	This article examines how central bank digital currencies (CBDCs) can be designed to be inherently resistant to money laundering and terrorist financing, leveraging strong digital identity and algorithmic transaction monitoring. It emphasizes the balance between anti-money laundering (AML) priorities, privacy, financial inclusion, and compliance costs.
10	A Study on the Influence Mechanism of CBDC on Monetary Policy: An Analysis Based on e-CNY	DOI link	Jiemeng Yang, Guangyou Zhou – PLOS ONE, 2022	This paper explores how China's e-CNY, the central bank digital currency, affects monetary policy by influencing money demand, money supply, and monetary policy transmission mechanisms. It highlights e-CNY's role in improving the velocity of money, controlling money supply, and enhancing monetary policy transmission.
11	CBDC: Banking and Anonymity	DOI link	Yuteng Cheng, Ryuichiro Izumi – Bank of Canada, 2024	This paper examines the optimal level of anonymity in CBDCs from a banking perspective. It shows that moderate anonymity in CBDCs can lead to inefficient outcomes in bank lending, suggesting that anonymity levels should either be very low to encourage transparency or very high to discourage bank lending.
12	The Urgency of Money Laundering Policy Reform for Digital Rupiah Implementation	DOI link	Sendy Pratama Firdaus – AML CFT Journal, 2023	This paper explores the challenges and opportunities for money laundering policy reform in light of the planned implementation of the Digital Rupiah in Indonesia. It emphasizes the need for stronger AML frameworks to address risks posed by digital currency's cross-border transaction capabilities.
13	The Positive Case for a CBDC	epe.lac-bac.gc.ca	Bank of Canada, 2021	This paper discusses the arguments for issuing a CBDC to enhance competition and foster innovation in digital payments. It highlights the role of a CBDC as a tool to address market failures, improve competition, and support the development of a vibrant digital economy through innovations such as smart contracts and programmable money.
14	CBDC: Context, Challenges, and Conditions for a Successful Adoption	ink.library.smu.edu.sg	Charlie Nhuc Hiang Lay – Singapore Management University, 2023	This dissertation examines the context and challenges of CBDC adoption, emphasizing the foundational elements needed for success. It highlights privacy, cybersecurity, and public acceptance as critical factors for CBDC implementation.
15	CBDC, Fintech and Cryptocurrency for Financial Inclusion and Financial Stability	papers.ssrn.com	Peterson K. Ozili – Digital Policy, Regulation, and Governance Journal, 2023	This paper discusses the combined role of CBDC, Fintech, and cryptocurrency in promoting financial inclusion and preserving financial stability. It highlights both the opportunities and risks these technologies pose to the financial system and emphasizes the need for effective regulation to mitigate financial stability risks.
16	Designing a Central	papers.ssrn.com	Jonas Gross,	This paper explores how zero-knowledge

Academic Journals				
SN	**Document**	**Link**	**Published**	**Key Insight**
	Bank Digital Currency with Support for Cash-like Privacy		Johannes Sedlmeir, Matthias Babel, Alexander Bechtel, Benjamin Schellinger – 2021	proofs (ZKPs) can be used to support fully private transactions in CBDCs while ensuring compliance with anti-money laundering (AML) and counter-terrorism financing (CFT) regulations. It proposes a two-tier CBDC system with privacy-focused and transparent accounts, allowing for different levels of transaction privacy.
17	Anti-Money Laundering and Counter-Terrorism Financing Disclosure by Money Exchange Providers in the GCC Countries	papers.ssrn.com/ sol3/papers.cfm? abstract_id= 3923718	MD Abubakar Siddique Abu Dhabi University Haitham Nobanee University of Oxford; Abu Dhabi University; University of Liverpool	The purpose of this paper is to measure anti-money laundering (AML) and counter-terrorism financing (CTF) disclosures by money exchanger providers in the Gulf Cooperation Council (GCC) countries. Design/methodology/approach: We conduct a content analysis on firms' websites to compare their AML/CTF disclosure against the recommendations of the Financial Action Task Force (FATF). We use a one-sample t-test to examine the degree of these disclosures. Findings: Overall, money exchange providers in GCC countries do not demonstrate a high degree of AML/CTF disclosure (20.27%). Country-wise disclosure levels are: Qatar 31%, UAE 19%, Kuwait 17.1%, Oman 26.27%, Bahrain 23.27% and KSA 6.1%. Originality: Our study is a novel attempt. No study has been undertaken before to investigate AML and CTF disclosure by money exchange providers either globally, regionally, or in any country.
18	Essays in Electronic Money and Banking	repositories.lib. utexas.edu/ items/ acdfd48e-6c5a- 439e-a9b1-6d2abaa3847e	Haibo Huang – The University of Texas at Austin Texas ScholarWorks - 2015	This dissertation explores the economic implications of private electronic money systems and evaluates the factors influencing consumer acceptance of electronic banking services. It provides a theoretical framework for understanding the role of e-money in modern banking systems.
19	Argument by False Analogy: The Mistaken Classification of Bitcoin as Token Money	SSRN link	Alistair Milne – SSRN, 2020	This paper argues that cryptocurrencies like Bitcoin are not token money but rather account-based systems. It challenges the common assumption that digital currencies are fundamentally new and highlights the need for regulation and policy to adapt to the technological nuances of cryptocurrencies.
20	Anti-money laundering and counter-terrorism financing disclosure by money exchange providers in the GCC countries	ssrn.com/ abstract=3923718	Haitham Nobanee, Osama F. Attayah, Mohammed Khereldin Bayzid – Abu Dhabi University	The paper highlights the poor AML and CTF disclosures by money exchange providers in GCC countries, identifying that Qatar has the highest disclosure (31%) while KSA has the lowest (6.1%). It calls for stricter regulations and better transparency practices to address money laundering risks.
21	Regulatory Guidelines on the eNaira	threshold-attorneys.com	Central Bank of Nigeria – October 25, 2021	These guidelines provide a framework for the implementation of the eNaira, including its issuance, management, and operational standards. It outlines the roles of stakeholders, security measures, and compliance requirements related to AML/CFT and KYC.
22	Instruction No. 008-	threshold-	BCEAO, 2015	This instruction outlines the conditions for

Academic Journals				
SN	**Document**	**Link**	**Published**	**Key Insight**
	05-2015 on Electronic Money Issuance in UEMOA	attorneys.com		electronic money issuance in the UEMOA region, focusing on the responsibilities of issuers, security requirements, compliance with AML/CFT regulations, and consumer protection measures.
23	Electronic Banking in Nigeria: Concept, Challenges and Prospects	ajol.info	Ikechukwu A. Acha – University of Uyo, 2008	This study explores the adoption of electronic banking in Nigeria, highlighting its potential benefits, such as increased transaction efficiency and reduced costs. It also examines the challenges, including infrastructure inadequacies, legal issues, and security concerns, emphasizing the need for steady power supply and robust security measures to foster growth.
24	La régulation du Bitcoin dans l'espace UEMOA	cres-sn.org	Mouhamoud Sangaré – 2020	This document provides a comprehensive analysis of the legal and regulatory challenges related to Bitcoin within the UEMOA region. It advocates for the creation of a legal framework and attractive tax policies to support the development of the cryptocurrency market in UEMOA while ensuring compliance with AML/CFT standards.
25	Central Bank Digital Currencies: Towards a Chinese Approach	diva-portal.org/ smash/get/ diva2:1433870/ FULLTEXT01.pdf	Ye Shi and Shucheng Zhou – Jönköping University, 2020	This thesis explores the design choices and mechanism of China's CBDC, Digital Currency Electronic Payment (DCEP). It focuses on how DCEP addresses both general public demands and central bank requirements, highlighting privacy, security, and the balance of control in the development of DCEP.
26	Innlegg: Kven kontrollerer bitcoin?	dn.no innlegg/ innlegg -kven-kontrollerer-bitcoiW2-1-107 4957	Dagens Næringsliv	Decentralization and dynamic distribution of power in Bitcoin is difficult to understand and achieve
27	Middelaldrande mann rasar mot bitcoin	dn.no/innlegg/ bitcoin/ kryptovaluta/ blokkjedeteknologi/m iddelaldrande- mann-rasar-mot-bitc oiW2-1-1376362	Dagens Næringsliv	Bitcoin's revolutionary aspect lies in the integration of money and technology in a decentralized system. rather than just the blockchain technology itself.
28	Central Bank Digital Currency: Central Banking for All?	elsevier.com/ locate/red	Jesús Fernández-Villaverde, Daniel Sanches, Linda Schilling, Harald Uhlig – 2020	This paper explores the implications of CBDCs on financial intermediation, highlighting competition between central and commercial banks and the risks of central banks monopolizing deposits. It also examines how CBDCs can affect financial stability, particularly during crises.
29	CBDC - Digital Currency of Central Banks: Advantages and Disadvantages	researchgate.net/	Malkhaz Chikobava – PhD in Economics	The article discusses the advantages and possible disadvantages of CBDC. This issue gained special relevance after the global financial crisis of 2008-2009.
30	CBDC, TRUST IN THE CENTRAL BANK AND THE PRIVACY PARADOX	researchgate.net/	Viktor Koziuk, Yurii Ivashuk, Yurii Hayda	Privacy/anonymity of digital transactions is an issue that may affect demand for CBDC. The study explores the privacy paradox through survey-based indexes of privacy preferences.
31	CBDC - Digital Currency of Central Banks: Advantages and Disadvantages	researchgate.net/	Malkhaz Chikobava– PhD in Economics	The article discusses the advantages and possible disadvantages of CBDC (Central Bank Digital Currencies). This issue gained special relevance after the global financial

Academic Journals				
SN	**Document**	**Link**	**Published**	**Key Insight**
				crisis of 2008-2009. It is no exaggeration to say that in recent years the entire world has been swept up in the fever of creating Central Bank Digital Currency (CBDC).
32	HybCBDC: A Design for Central Bank Digital Currency Systems Enabling Digital Cash	researchgate.net/ publication/ 3458451	Ricky Lamberty, Daniel Kirste, Niclas Kannengießer, Ali Sunyaev – German University of Digital Sciences and Karlsruhe Institute of Technology	HybCBDC presents a hybrid CBDC model that integrates both account-based and UTXO-based subsystems to support confidential payments with cash-like privacy while enforcing AML and CFT regulations.
33	Designing a Central Bank Digital Currency with Support for Cash-Like Privacy	researchgate.net/ publication/ 353444913	Jonas Gross, Johannes Sedlmeir, Matthias Babel, Alexander Bechtel – University of Bayreuth, University of Luxembourg, University of St.Gallen	The paper presents a CBDC design that uses zero-knowledge proofs (ZKPs) to provide cash-like privacy while complying with AML/CFT regulations.
34	Protecting the Financial System Regulation using the new technology of CBDCs	researchgate.net/ publication/ 357377447	Rosinara Ferreira – Post Graduate at Financial Investment & Banking, Pontifical Catholic University of Rio Grande do Sul	The paper discusses how CBDCs can enhance financial system regulation by integrating technological innovation with legal frameworks to mitigate risks like AML/CFT.
35	Central Bank Digital Currency: Critical Analysis of the Two-Tier Model	researchgate.net/ publication/ 363270488	Kombe Kaponda, Austin Mwange, Oswald Mungule – University of Zambia	The paper investigates the advantages of adopting a two-tier CBDC model for Zambia, emphasizing the importance of interoperability with existing payment systems and promoting financial inclusion while addressing AML/CFT challenges.
36	The Cost of Cash Processing as a Determinant of the Central Bank Digital Currency: A Critical Analysis of The Zambian Case	researchgate.net/ publication/ 363298737	Kombe Kaponda, Oswald K. Mungule, Austin Mwange – University of Zambia	This study evaluates the cost of processing cash in Zambia, concluding that while CBDCs could reduce currency processing costs, the hybrid two-tier model's reliance on fiat currency limits its ability to fully mitigate these expenses.
37	The Cost of Cash Processing as a Determinant of the Central Bank Digital Currency: A Critical Analysis of The Zambian Case	researchgate.net/ publication/ 363298737	Kombe Kaponda, Oswald K. Mungule, Austin Mwange – University of Zambia	This study highlights that while Central Bank Digital Currencies (CBDCs) can reduce the cost of cash processing, their efficiency is influenced by factors such as mobile penetration, internet access, and the existing monetary infrastructure.
38	Cryptocurrency and Central Bank Digital Currency: An Insight from the Regulatory Perspective	researchgate.net/ publication/ 373989863	Bhaskar Podder, Central Bank of Bangladesh & Shiv Nadar University	The paper compares cryptocurrencies and CBDCs, emphasizing the need for distinct regulatory approaches to address their differences. It highlights the benefits of CBDCs in achieving financial stability while underlining the risks of decentralized cryptocurrencies.
39	Assessment of Nigeria's Financial Services Sector Stability and Diversity	researchgate.net/ publication/ 381520768	Sunday Emeka Enebeli-Uzor, Zenith Bank Plc & Innocent Ifelunini, University of Nigeria	The study evaluates Nigeria's financial sector stability and diversity, highlighting that financial diversity positively influences stability. It calls for policies that integrate diversity to strengthen resilience and avert crises.

Academic Journals				
SN	**Document**	**Link**	**Published**	**Key Insight**
40	Central Bank Digital Currencies Adoption: Threat or Opportunity?	researchgate.net/ publication/ 382028671	Mounir Khatoui – PhD, University of Ghardaia	The article explores the dual nature of CBDCs, weighing their potential to enhance financial inclusion and payment systems against risks like financial instability and privacy concerns.
41	Research on The Implement of a New Monetary Form - Central Bank Digital Currency (CBDC): Cross-border payments, CBDC's adoption and its impact on the monetary system	researchgate.net/ publication/ 383025874	Vui Dieu Linh, Toyo University	This thesis explores how CBDC adoption can streamline cross-border payments, improve financial inclusion, and strengthen financial stability. It highlights interoperability challenges, regulatory concerns, and the evolving landscape of digital payments in the context of global economic trends.
42	Central Bank Digital Currency: An Opportunity for Financial Inclusion in Developing and Emerging Economies	researchgate.net/ publication/ 383054733 sciencedirect.com/	Special Report	This report explores how CBDCs can improve financial inclusion in developing and emerging economies, highlighting the importance of tailored CBDC designs to overcome unique challenges.
43	The Impact of CBDC on a Deposit-Dependent Banking System	researchgate.net/ publication/ 384025874 sciencedirect.com/	Journal of Financial Stability (2024)	This paper analyzes how the introduction of CBDCs could impact banks reliant on customer deposits, focusing on risks to liquidity, profitability, and stability.
44	Blockchain Application for Central Banks: A Systematic Mapping Study	Semantic scholar.org	Natalia Dashkevich, Steve Counsell, and Giuseppe Destefanis – 2020	This paper systematically maps the use cases of Distributed Ledger Technology (DLT) for central banks, identifying the most research-intensive areas: CBDCs, regulatory compliance, and payment clearing and settlement systems. It highlights both the opportunities and challenges of blockchain adaptation, including gaps in research between industry and academia.

Government and Regulatory Publications				
SN	**Document**	**Link**	**Published**	**Key Insight**
1	ORDONNANCE N°2024-011/PT-RM DU 30 AOUT 2024 PORTANT LUTTE CONTRE LE BLANCHIMENT DE CAPITAUX, LE FINANCEMENT DU TERRORISME ET DE LA PROLIFERATION DES ARMES DE DESTRUCTION MASSIVE	sgg-mali.ml JOURNAL OFFICIEL	August 30th 2024	The ordinance aims to combat money laundering, terrorism financing, and the proliferation of weapons of mass destruction. This is typically achieved by strengthening financial regulations and oversight. It likely establishes or updates the legal framework for reporting suspicious transactions, customer due diligence, and record-keeping requirements for financial institutions. The ordinance may define the roles of various institutions, such as financial intelligence units, regulatory bodies, and law enforcement

Government and Regulatory Publications				
SN	**Document**	**Link**	**Published**	**Key Insight**
				agencies, in enforcing anti-money laundering (AML) and combating the financing of terrorism (CFT) measures. Such ordinances often align with international standards set by bodies like the Financial Action Task Force (FATF) to ensure compliance with global AML/CFT regulations.
2	Central Bank Digital Currency Policy-Maker Toolkit	imf.org		As policy-makers navigate this process, they should consider how CBDC may introduce new capabilities that support regulatory goals while also introducing new risks or compliance vulnerabilities. CBDC could potentially be used as a tool to achieve policy objectives such as improved safety and resilience in payments systems; increased efficiency, access and competitiveness of payments systems; better data transmission and reporting to central banks; and financial inclusion. The achievement of these goals with CBDC must be evaluated in the full context of the associated trade-offs and risks that CBDC may entail.
3	CBN Press Release on Cryptocurrencies (February 2021)	sec.gov.ng	Central Bank of Nigeria – 2021	This press release provides justifications for the Central Bank of Nigeria's position on cryptocurrencies, citing concerns over their speculative nature, use in money laundering and terrorism financing, and the risks they pose to the financial system. The CBN reiterates its commitment to safeguarding the financial system and protecting citizens from fraudulent schemes associated with cryptocurrencies.
4	BCEAO - Instruction n°01/2006 relative à l'émission de monnaie électronique et aux établissements de monnaie électronique	bceao.int	BCEAO, 31 July 2006	This instruction outlines the regulatory framework for issuing electronic money in the WAEMU region, detailing the requirements for electronic money institutions, their operation, and compliance with monetary laws.
5	Instruction_no008_05_2015 sur EME	bceao.int/sites/default/files/2017-11/instruction_no008_05_2015_intranet.pdf	BCEAO	Instruction a pour objet de régir les conditions et modalités d'exercice des activités d'émission et de gestion de monnaie électronique dans les Etats membres de l'Union Monétaire Ouest Africaine;
6	E-Money and Monetary Policy Transmission	imf.org	IMF – 2024	This paper explores the impact of e-money on monetary policy transmission across 21 countries. It highlights that e-money strengthens financial intermediation, promotes financial inclusion, and enhances competition among banks, particularly in regions with limited financial inclusion. The study concludes that e-money development complements traditional banking and improves monetary policy efficiency.
7	A Guide to Central Bank Digital	imf.org/-/media/Files/Publications/	IMF	arge projects, whether digital or not, often follow a well-established sequence of research,

Government and Regulatory Publications				
SN	**Document**	**Link**	**Published**	**Key Insight**
	Currency Product Development 5P Methodology and Research and Development	FTN063/2023/English/FTNEA2023007.ashx		experimentation, development, testing, and operations phases. This linear approach works relatively well when the goals of the project are clear; proven technology is readily available; and a wide range of experience is offered by technology providers, consulting firms, and former clients.
8	central-bank-digital-currency/virtual-handbook	imf.org/en/Topics/fintech/central-bank-digital-currency/virtual-handbook	IMF	
9	UNDP & UNCDF Technical Paper 1.2: Digital Currencies and CBDC Impacts on Least Developed Countries (LDCs)	undp.org	Katherine Foster, Sofie Blakstad, Sangita Gazi and Martijn Bos – 2021	This paper outlines the macroeconomic implications and regulatory challenges of CBDCs in LDCs, discussing their impact on financial inclusion, monetary policy, and potential risks related to regulatory gaps.
10	CENTIF Mali (2022). Annual Report on AML/CFT Compliance. Bamako: CENTIF.			

Online Databases				
SN	**Document**	**Link**	**Published**	**Key Insight**
1	cbdctracker.org/	cbdctracker.org/	World CBDC Tracker	Current status of Central Bank Digital Currencies (CBDC) worldwide Description Cancelled Countries that cancelled or decommissioned a CBDC. Research Countries that have conducted first explanatory CBDC research. Proof of Concept Countries that are in an advanced research stage and have published a CBDC proof of concept. Pilot Countries that have developed a CBDC that is tested in a real environment either with a limited number of parties or on a wide scale. Launched Countries that officially fully launched a CBDC.
2	cbdctracker by atlanticcouncil.org	atlanticcouncil.org/cbdctracker/	Atlanticcouncil	Central Bank Digital Currency (CBDC) Tracker takes inside the rapid evolution of money all over the world. The interactive database now tracks over 130 CBDCs.