Securing Digital Identity Management in the Nigerian Banking Sector Using Blockchain Technology

Korede Israel Adeyanju [0009-0009-3860-3978]
Department of Computing, College of Business, Technology and Engineering, Sheffield Hallam University, United Kingdom
K.adeyanju@kia-techs.com

Abstract

This study explores how BCT ensures Digital Identity Management (DIM) in Nigerian banks. Due to rising identity theft, fraud, and cybercrime, secure and efficient identity management systems are needed. BCT, a decentralized, immutable, and secure data management solution, is needed because conventional methods have failed. The study uses mixed-methods to obtain quantitative and qualitative data. Online surveys targeted bank consumers and personnel to acquire quantitative data. In-depth interviews with bankers and IT specialists provided qualitative information. Nigerian banks face regulatory concerns, technological barriers, and BCT misunderstandings while implementing strong DIM practices, according to the report. Incorporating BCT into DIM operations could improve data security and privacy, reduce fraud, and boost operational efficiency in Nigerian banks. BCT adoption may improve DIM, according to study. Successful implementation requires strategic adoption, supportive legal frameworks, and improved awareness. This study analyzes the potential and challenges of using blockchain-based identity management solutions in the banking sector and makes practical recommendations for banks and policymakers to create a secure and trustworthy banking environment in Nigeria.

Keyword: Blockchain Technology, Data Integrity Management, Personally Identifiable Information, Nigeria Banking Sector, Financial Transaction Security

1. Introduction

Blockchain Technology (BCT) to secure Digital Identify Management (DIM) in Nigerian banks is an important area of research and resource investment to fully adopt the technology to combat cybercrime and insecurity. DIM adoption in Nigeria's banking sector is critical owing to rising fraud, cybercrime, and identity theft. Security breaches and inefficiencies have plagued the traditional bank client identification system. As technology advances, BCT's decentralized and irreversible qualities will solve these problems [1, 2, 3]. Decentralized BCT saves and verifies transactions utilizing a global network of computers. It is also a distributed, internet-accessible database or ledger, a decentralized record-keeping system or digital database [4, 5]. Decentralized and secure BCT enables for more transparent, reliable, and efficient transactions. BCT's decentralized design makes it reliable and secure. Encryption secures data privacy. By dispersing data replication to network nodes, blockchain is more reliable and less subject to disasters than centralized systems [6].

DIM describes digital data and activity management technologies. It involves generating, preserving, and using digital identities to secure resource access, data governance and privacy, and regulatory compliance. Identity can be viewed from many aspects and implemented in many industries, depending on the objective of digital identification. One of the most significant corporate technologies is blockchain. BCT can solve an economic system with many distrustful participants [7, 8]. DIM ecosystems need BCT to handle security and trust challenges. Blockchain's decentralized structure is highly secure. This framework boosts DIM system data confidentiality, integrity, and availability, following information security rules [9, 10, 11].

One of Africa's most prosperous banking sectors is found in Nigeria. However, Nigerian banks face significant challenges when it comes to managing digital identities. The ineffectiveness of standard identification verification methods, fraud, and theft are banking problems that put both customers and financial organizations at risk. Critical situations require robust, secure, and innovative solutions [12]. Due to its decentralized, irreversible, and transparent nature, BCT may solve these issues. Because BCT is transparent, decentralized, and irreversible, it could be able to address these issues. BCT reduces fraud, identity theft, and other online crimes by safeguarding digital identities [13]. Furthermore, smart contracts can boost client trust, streamline identity verification, and improve operational performance [2, 9, 14]

The complexity and slowness of the current identity management solutions regularly generate customer dissatisfaction. Nigerian banks make greater investments in traditional methods of customer service and security. Wait times are increased by manual verification, which is laborious and prone to errors even if the bank makes an effort to please its clients [15]. Although BCT can allay these worries, Nigerian banks are hesitant to use it. The distributed and indestructible security and efficiency of BCT are advantageous for DIM solutions. However, little research has been done on the benefits, drawbacks, and real-world applications of BCT in this context. Financial institutions are unable to use BCT to modernize their DIM system because of a lack of understanding [12]. Bitcoin and other cryptocurrencies are occasionally compared to BCT applications. Nigerians are wary about cryptocurrencies due to online fraud and application processes. Legislators, business leaders, and prospective blockchain users are therefore terrified of the technology [16].

Legislative and infrastructure barriers to the banking system's adoption of BCT in Nigeria. Financial institutions are cautious due to the ambiguity around digital identification and BCT legislation. How BCT might be successfully integrated into Nigerian banks' DIM processes is unknown. This study will provide helpful guidance and insights for improving consumer security by utilizing BCT to boost the efficacy of DIM. The study's objectives are as follows: Analyze the corpus of existing content in-depth and critically:

- To ascertain the challenges Nigerian banks face in order to make the most of DIM.
- To determine how DIM might be enhanced by BCT to offer effective security in Nigerian banks.
- To evaluate the benefits and drawbacks of using blockchain-based DIM in Nigeria's banking sector.
- To assess if adopting DIM on BCT would enhance financial transaction security and data privacy.

Paper organisation

The remaining part of this paper is organized as follows. Section 2 presents the literature review. Section 3 presents the methodology, research design, research techniques and procedures that describe the study. Section 4 results and discussion. Finally, Section 5 presents the conclusion and future works

2. Literature review

2.1 Digital Identity Management

A person's representation in the digital sphere is referred to as their "digital identity," which is made up of a unique identification associated with a number of characteristics. An identifier is a piece of data that is used to distinguish one person from another within a

system. The tax code is the unique identity for a digital ID. A person's given name, family name, date of birth, residential address, and physical characteristics are all considered aspects of their digital identity. Identity management techniques have been developed based on three main criteria: security, control, and portability. There are five main models of identity management: The Isolated Identification Model, Centralized Identity Model, Federated Identity Model are among the various identification models [17].

Gopal and Omeleze-Baror, [6] noted that in recent years, sharing sensitive information via digital media has grown in popularity. Customers typically decide not to consider the ramifications of sharing their information online, which has sparked worries about this trend. Rather, they simply click the "accept" button without carefully reading the digital channel's terms and conditions. The quick development of broadband technology provides consumers with a number of contemporary conveniences in their personal, professional, and educational lives. It makes it simple to access services and allows data and information to be transmitted across several application service providers using multiple digital identities. The digital identity verification and management system of application service providers exposes and stores users' digital identities and related behavioral data, even though they are benefiting from a variety of Internet services. Network security problems have resulted from this, such as identity theft, unauthorized use of identities, and the release of private data that might be used for extortion [18].

2.2 Blockchain Technology

The invention of the cryptocurrency Bitcoin served as the first introduction to the idea of blockchain [19]. BCT is a transparent, decentralized technology that makes it possible to record transactions between two parties in an effective and safe manner. It does not require centralized control and stores data in an unchangeable, chronological fashion [20]. The fervor for BCT has had a significant impact on the world economy. Blockchain is starting to have an impact even in low-resource countries, especially in the financial and associated sectors [16]. BCT is predicted to be the ground-breaking invention of the future that will transform corporate operations procedures as well as the banking and finance industries. The goal of BCT is to provide an open, decentralized ledger that is available to anyone. Its goal is to instill trust in an unprotected ecosystem without the involvement of a third party. The ledger contains the consensus-based state of the blockchain, which includes an exhaustive history of all past transactions that cannot be changed. Additionally, it can be used in combination with other technologies, such as identity management, digital signatures, and corporate regulations, to modify such technology to meet the challenges of the present [21]. Nikbakht, et al., [22] characterized BCT as a decentralized system that significantly lowers the danger of data loss, theft, or manipulation while guaranteeing a high degree of data integrity. Compared to a backup system that is restricted to a single location, the data is dispersed over numerous sites worldwide, providing increased security and redundancy in the event that the server that oversees the chain is destroyed. The blockchain provides increased transparency and responsiveness since every transaction is recorded in a distributed database dispersed over the whole network.

2.3 Types of Blockchain technology

Blockchains come in three main varieties: consortium, private, and public. Each kind has distinct qualities, and their responsibilities and configurations differ slightly.

2.3.1 Public Blockchain

Open or permissionless blockchains are other names for public blockchains. According to [22] Any member of the public can access a public blockchain network. One of the core features of the blockchain system, decentralization, is fully integrated into this BCT. Every user in the peer-to-peer network has an immutable copy of the ledger in this type of distributed ledger system. A decentralized and distributed system known as a public blockchain allows an arbitrary number of users to collaborate and exchange transaction data that occurs within the system. No specific regulating body exists. There is no restriction on who can exert authority or control, and anyone can participate in the activity without disclosing who they are. The underlying technology of Bitcoin, a well-known cryptocurrency that is currently in use worldwide, is a recent use of the public blockchain [23]. Because data is on a larger network node, public blockchain's decentralization and transparency can offer a platform for digital identity management where no entity will control user identities, thereby lowering the risk of identity theft and authorized access. The foundation of self-sovereign identification is the public blockchain, which gives users or individuals complete authority or control over their own personal data without the intervention of middlemen or third parties. This ensures privacy and data protection while allowing the user to choose which aspects of their identification they feel comfortable revealing with the service provider [24].

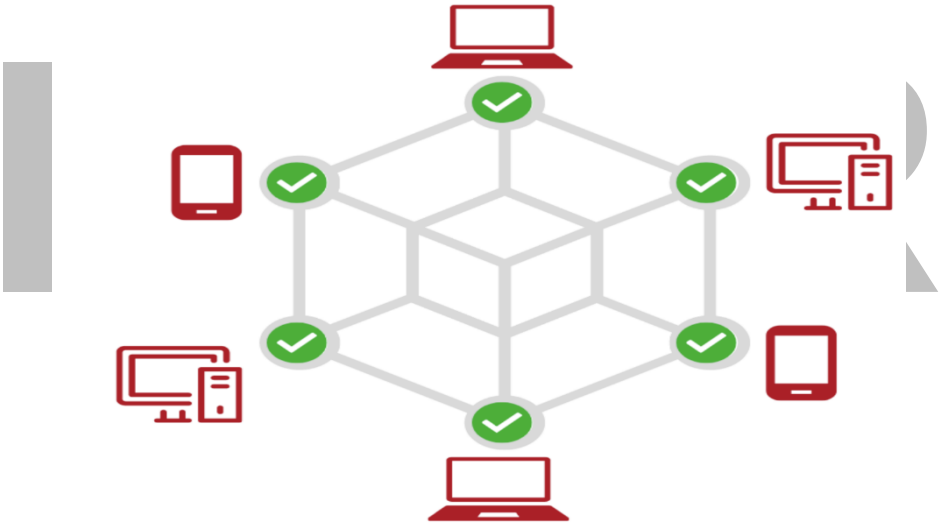

Figure 1: Public Blockchain [25]

The permissionless blockchain, also known as a public blockchain, is shown in the following diagram, which is designated as Figure 1. All devices can access this kind of blockchain, which enables everyone to view and validate transactions. It is a decentralized, self-governing digital public ledger that functions independently and autonomously.

2.3.2 Private Blockchain

Another name for a private blockchain is a permissioned blockchain. As its name suggests, a single private organization with total control and authority is the only entity overseeing the network. This blockchain cannot be read or written to by the general public, in contrast to permissionless blockchains. A private blockchain, in contrast to a public blockchain, is independently managed by a single party [23]. Therefore, each participant must have acquired the required authorizations in order to access transactions. Only legally obligated entities are permitted to create transactions on a private blockchain, and only authorized and verified entities are able to both authorize and confirm transaction histories and data [25]. Because only authorized nodes participate in private blockchains, the block production cycles, or verification time, are shortened. Because of this, clearance and verification from

unauthorized nodes are no longer required. However, compared to public blockchains, the dependability of private blockchains is limited because users of these blockchains are entirely dependent on the service provider. Strict controls on who can access or manage digital identities are in place on permissioned blockchains. For businesses like banks and other data-oriented organizations who need to protect sensitive data, this kind of BCT is a helpful solution.

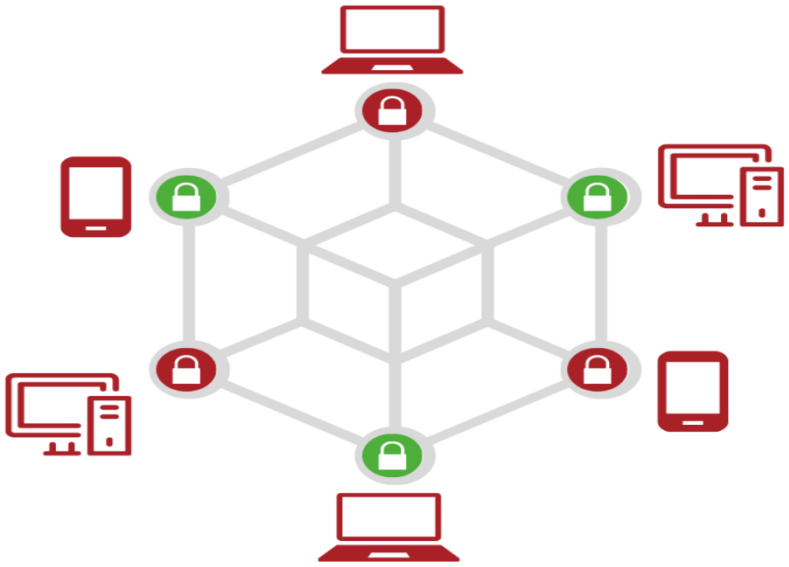

Figure 2: Private Blockchain [25]

The aforementioned diagram, designated Figure 2, depicts a permissioned blockchain under the supervision of a single private entity. They have total authority over the network and decide which users are allowed to sign up, access it, and validate transactions.

2.3.3 Consortium Blockchain

A consortium blockchain, or federated blockchain, is a type of blockchain technology maintained by numerous companies rather than a single entity, similar to private blockchains. Only authorized members of the organization can access the network since it is permissioned. However, because decision-making power is shared across several organizations, the network is only partially decentralized. This blockchain technology was put into place to help organizations work together. It makes it possible for entities to communicate data securely and easily, allowing them to work together to solve business problems [25]

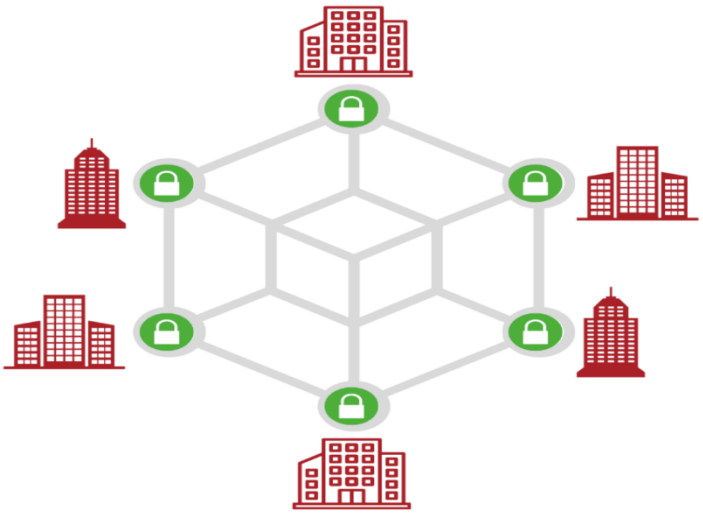

Figure 3: Consortium Blockchain [25]

The above diagram, known as Figure 3, shows how many organizations administer a consortium blockchain. Because the network is permissioned, only individuals with authorized access within the organization are permitted to use it. This method of overseeing blockchain transactions is commonly employed by banks and other entities within the financial services sector. Multiple banks can create a consortium blockchain, in which the participants have the power to choose which nodes are in charge of transaction validation [4].

2.4 Digital Identity Security and Data Privacy Using BCT

Concerns about user privacy in the existing identity management ecosystem are being heightened by increasing surveillance and security breaches. In order to provide user-centric services, organizations amass enormous amounts of sensitive data. Following collection, the information is used to forecast, profile, and promote economic growth. Users are frequently unaware of the data that is saved on them and how service providers use it. Users have little to no control over data sharing and privacy, and identities and personally identifiable information (PII) are centralized. Additionally, the collection of PII exposes service providers to attacks, resulting in security lapses and privacy violations [26]. Digital identity authentication confirms a person's real identity on internet networks. Establishing credibility in identity management requires confirming the legitimacy of individuals and protecting sensitive information. To gain services in exchange, users must provide organizations their personal information (such as credentials, PII, etc.). Service providers must utilize identity management and multi-factor authentication to avoid centralized theft, abuse, or modification of this data, which makes the systems more difficult [27].

Singh & Shiho, [28] The most reliable way for autonomous cars to exchange information is through blockchain describe how the BCT will be used to protect and preserve the privacy of Internet of Things (IoT) data. The study focuses on protecting personal information when using the Internet of Things and recommends using BCT to enable safe authorization, approvals, and transactions. Because BCT is distributed and eliminates middlemen, it can reduce data fraud brought on by the centralization of data in traditional [28, 29].

2.5 Role of BCT in Banking & Financial Sectors

In order to eliminate any chance of retroactive change or tampering, BCT was first implemented in 1991 as a means of timestamping digital documents. These blockchain networks use cryptographic methods to safely store documents with timestamps. The creation

of a decentralized digital currency called "bit gold" is thought to be a direct forerunner of the Bitcoin system [29]. Financial service companies, particularly banks, can now build their own application systems and organizational networks that link various internal departments and offices thanks to recent technological advancements [30]. A particularly promising and pervasive change in the world of technology is the use of BCT in the banking and financial sectors, as well as the discussion surrounding its application. By improving the lawful, transparent, safe, and effective nature of operations, blockchain has the ability to completely transform the sector [31] BCT incorporates cutting-edge technology such encryption techniques, consensus processes, distributed data storage, and node-to-node communication. Additionally, it has the potential to develop into a decentralized ledger that can independently monitor transactions involving several entities [32]

BCT enables the quick, economical, and tailored issuance of digital securities. The advent of digital financial instruments can broaden the market for investors, reduce costs for issuers, and alleviate counterparty risk by enabling customization to align with investor expectations. It employs standardized, protocol-driven, and collaborative techniques to furnish network users with a cohesive and authoritative information source. The advantages of employing BCT encompass optimizing business processes, reducing operational costs, and enhancing collaborative productivity. Implementing BCT can enhance procedures and operational frameworks, while concurrently establishing an intelligent, real-time, user-friendly, highly efficient, and securely encrypted blockchain e-commerce system. This technology enhances user experiences, guarantees the secure and reliable functioning of the network through processes that incentivize users, and provides personalized administration tools for consortium and private chains [34]

Kaushik et al. [29] suggested a distributed ledger is a collection of client-specific records that manage the bank record, provide as evidence of regulatory compliance, and identify organizations trying to create false histories. The transactions are encrypted and recorded in a networked database using Distributed Ledger Technology (DLT). However, BCT is revolutionizing the financial technology industry and bringing about a new era of industrial disruption and technical innovation.

2.6 Benefits of Using Blockchain for Identity Management

The ideas of identity and access are central to BCT. Every interaction with the blockchain is tracked and associated with a unique identity created using a pair of keys. This identity is then used to determine whether this address has the necessary permission to interact with the particular block of the blockchain that it is trying to access. Each action is carried out from a distinct point of view, and these actions may be visible to the general public or limited to particular people. By limiting access to only selected identities for specific off-chain data repositories, this capability can be used to directly regulate access to particular data categories. Additionally, it can be used to control who has access to actions carried out by smart contracts. This approach is incredibly flexible for precisely controlling data access. Real-world identities and established identity systems, such as Active Directory, can be linked to blockchain identities. This would facilitate seamless integration with existing identity management techniques [30, 11]. Adopting BCT into digital identity management has several noteworthy benefits.Strengthening User Consent and Data Control, Increasing Security and Privacy, Improving Interoperability and Simplifying Identity Verification, and Saving Money and Scaling.

2.7 Blockchain Technology in Nigeria

The Central Bank of Nigeria has been known to oppose the adoption of this technology in Nigeria, where BCT is commonly linked to cryptocurrencies. There is a significant tendency for BCT technology and bitcoin to be mistaken with one another. However, there is a different narrative being conveyed about cryptocurrencies in Nigeria, which affects how the people there view BCT. Victor, [31] demonstrates that, in terms of Bitcoin and cryptocurrency use per capita, Nigeria is the country with the highest ranking in the world. In 2020, almost one-third of Nigerians said they used or owned cryptocurrency. By 2023, 47% of Nigerian respondents reported owning or using digital currency, a further increase in this ratio[4].

The favorable climate for cryptocurrency adoption in Nigeria is influenced by a few factors. These factors include the population's relative youth, the existence of mobile device-based distributed ledger payment networks, and the official currency's volatility and unpredictability. People under the age of thirty make up more than half of Nigeria's population. Cryptocurrencies are frequently used for regular money transfers to friends and family as well as in-store payments. It turns out that BCT is used more often than one might think. Cryptocurrency is used in Nigeria not just as an investment tool but also as a useful way to carry out everyday transactions [13]. BCT is generally viewed as dualistic. Although millions of Nigerians embrace it, those in positions of authority in the country view the idea with suspicion and hesitancy. The implementation of the National Blockchain Policy in May 2023 will result in a substantial change. Given that individuals are already aware of the benefits BCT offers in their daily lives, the strategy's potential for growing its use may be easily embraced by the public. The circumstances are favorable for expanding the use of BCT across a wider range of applications, as evidenced by the broad public support and the government's adoption of BCT as policy [29]

3. Methodology

The strategies and techniques used to conduct research are known as the research approach. encompassing anything from broad conclusions to particular methods for collecting, evaluating, and interpreting data [32]. This research employs both qualitative and quantitative methodologies. The methodology employed for this study is depicted in Figure 4, the block diagram for a secured digital identity management in the Nigerian Banking Sector based on Blockchain Technology

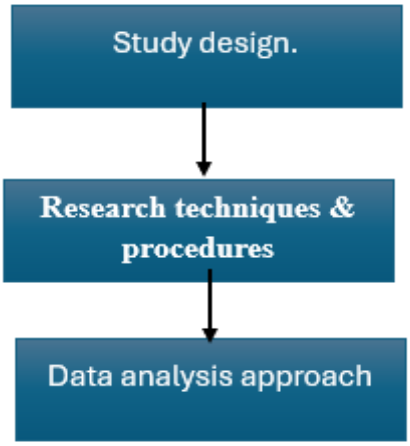

Figure 4: Block Diagram for a Secure Digital Identity Management in the Nigerian Banking Sector Using Blockchain Technology

3.1 Study Design

The systematic framework and approach used to collect and analyze data related to specific variables indicated in each research challenge is referred to as research design [28]. In order to thoroughly examine the importance of banks implementing BCT (BCT) to increase security, This study employs a mixed methods approach that integrates qualitative and quantitative research methodologies.

3.1.1 Qualitative Approach

This approach looks into and understands the importance that people or groups place on a topic. Formulating questions and procedures, gathering data—typically within the participant's context—analyzing the data by progressively shifting from specific details to more general patterns, and interpreting the data's applicability are all steps in the research process. This strategy would involve conducting in-depth interviews with important players in the Nigerian banking industry, such as bank staff members, general IT specialists, and IT security experts. Gaining understanding of the attitudes, experiences, and difficulties surrounding DIM and the possibilities of BCT is the goal of this strategy.

3.1.2 Quantitative Approach

This method is utilized to assess objective concepts through the analysis of variable correlations. These variables can be observed with instruments, yielding numerical data that can be analyzed by statistical methods. This strategy involves developing a structured questionnaire and disseminating it to the target population. The aim of employing this quantitative methodology is to gather empirical evidence concerning the current benefits and challenges associated with the implementation of DIM BCT in Nigeria.

3.2 Research Techniques and Procedures

3.2.1 Study Area and Population

All Nigerian banks, including commercial, microfinance, and other internet-related institutions, are the subject of this study. Customers and staff members of commercial and microfinance banks' IT and data protection departments make up the study's demographic.

3.2.2 Sampling Techniques

For the qualitative portion of the study, purposive sampling is used, with participants chosen expressly for their knowledge and familiarity with DIM and BCT. Stratified random sampling is used to address the quantitative component, ensuring that people from different groups of banking professionals and customers are included.

3.2.3 Sample Size

Ten (10) banking industry participants with roles in IT, cybercrime, security, and data protection officers make up the qualitative sample, while 150 survey respondents make up the quantitative sample for compliance.

3.2.4 Method of Data Collection

Data for this study was gathered through interviews, an online survey, and other pertinent materials. The chosen bank workers from the different IT, security, and compliance departments of the chosen banks (commercial and microfinance banks) participated in semi-

structured interviews. The interviews focused on comprehending DIM issues and the possible benefits that BCT could provide in resolving them, provided that BCT is fully utilized. One hundred fifty bank employees and clients were given the structured questionnaire. Two open-ended questions were included in the closed-ended question structure to allow the respondent to provide additional thoughts or suggestions that were not covered in the closed-ended questions. To supplement the study findings, pertinent materials on DIM and BCT, including industry regulation guidelines and literature, were studied.

3.3 Data Analysis Approach

The replies that were gathered from the interviewees were analyzed using thematic analysis techniques. Thematic analysis is used because it facilitates the identification of recurrent concepts or ideas that surface frequently throughout the interview. The Statistical Package for Social Science (SPSS) was used to analyze the online survey responses using frequency tables, descriptive statistics, and inferential statistics. While the correlation was employed under the inferential statistics to determine the correlation between BCT and DIM based on the developed research questions, the descriptive statistics provide an overview of the data obtained from the disseminated online questionnaire.

4. Result and Analysis

Demographic Profile of Respondents

A total of 158 individuals answered the online survey questionnaire, comprising customers, IT specialists, bank staff, and regulatory representatives. Two (2) of the 158 respondents who took part in the survey did not finish it and nine (9) of the respondents' responses were deemed invalid, for a total of 147 responding respondents. Table 1 displays the respondents' demographic characteristics (7).

Table1: Respondents Demographic Profile

Variable	Category	Frequency	Percentage
Age group	Under 25	6	4.1%
	25-34	55	37.4%
	35-44	67	45.6%
	45 – 54	16	10.9%
	55 and above	3	2.0%
Gender	Male	94	63.9%
	Female	53	36.1%
Educational level	Diploma/OND	2	1.4%
	Bachelor's degree/HND	80	54.4%
	Master's degree	63	42.9%
	PhD	2	1.4%
Occupation	Student	17	11.6%
	Employed	111	75.5%
	Self-employed	18	12.2%
	Unemployed	1	0.7%
Digital Identity Category	Users (Bank Customers)	116	63.4%
	Provider (Banks/FinTech)	35	19.1%
	Third party services providers	133	7.1%
	Regulatory and compliance entities	9	4.9%
	Prefer not to say	10	5.5%
Role in the Banking Sector	Customer	126	85.7%
	Banker	19	12.9%
	Compliance/Legal	2	1.4%

Source: Researcher's Online Survey, 2024

Age Group Analysis:

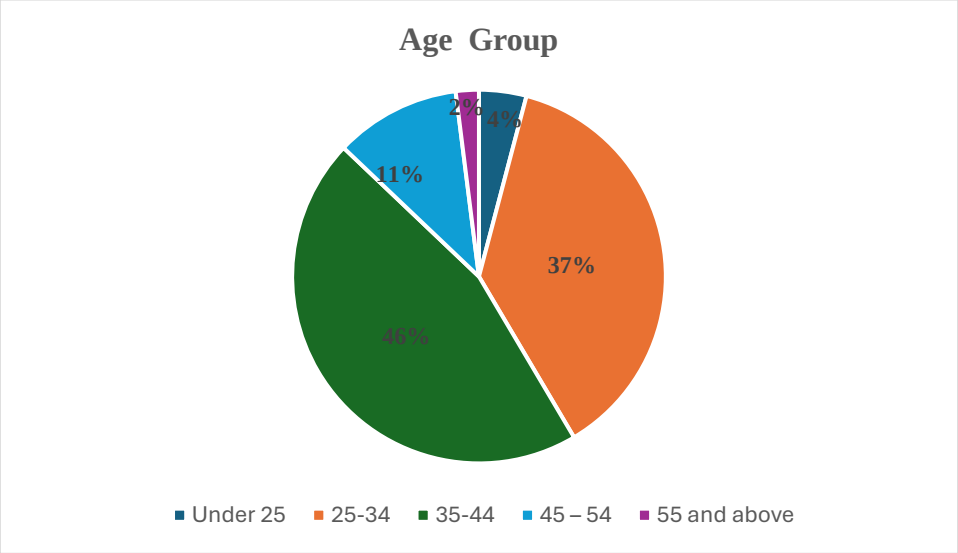

Figure 5: Age Distribution of Respondents

According to the statistics in Table 1 and Figure 5, the majority of respondents—45.6% of the sample as a whole—are between the ages of 35 and 44. The next largest age group is between the ages of 25 and 34, which makes up 37.4% of the participants. The percentage of respondents under 25 is 4.1%, while the percentage of respondents between the ages of 45 and 54 is 10.9%.

Just 2% of responders were 55 years of age or older. As a result, the age distribution of the respondents is within the range of ages at which people are most actively employed, indicating a high probability of active use of digital banking services and a high level of care for safeguarding one's online identity. The relatively low participation of people under 25 is depicted in Figure 5.

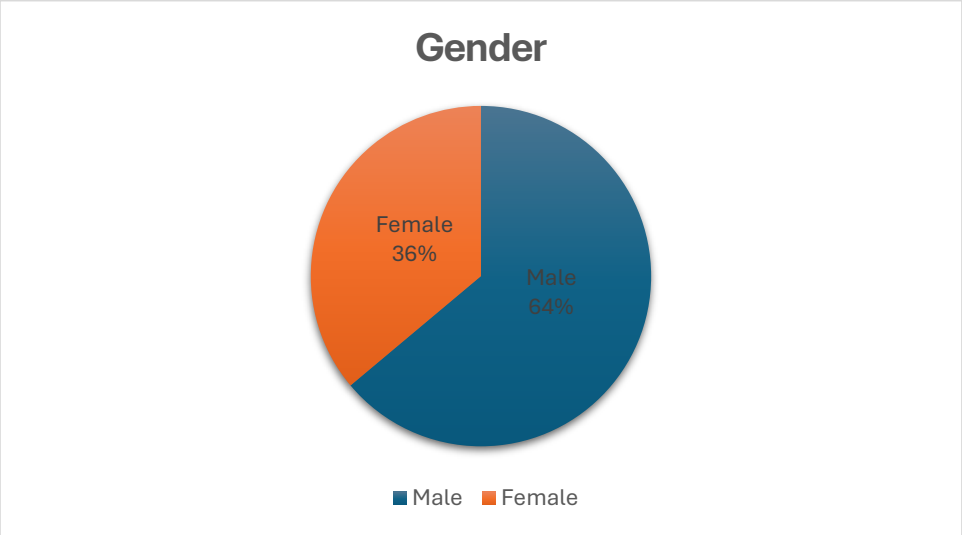

Figure 6: Gender Distribution

The gender distribution of respondents is displayed in Table 1 and Figure 6, showing that 36% of respondents are women and 64% of respondents are men. The gender gap implies that men use digital financial services more frequently and are more likely to engage in technology-related activities.

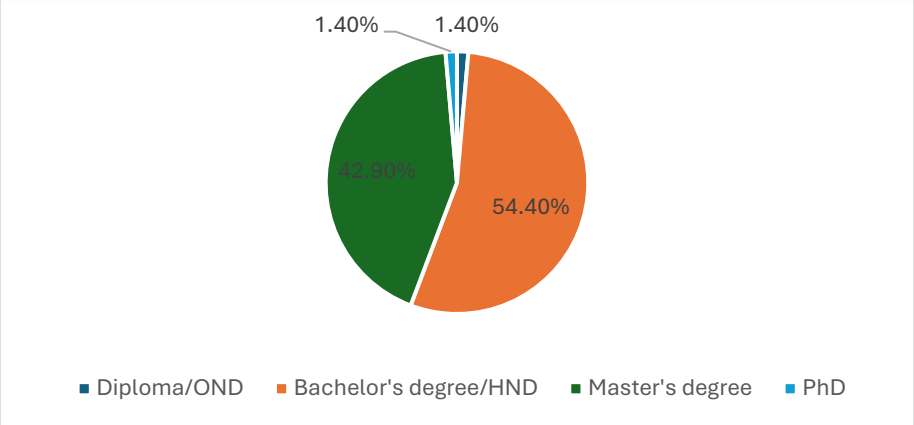

Figure 7: Respondents Educational Level

A significant amount of participants (54.4%) hold a bachelor's degree or HND, whereas a significantly lower percentage (42.9%) hold a master's degree, according to Table 1 and Figure 7. Only 1.4% of those surveyed have a PhD or a diploma/OND, respectively. The respondents have a relatively high degree of education, as seen by their high educational attainment. Higher educated people tend to be more informed and engaged in topics like digital identity security, so this is important for the study. Their responses to inquiries about the implementation of BCT in the Nigerian banking industry may be influenced by this awareness.

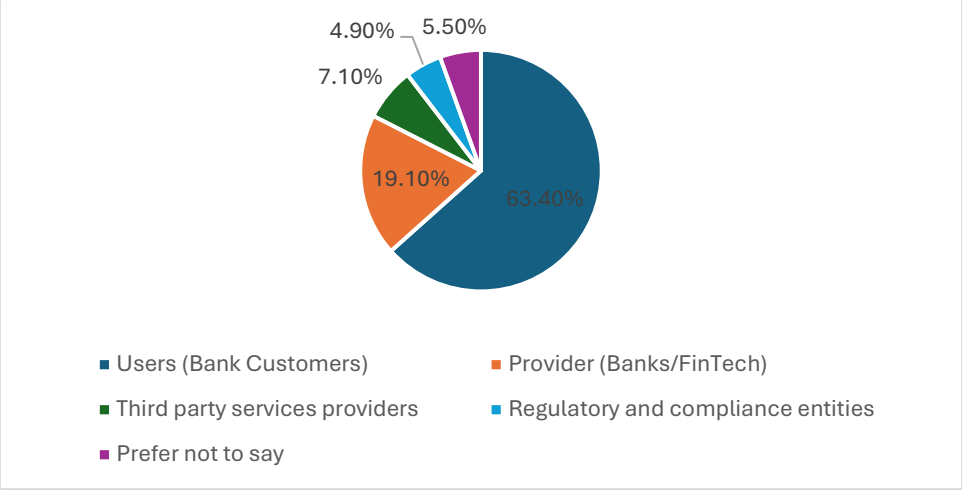

Figure 8: Digital Identity Management Categories

The question "which digital identity management categories do you belong to?" is depicted in Figure 8 above as "Digital Identity Category," and it asks respondents to choose the one that best fits their situation. According to the distribution, 63.4% of people are bank clients, 19.1% are digital identity suppliers (banks and FinTech companies), and third-party providers and regulatory bodies—albeit smaller—provide important context for understanding the operational and compliance issues that the banking industry faces.

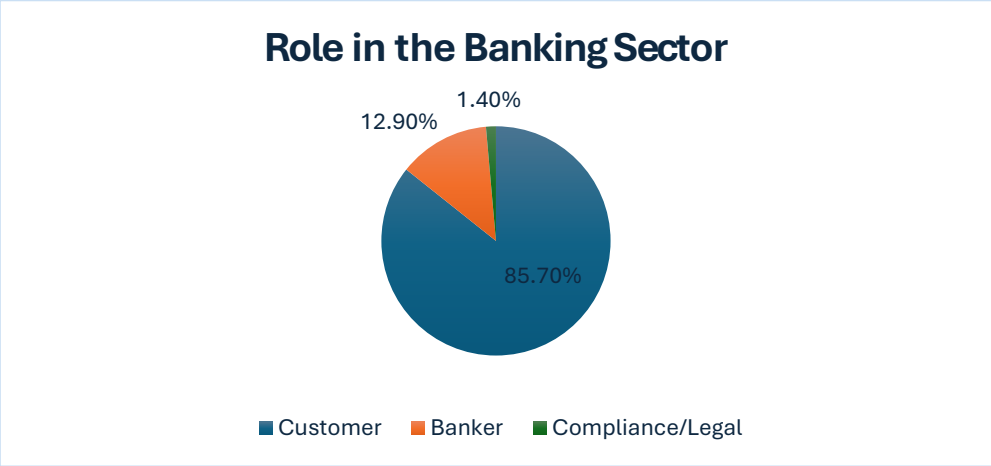

Figure 9: Distribution of Respondent Role in the Bank

According to Figure 9, 85.7% of respondents identify as consumers, 12.9% as bankers, and 1.4% as compliance/legal specialists. The significant proportion of respondents who were customers indicates that the data is substantially influenced by customer perspectives, which is crucial for evaluating the adoption and perceived security of digital identity management systems. Although their contributions are limited, bankers' and compliance experts' opinions are essential to understanding the operational and legal aspects of using BCT.

4.3 Data Analysis

A number of questions in the online poll are intended to gauge respondents' knowledge, perceptions, and possible obstacles regarding BCT in protecting digital identity management. The Statistical Package for Social Science (SPSS 28) program was used to code and analyze the data collected via the online questionnaire survey. This section (4.3.1, quantitative

analysis) would analyze the analysis's output, and appendix 4 contains the output result for reference. In-depth interviews with bankers and IT specialists provided the data for the qualitative analysis; the interview transcript is available for reference in appendix 5.

4.3.1 Quantitative Data Analysis (Questionnaire Responses Analysis)

What type of bank do you use?

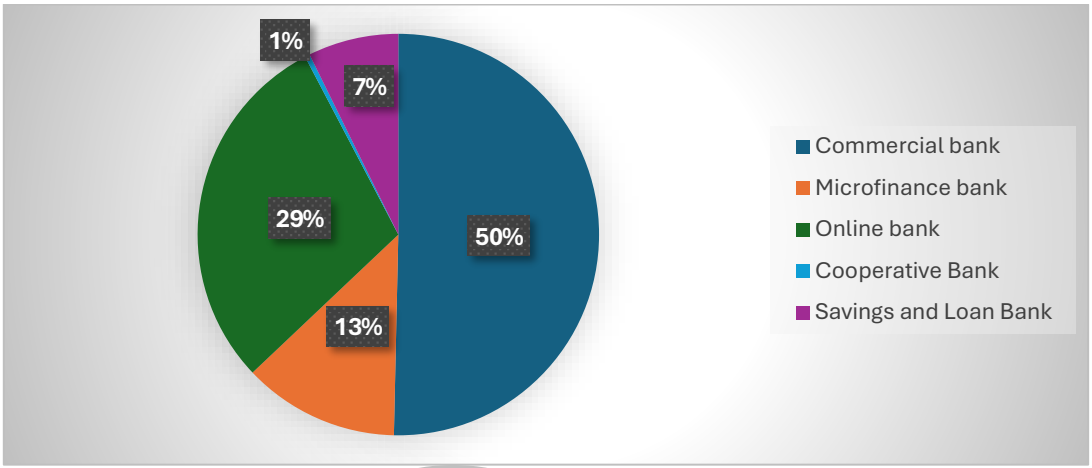

Figure 10: Types of Bank Usage

According to respondents' answers to the question, "What type of bank do you use?" 50.4% of respondents said they mostly use commercial banks for their banking needs. This research indicates that a sizable portion of the population is interested in the traditional banking industry; this may be due to the variety of services that banks offer as well as their longstanding reputation for reliability. However, a notable trend toward digital banking solutions is the use of online banks by 29.4% of the respondents. This inclination is likely driven by the convenience provided by online banks to their consumers, together with technical improvements. The standard deviation of 1.21286 is rather large, and the positive skewness of 0.970 suggests that the respondent can select from a variety of banks across all bank categories. The distribution of bank usage is in line with a slight preference for more established banks over more micromarket options, like savings and loan banks (7.3%) and cooperative banks (0.4%).

How would you rate your knowledge of digital identity management?

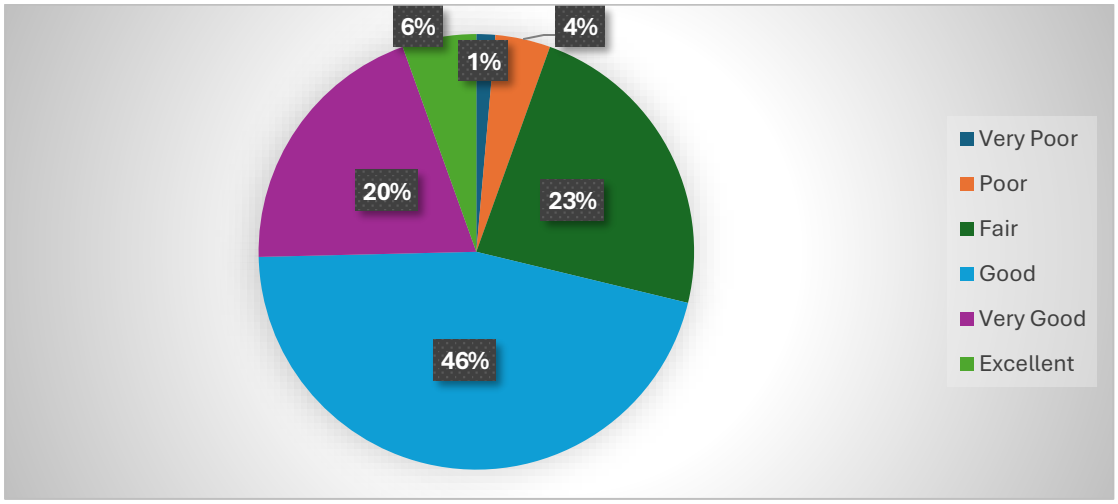

Figure 11: Knowledge of Digital Identity Management

Regarding the respondent's familiarity with DIM With a mean score of 3.9521, 45.9% of respondents said they knew "good" about DIM. The distribution of 19.9% who said they understood DIM "very well," 5.5% who said they understood it "excellently," 1.4%, 4.1%, and 23.3% who said they understood it "very poor, poor, and fair," respectively, supports the slightly negative skewness, or bias towards higher knowledge levels, indicated by the -0.178. The results indicate that a moderately knowledgeable group of respondents knew about DIM, which might be indicative of a larger industry trend emphasizing the significance of comprehending DIM in light of privacy issues and cybercrime.

How does your bank currently manage digital identities

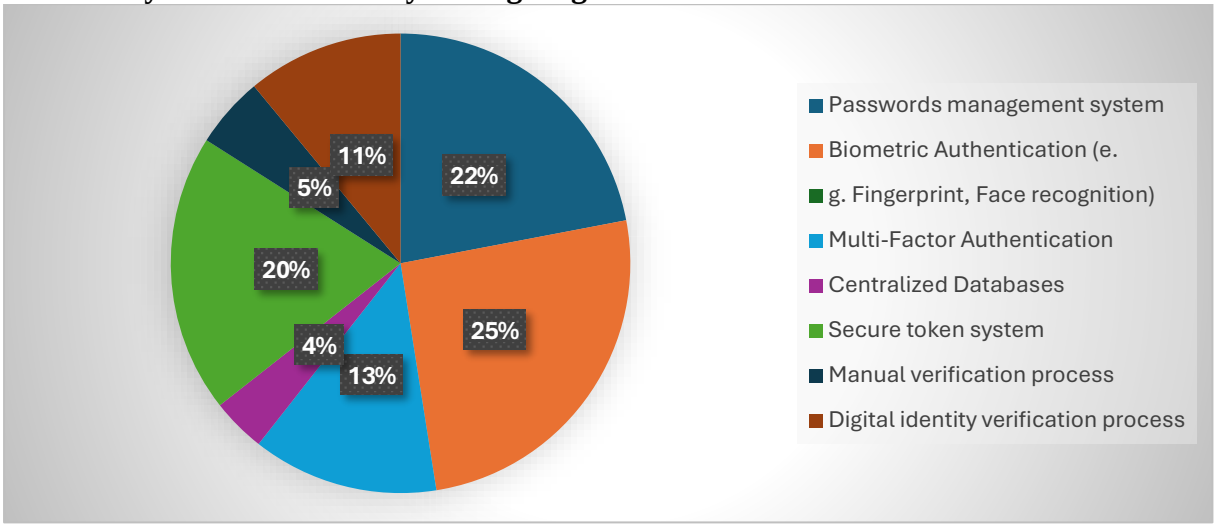

Figure 12: Method of managing DIM in Banks

According to the respondents, among the current methods used by banks for digital identity management, password management systems (22.0%) and biometric authentication (25.5%) are clearly preferred. These results provide a dual strategy for safeguarding digital identities, heavily relying on both contemporary (biometrics) and conventional (passwords) security methods. The range of methods is remarkable, with a mean of 3.3246 and a standard deviation of 2.01659 as follows: simple manual verification processes (5.0%), sophisticated digital identity verification (11.0%), multifactor authentication (13.1%), centralized database (3.8%), and secure token system (19.6%). The skewness, which is slightly positive at 0.490, shows that more often used procedures are being chosen.

What are the main challenges faced by your bank in maximizing the use of digital identity management?

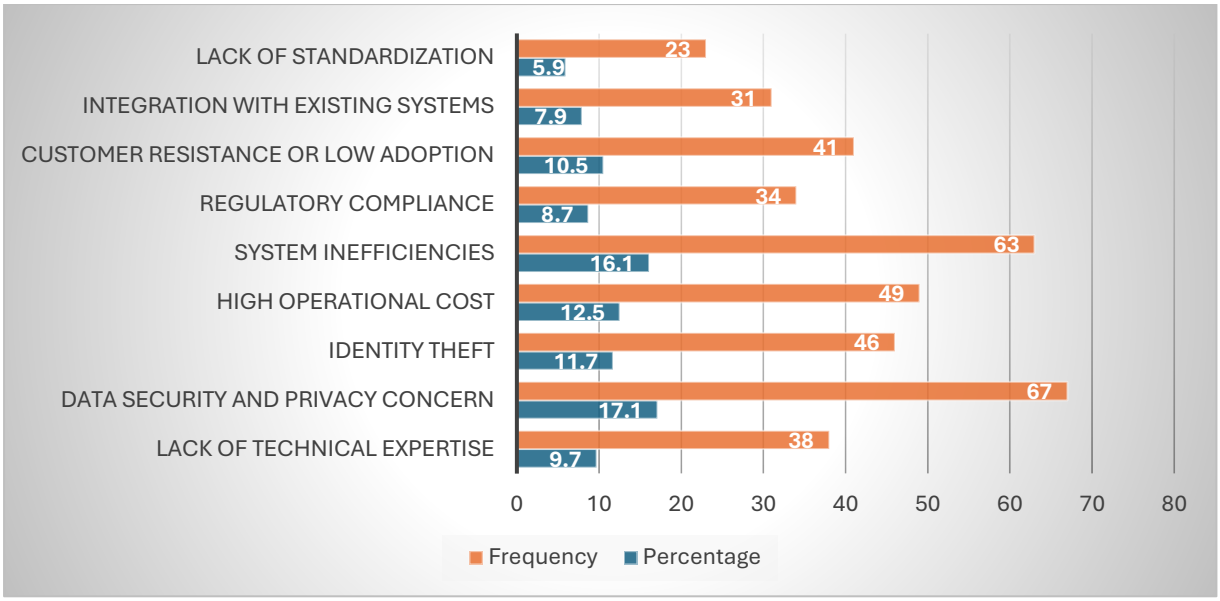

Figure 13: Challenges faced by Bank using DIM

According to the survey, "data security and privacy concerns" (17.1%) and "system inefficiencies" (16.1%) are the two biggest challenges facing DIM. Even though the operational and technological challenges are well-known, it seems that the emphasis is still on protecting sensitive data. Other difficulties include a lack of standardization (5.9%), integration into the current system (7.9%), customer resistance (10.5%), high operational costs (12.5%), identity theft (11.7%), and a lack of technical expertise (9.7%). The relatively low skewness (0.251) and negative kurtosis (-1.012) indicate a remarkably uniform distribution of worry across the several problems addressed, indicating that no issue dominates the landscape. The combined focus on security and system performance highlights the importance of these factors in effectively deploying digital identity management techniques.

Do you believe BCT can enhance the security of digital identity management?

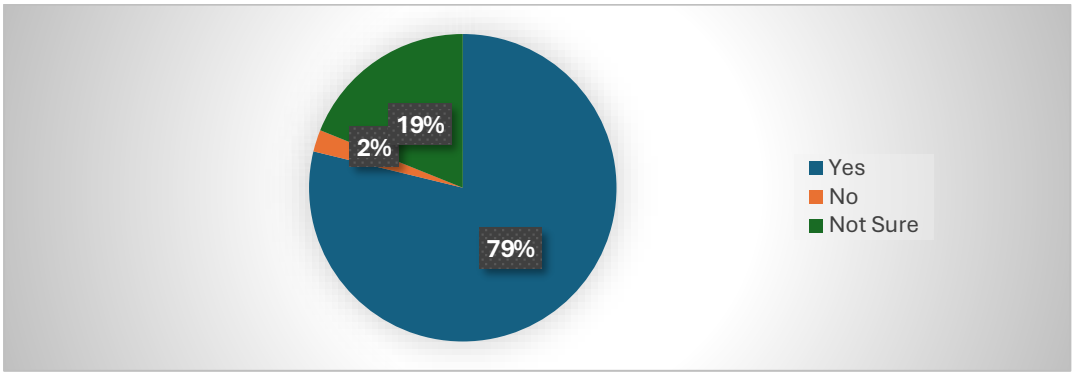

Figure 14: BCT Enhanced Security of DIM

Figure 14 shows 79% of respondents think BCT can increase DIM system security, while 19% aren't sure. Only 2.3% of respondents said "No" in response to skepticism or hesitation. There is strong support for the security benefits of blockchain, as seen by the average score of 1.4015 and the highly positive skewness of 1.511. The generally favorable opinion shows

growing confidence in blockchain's potential to provide robust and unchangeable security solutions.

What issues or drawbacks do you associate with blockchain-based digital identity management?

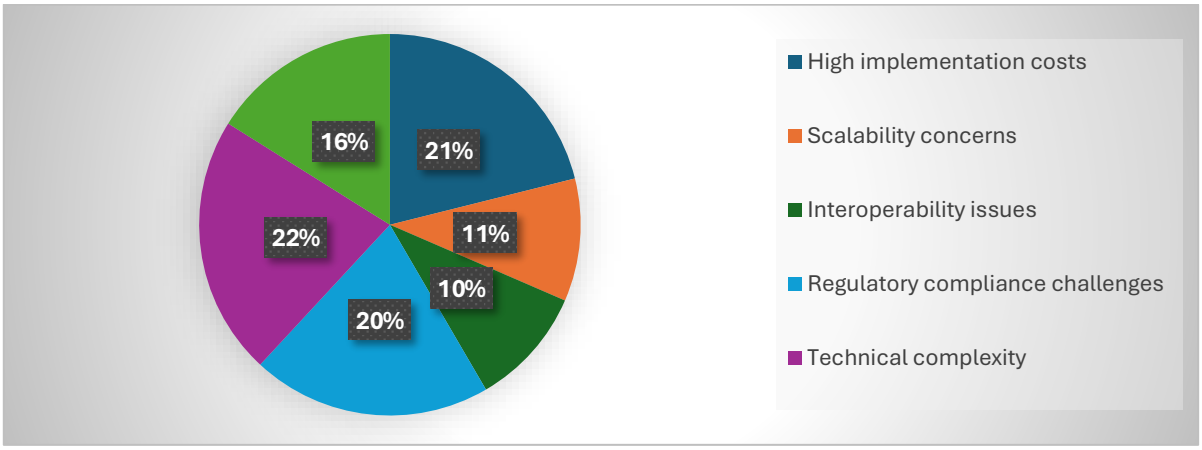

Figure 15: Associated Issues with Blockchain-based DIM

"Technical complexity" (22.0%), "high implementation costs" (21%), "scalability concern" (11%), "interoperability issues" (10%), "regulatory compliance challenges" (20%), and "potential for BCT misuse" (16%) are the primary concerns that respondents voiced about blockchain-based DIM. These issues draw attention to the challenges associated with utilizing cutting-edge technology, where having the required resources and expertise can be a major barrier. The existence of kurtosis (-1.305) and negative skewness (-0.237) suggests that there are a number of important barriers to blockchain adoption for DIM. These obstacles are not specific to any one problem, indicating a comprehensive awareness of the complexity of the difficulties at hand.

What technological barriers exist in adopting blockchain for digital identity management?

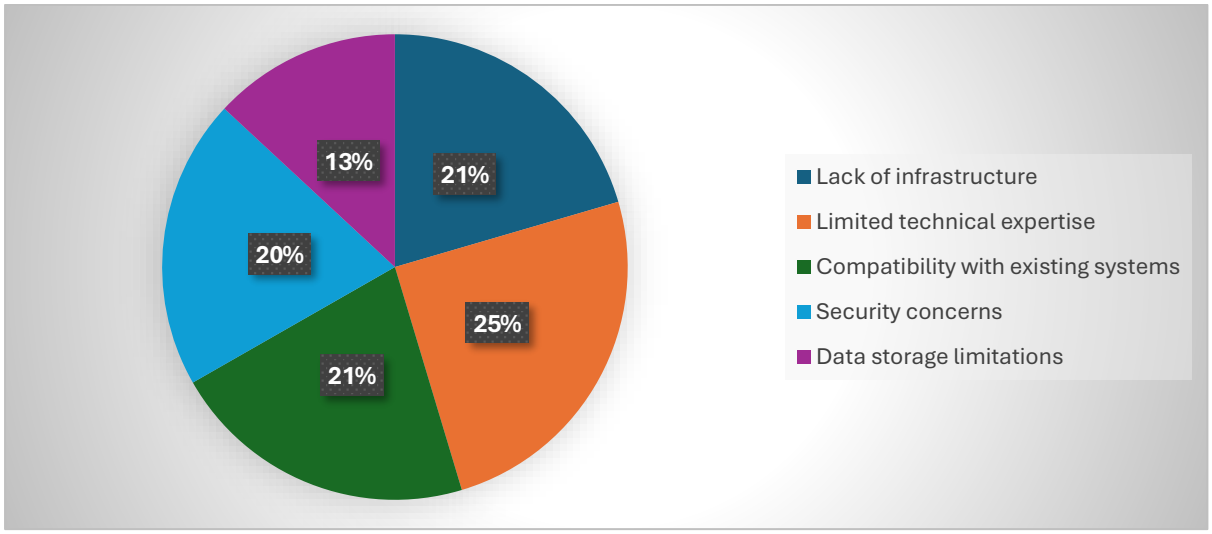

Figure 16: Existed Technological Barriers for DIM

The use of blockchain for DIM in Nigerian banks is hampered by a number of technological issues, as shown in Figure 16. The most frequently cited obstacles include a lack of technical

competence in BCT (25%), problems with existing systems (21%), which could result in significant costs if integration has to occur, and a lack of infrastructure (20%). Additional noteworthy obstacles are data storage limitations, which made up 13% of replies to the barriers affecting adoption, and security concerns, which accounted for 20% of responses. With an average response of 2.80, the respondents appear to have a reasonable grasp of these technological challenges. There is a considerable degree of variation in the responses, as indicated by the 1.33 standard deviation. There is broad agreement regarding the existence of these hurdles, as seen by the replies' slight positive skewness of 0.172, which leans slightly towards the lower end of the spectrum. The distribution of responses is flatter than the normal distribution, as indicated by the negative kurtosis score of -1.139, suggesting a wide variety of opinions on the severity of these technological barriers.

Do you believe that the adoption of digital identity management with BCT can enhance data privacy?

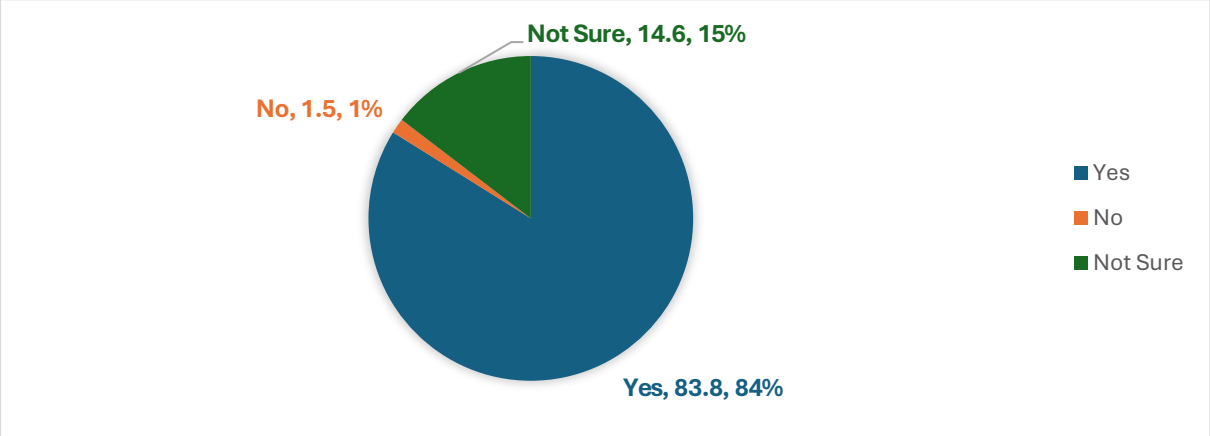

Figure 17: Can Adoption of BCT Enhanced Data Privacy

According to the diagram in Figure 17 above, a significant majority of respondents (84%) think that data privacy can be enhanced by including BCT into DIM. This suggests a very positive view of blockchain's possibilities in this field. 15% of respondents were unsure, while a small percentage (1%) disagreed. An predisposition towards agreement is indicated by the average response of 1.31, which is closer to the "Yes" response. A considerable degree of variability in the responses is indicated by the standard deviation of 0.71. Furthermore, a clustering of replies towards the "Yes" choice is revealed by the positive skewness of 1.941, suggesting a tendency to believe in increased data privacy. The distribution is more peaked than a normal distribution, as indicated by the positive kurtosis value of 1.854. This indicates that the majority of respondents firmly believe that blockchain technology can improve data privacy.

What strategies should bank, and policymakers implement to encourage the adoption of digital identity management using BCT?

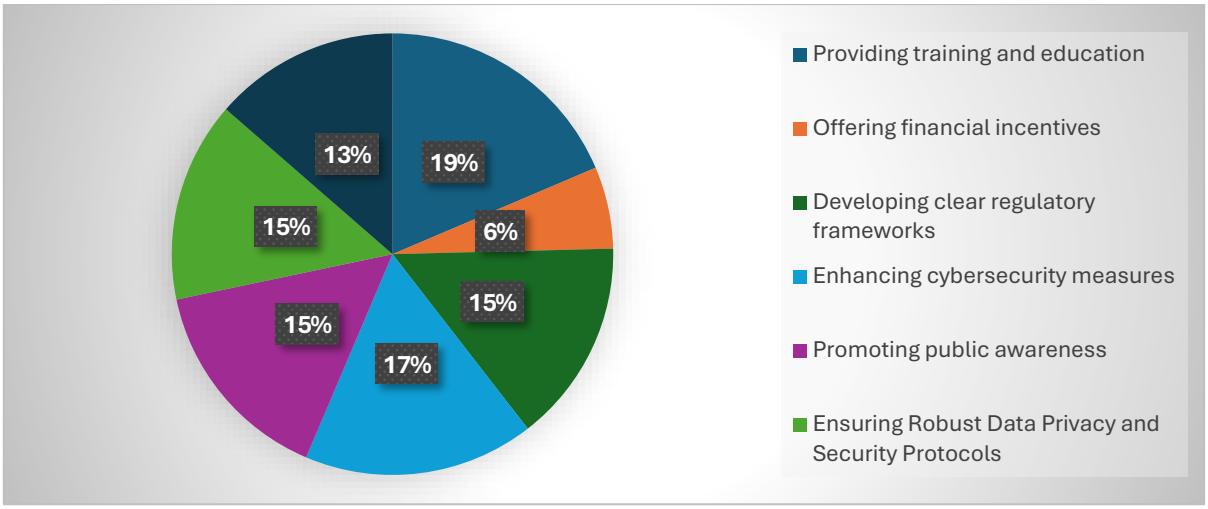

Figure18: Strategic Adoption for Banks and Policymakers

Figure 30 shows key measures for encouraging blockchain-based DIM adoption. The most popular method is "Providing training and education" (19%), emphasizing stakeholder education. "Enhancing cybersecurity measures" (17%) and "Promoting public awareness" (15%) emphasize security and public comprehension. A supportive environment requires clear regulatory frameworks (15%) and effective data privacy and security protocols (15%). Practical implementation requires streamlining the integration process with current systems, which accounts for 13% of the effort. The average response of 4.03 suggests unanimity, but the standard deviation of 2.01 suggests substantial disagreement. The replies are balanced, with a slight preference for more thorough strategies.

5. Conclusion

The research summary included the results from prior sections and shed light on BCT's involvement in DIM security in Nigerian banks. The study examined how BCT affects Nigerian bank DIM security and effectiveness. BCT, which is decentralized, irreversible, and secure, was anticipated to combat identity theft, fraud, and cybercrime. The mixed-methods study included quantitative and qualitative methods. Online surveys were sent to bank customers and employees to acquire quantitative data. However, in-depth interviews with bankers and IT specialists yielded qualitative data. Section 4 investigated survey respondents' demographics and gave a complete analysis of the findings in relation to the research themes.

The following are the key findings in this research work:

- DIM implementation in Nigerian banks faces challenges because to limitations of traditional, centralized identity management systems. Inefficiencies result from security breaches and cyberattacks on these systems.
- BCT can improve DIM with its safe, transparent, and decentralized features. This might reduce fraud and identity theft risks and boost efficiency. Implementation issues hinder BCT use in Nigerian banks due to regulatory ambiguity, infrastructural constraints, digital literacy issues, and misconceptions that equate blockchain just with cryptocurrency.
- The study found legislative and technological barriers to DIM adoption using BCT. These constraints include data protection, legal frameworks, and banking sector technical readiness.

Future Work

The outcomes of this study demonstrate the potential of BCT and offer useful insights into its role in increasing DIM in Nigerian banks; nonetheless, numerous areas necessitate more research:

- Future research should examine how regulatory norms affect blockchain-based DIM systems in banking. This will help explain how regulatory changes affect technological adoption. Blockchain-based DIM systems should be studied in conjunction with AI, IoT, and conventional systems. This would create more resilient, flexible, and future-oriented DIM systems that can better handle a networked and technology-driven global world.

Conflicts of Interest

The authors declare that they have no conflicts of interest concerning the publication of this paper.

Data Availability Statement

Data will be available on request

Author Contributions: Conceptualization, methodology writing—original draft, and data curation, project administration, methodology and validation, data curation and resources, software, visualization, editing and review.

Funding Statement

The author receives no fund for the project

References

[1] H. Florez, M. Sánchez and J. Villalobos, "iArchiMate: A Tool for Managing Imperfection in Enterprise Models," in *2014 IEEE 18th International Enterprise Distributed Object Computing Conference Workshops and Demonstrations*, Ulm, Germany, 2014 .

[2] S. A. Ajagbe, H. Florez and J. B. Awotunde, "AESRSA: A New Cryptography Key for Electronic Health Record Security," in *Applied Informatics ICAI 2022. Communications in Computer and Information Science*, 2022.

[3] E. Mentasti, "Digital Identity in Italy: challenges and opportunities for the adoption in banking, insurance and utility sectors.," MSc Thesis at Politec nico di milano, 2020.

[4] A. Hayes, “Blockchain facts: What Is It, How It Works, and How It Can Bee Used,” 2024. [Online]. Available: Investopedia: https://www.investopedia.com/terms/b/blockchain.asp.

[5] G. A. Taiwo, T. O. Akinwole and O. B. Ogundepo, “Statistical Analysis of Stakeholders Perception on Adoption of AI/ML in Sustainable Agricultural Practices in Rural Development,” in *Proceedings of Ninth International Congress on Information and Communication Technology. ICICT 2024 2024. Lecture Notes in Networks and Systems*, 2024.

[6] J. Gopal and S. Omeleze-Baror, “Using Blockchain to Secure Digital Identity and Privacy Across Digital Sectors,” in *International Conference on Cyber Warfare and Security*, 2024.

[7] C. C. Nwabuike, V. A. Onodugo, A. Arachie and U. C. Nkwunonwo, “Blockchain technology for cyber security: performance implications on emerging markets multinational corporations, overview of Nigerian internationalized banks.,” *International journal of scientific & technology research,* vol. 9, no. 8, 2020.

[8] G. A. Taiwo, A. Alameer and T. Mansouri, “Review of farmer-centered AI systems technologies in livestock operations,” *Cabireviews.2024.0038, CABI Reviews,* 2024.

[9] J. Benedit, “An Appraisal of Database Security in a Business Organization (Case Study: Fintrak Software Company Limited),,” University of East London, United kingdom, 2023.

[10] N. Ghadge, “Analyzing the Role of Blockchain in Identity and Access Management Systems,” *International Journal of Science and Research Archive,* vol. 12, no. 1, pp. 2249-2256, 2024.

[11] G. A. Taiwo, M. Saraee and J. Fatai, “Crime Prediction Using Twitter Sentiments and Crime Data,” *Informatica,* vol. 48, no. 6, p. 35–42, 2024.

[12] C. Mulligan, J. Z. Scott, S. Warren and J. P. Rangaswami, “Blockchain beyond the hype: A practical framework for business leaders,” in *white paper of the World Economic Forum*, 2018.

[13] N. Kshetri, “Blockchain's roles in strengthening cybersecurity and protecting privacy,” *Telecommunications policy,* vol. 41, no. 10, pp. 1027-1038, 2017.

[14] S. A. Ajagbe, J. B. Awotunde and H. Florez, “Intrusion Detection: A Comparison Study of Machine Learning Models Using Unbalanced Dataset,” *SN Computer Science ,* vol. 5, p. 1028, 2024.

[15] W. Serrano, “The blockchain random neural network for cybersecure IoT and 5G infrastructure in smart cities,” *Journal of Network and Computer Applications,* vol. 175, p. 102909, 2021.

[16] F. O. Jimoh, U. G. Abdullahi and I. A. Ibrahim, “An overview of blockchain technology adoption,” *Journal of Computer Science,* vol. 7, no. 2, pp. 26-36, 2019.

[17] R. Soltani, U. Nguyen and A. An, “A Survey of Self-Sovereign Identity Ecosystem,” *Security and Communication Networks,* vol. 2021, no. 1, p. 8873429, 2021.

[18] Z. Song, G. Wang, Y. Yu and T. Chen, “Digital Identity Verification and Management System of Blockchain-Based Verifiable Certificate with the Privacy Protection of Identity and Behavior. 2022(1), 6800938,” *Security and Communication Networks,* vol. 2022, 2022.

[19] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system,” *Decentralized business review,* p. 21260, 2008.

[20] M. Iansiti and K. R. Lakhani, “The truth about blockchain,” *Harvard business review,* vol. 95, no. 1 , pp. 118-127, 2017.

[21] M. Osmani, R. El-Haddadeh, N. Hindi, M. Janssen and V. Weerakkody, “Blockchain for next generation services in banking and finance: cost, benefit, risk and opportunity analysis,” *Journal of Enterprise Information Management,* vol. 34, no. 3, pp. 884-899, 2020.

[22] E. Nikbakht, M. Shahrokhi and A. Corriette, “Blockchain & distributed financial data,” *Managerial Finance,* vol. 46, no. 6, pp. 749-760, 2020.

[23] J. W. Kim, “Blockchain technology and its applications: Case studies,” *Journal of System and Management Sciences,* vol. 10, no. 1, pp. 83-93, 2020.

[24] Z. Zheng, S. Xie, H. N. Dai, X. Chen and H. Wang, “Blockchain challenges and opportunities: A survey,” *International Journal of Web and Grid Services,* vol. 14, no. 4, pp. 352-375, 2018.

[25] P. Lin, “What is private blockchain? everything you need to know,” 2023. [Online]. Available: https://blog.cfte.education/what-is-private-blockchain/.

[26] K. Gilani, E. Bertin, J. Hatin and N. Crespi, “A survey on blockchain-based identity management and decentralized privacy for personal data,” in *2020 2nd*

Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS), 2020.

[27] S. Nagaraju and L. Parthiban, "SecAuthn: provably secure multi-factor authentication for the cloud computing systems," *Indian Journal of Science and Technology,* vol. 9, no. 9, pp. 1-18, 2016.

[28] M. Singh and K. Shiho, "Blockchain based intelligent vehicle data sharing framework," *arXiv preprint arXiv: 1708.09721,* 2017.

[29] S. A. Ajagbe, P. Mudali and M. O. Adigun, "Internet of Things with Deep Learning Techniques for Pandemic Detection: A Comprehensive Review of Current Trends and Open Issues," *Electronics,* vol. 13, p. 2630, 2024.

[30] P. Kaushik, N. Kukrety and N. Saxena, "Blockchain Technology in Indian Banking Sector: A Systematic Review Envisaging Application in the Banking Sector," *Empirical Economics Letters,* pp. 1-18, 2023.

[31] Z. Saidat, M. Silva, D. Al-Daboubi, A. A. AL-Naimi and R. Aldomy, "How Can Blockchain Revolutionize the Jordanian Banking Sector?," *Journal of Southwest Jiaotong University,* vol. 57, no. 3, pp. 23-34, 2022.

[32] J. Laura, "The blockchain technology and its applications in the financial sector," Aalto University, Bachelor Thesis., 2017.

[33] T. Shah and S. Jani, "Applications of blockchain technology in banking & finance," in *Parul CUniversity, Vadodara*, India., 2018.

[34] X. Zhu and D. Wang, "Research on blockchain application for E-commerce, finance and energy," *IOP Conference Series: Earth and Environmental Science,* vol. 252, no. 4, p. 042126, 2019.

[35] N. Gbadge, "Use of Blockchain Technology to Strengthen Identity and Access Management (IAM)," *International Journal of Information Technology (IJIT),* vol. 2, no. 2, pp. 1-17, 2024.

[36] O. Victor, "Nigeria is the leading country per capita for Bitcoin and cryptocurrency adoption in the world," 2021. [Online]. Available: https://africa.businessinsider.com/local/markets/nigeria-is-the-leading-country-per-capita-forbitcoin-and-cryptocurrency-adoption-in/drv4121.

[37] T. George, "Mixed methods research: Definition, guide & examples. Scribbr," 2023. [Online]. Available: Retrieved July 15, 2024, from https://www.scribbr.com/methodology/mixed-methods-research.