International Journal of E-Services and Mobile Applications
Volume 15 • Issue 1

Blockchain Maturity of Ghanaian Financial Institutions and Their Readiness to Adopt Distributed Ledger for KYC Processes

Forgor Lempogo, Ghana Communication Technology University, Ghana*
https://orcid.org/0000-0001-6329-012X

Willian Leslie Brown-Acquaye, Ghana Communication Technology University, Ghana
https://orcid.org/0000-0001-9679-5976

Millicent Agangiba, University of Mines and Technology, Ghana

Daniel Selassie Kwasi Twumasi, IT Consortium, Ghana

ABSTRACT

Although information technology has positively influenced operations in the Ghanaian financial sector, there is still a high operational cost in performing KYC procedures due to duplication of efforts during clients' onboarding. The decentralized nature of blockchains makes them ideal for addressing these challenges. In this paper, the blockchain maturity model was used to assess the maturity and readiness of Ghanaian banks to adopt blockchain technology for KYC processes. Using primary data obtained via questionnaires and interviews, the individual components of the blockchain maturity model were assessed. The results indicate that the network, hardware, and software components are at repeatable, defined, and managed stages, respectively, while the people component lags in the initial stage due to a lack of adequate staff training. Finally, security and privacy are at the defined stage, whereas policy and regulations are at the initial stage.

KEYWORDS

Blockchain, Blockchain Policy, Distributed Ledger, Know Your Customer, Maturity Model

INTRODUCTION

Financial institutions in Ghana engage in the onboarding of new customers daily as a measure to control money laundering and other fraudulent activities (AFI, 2019; Sullivan, 2015). The onboarding process involves a procedure called Know-Your-Customer (KYC), which constitutes the collection of customer information to be given to compliance officers who identify, analyze and effectively monitor high-risk customer accounts (Bukola, 2014). KYC is an elaborate process that involves

DOI: 10.4018/IJESMA.317925 *Corresponding Author

investigating a customer's profile based on self-evaluation and interviews and a steady examination of the customer's assets preferably assisted through different expert systems (Chorafas, 2006). KYC processes in Ghana are regulated by the Central Bank (Bank of Ghana), which is equally overseen by The Basel Committee on Banking Supervision (Bank of Ghana, 2022; Goodhart, 2011).

There are different KYC processes for individuals and corporate customers and the level of intensity of the process differs from one individual to another depending on unique circumstances. Customers are classified as high risk or low risk according to certain money laundering risk indicators or red flags that are crucial for fulfilling Anti-Money Laundering policies (Isa et al., 2015). These classifications determine the extensiveness of the KYC procedure to avoid any ambiguity regarding a customer's identity, location, and occupation.

Currently, there is duplication of effort across financial institutions in Ghana, as customers repeat the cumbersome KYC process in every financial institution they visit and provide the same documents they submitted to the previous institution due to the absence of a digital single source of identity for a seamless exchange of customer data and documents (Morabito, 2017).

Also, financial institutions incur high operational costs in performing KYC procedures to the extent that it makes low-balance accounts unprofitable (Alexandre et al., 2011; Islam, 2021). These operational costs include hiring and paying for the services of dedicated personnel, who spend a lot of man-hours processing customer personal and financial information as well as the accompanying document and the needed logistics that come with performing these operations. This especially put a huge financial strain on rural banks (Alexandre et al., 2011).

Additionally, the absence of a digital single source of identity and a synchronized source of customer KYC information has created a situation where fraudsters and loan defaulters, open multiple accounts across financial institutions with different KYC information that cannot be verified or tracked. They then can jump from one institution to the other without being noticed or flagged, causing various forms of losses to these institutions.

Lastly, the turnaround time for the completion of a single KYC process can typically take between 30 to 50 days (FinTech Network, 2016; Kinyua, 2020). This causes a delay in banking operations and frustrates customers who want to own bank accounts (Srinivasan, 2007). There are aspects of the KYC process such as identity verification, document verification, and the overall onboarding process and its associated exorbitant operational cost that could be optimized by applying technology.

According to Kirss and Milani (2021), even though KYC process is mandatory and expensive, with the potential to greatly reduce customer satisfaction, it does not by itself add value to the banks. Hence the recent efforts by most industry players to use technologies to optimize their KYC process, with blockchain becoming the most popular and viable technological alternative for achieving this goal (Kirss & Milani, 2021; Parra-Moyano & Ross, 2017).

Morabito (2017) describes the future financial infrastructure as a system that leverages an organization's digital identity to perform KYC activities quickly using blockchain. A distributed ledger system, such as a blockchain-based registry, not only solves the problem of duplication of effort in KYC processes but also provides a great level of security through encrypted updates to client details across all ledgers in near-real-time (Deloitte, 2016; Schlatt et al., 2022).

The distributed nature of Blockchain also allows for the dissemination of information across a peer-to-peer connection, making information available to all nodes in the network (Xu et al., 2016). Thus, Blockchain solves the problem of duplication of effort by enabling the creation of a chronological, decentralized, interbank ledger where financial institutions that need to conduct KYC verification for a new customer can access the customer's KYC information from their previous financial institutions to avoid the duplication of KYC verification procedures (Hong Kong Monetary Authority, 2017; Parra-Moyano & Ross, 2017). The operational costs are reduced as it is shared proportionally amongst the financial institutions involved (Parra-Moyano & Ross, 2017), and the turnaround time of performing KYC is significantly improved (Zheng et al., 2017). Additionally, blockchain's ability

to save transactions in an immutable, incorruptible, and irreversible manner will fundamentally help to prevent some financial information fraud (Bataev et al., 2020; Cai & Zhu, 2016).

Although blockchain has been largely touted as a potential solution to the numerous challenges in the financial sector, the technology itself is mostly considered to be in an early stage of maturity and its implementation is still faced with challenges such as scalability, security, privacy, latency, etc. (Chang et al., 2020; Üçoğlu, 2022). Hence financial institutions will be faced with numerous challenges when trying to implement Blockchain technology (Wright & De Filippi, 2015). There could be legal or policy drawbacks, business strategies, or business visions and missions that do not align with the blockchain concept (Fitzgerald et al., 2013). Some challenges such as resistance to change or the absence of key stakeholder buy-in, may not be tangible but very pronounced hindrances (Fitzgerald et al., 2013). Across the financial sector, each institution may identify some constraints that will be unique to them and other challenges that could be common across the board. Particularly, in the developing world, where investments in IT infrastructure are dangerously low (Lempogo et al., 2021), coupled with the fact that firms in these countries are usually considered to be late adopters of innovation, it has become apparent to assess the readiness to adopt blockchain in the financial sector in a country such as Ghana. In this paper, the Blockchain Maturity Model (BCMM) is used to assess the maturity of the Ghanaian financial sector to adopt Blockchain technology for KYC processes. The BCMM evaluates the level of maturity using multiple indicators namely, information systems architecture, security and privacy, policy and regulatory framework.

LITERATURE REVIEW

Blockchain Technology and Classifications

Blockchain is a disruptive technology maintained by a decentralized computer network and is considered an open general ledger where every online transaction is recorded in a chain of data blocks and available for the public to connect, transact and verify transactions (Nguyen, 2016). Dicuonzo et al., (2021) describe it as a record of a series of transactions in a decentralized shared public virtual database, without third-party intervention to validate operations, where the transactions are stored in data blocks and the set of all blocks constitutes a chain. Every node on the network can make transaction entries but not without proof-of-work and an agreement of all other nodes in the network to guarantee the accuracy of the information stored (Cai & Zhu, 2016). In other words, there is no intermediary or powerful trusted third parties such as governments or banks that manage or maintain the distributed ledger (Üçoğlu, 2022). Additionally, transactions or activities on the general ledger are timestamped and immutable thus making every transaction or activity permanent (Zhu & Chen, 2017). Blockchain provides a platform for many applications that require features such as decentralization, immutability, and transparency. In the financial sector, applications such as cryptocurrencies (Bitcoin, Ethereum, Dogecoin, etc.) are built on the blockchain infrastructure and are being used for peer-to-peer payments of services (Folkinshteyn et al., 2015).

Blockchain architecture is able to manage the participating nodes involved in transactions. Permission management on a blockchain network determines the type of Blockchain it is going to be and what it will be serving (Kirss & Milani, 2021). Two main classifications of blockchain regarding permission management include Permissionless and Permissioned networks (Xu et al., 2016). Current blockchain systems are also categorized roughly into three types, namely public, private, and consortium blockchains (Kirss & Milani, 2021; Yang et al., 2022; Zheng et al., 2017). These categorizations are so because of the principles used for their permission management. Public blockchains are permission-less blockchains whiles both private and consortium are permissioned blockchains (Frøystad & Holm, 2015). While the public blockchains have their records visible to the public and participation is open to the public without any permissions, the private and consortium blockchains are either fully or partially centralized with the regulation of participatory nodes (Zheng et al., 2017). Permissionless blockchains are open and decentralized networks that allow peers to

join and leave the network as readers or writers without the intervention of a centralized body to ban illegitimate peers from participating in blockchain activities (Wüst & Gervais, 2018). On the other hand, in permissioned blockchains, the identities of peers and validators are whitelisted through some types of KYC procedures similar to the financial institutions (Xu et al., 2016).

Smart Contracts

Another very essential disruption of blockchain has been in the area of smart contracts. Smart contracts are a collection of computerized transactional protocols that facilitate, verify and enforce the negotiation or performance of a contract by automatically executing the terms of the contract and hence reducing the transaction costs associated with conventional contracting and also hopefully providing better assurance than the conventional paper-based contract management (Sun et al., 2022; Yu et al., 2017). It is the translation of contractual clauses into code that is embedded into hardware or software and can be self-enforced when executed to minimize the need for trusted intermediaries between transacting parties (Christidis & Devetsikiotis, 2016).

On a blockchain-based system, smart contracts are snippets of code that are executed if each entry satisfies a written condition. The conditions usually take the form of an 'IF-THIS-THEN-THAT' logic and will only be passed and added to the blockchain if the set of rules and conditions are met (Morabito, 2017). Applications of smart contracts in the financial sector could be endless, from forex trading, anti-money laundering, and KYC procedures to crypto exchanges, and crypto-transaction. Specific bank products such as remittance services, investment products and financial instruments such as sub-currencies, financial derivatives, and wills can all ride on the blockchain network to pay out funds (Luu et al., 2016).

Blockchain for KYC Processes

Using blockchain, banks will be able to provide superior interactive personalized services with cloud advancements, while maintaining higher security of the information and assets (Singh et al., 2022). Blockchain architecture is characteristically decentralized, anonymous, secure, immutable, and supports the use of smart contracts for the verification of documents and information (Zhu & Chen, 2017), which are essential attributes for effective and credible KYC procedures. It is inefficient for financial institutions to repeat a process that has already been done by another institution especially when the same requirements are involved (Parra-Moyano & Ross, 2017).

Blockchain has become a platform for building important features and add-ons like GPS-based enabled services or tracking technologies and for the implementation of identity management tools (De Kruijff & Weigand, 2017). As part of the verification process of the customer's KYC information, the financial institution is required to confirm the identity of the customer and the address stated in their documents which are simplified by the built-on services on the blockchain (Fu & Fang, 2016). Using blockchain for KYC essentially requires a system that enables secure and reliable companies-to-company and company-to-regulator sharing of customers' information in near real-real time

Over time, there is a considerable buildup of academic literature on the use of blockchain for KYC. To provide banks with a fast and inexpensive way to share customer KYC documents, Norvill et al., (2019) presented the architecture and demonstrated the inner workings of a blockchain system for KYC in the financial sector. The system allows automated and simplified, permissioned document sharing between banks to improve the overall efficiency of KYC processes. Being that security of KYC data is very paramount, Norvill et al. (2020), as an improvement on the previous system, proposed a blockchain-based KYC system that maintained the banks' control over the data as well as the security and privacy of data. Using the improved system, they observed that the full cycle of adding a customer, granting and checking access, and then removing access and checking were much faster than a customer is likely to request them in a real-world scenario.

Also, Parra-Moyano and Ross (2017) presented a blockchain-based KYC system for a national regulator, aiming to improve the efficiency of customer-onboarding processes as well as compliance.

This was later refined by Parra-Moyano et al. (2019) into a dynamic, blockchain-technology-based KYC system, accompanied by a Proof of Concept (PoC) for both financial institutions and regulators, which reduces cost by allowing cost to be shared proportionally by participating institutions, as well as eliminates the need for a third-party provider (TPP) to manage permissions.

Security and privacy in a blockchain-based KYC system are mostly achieved by using blockchain in combination with other more secure technologies. Schlatt et al. (2022) demonstrated the potential to combine blockchain and self-sovereign identity (SSI) for KYC by presenting a framework that utilizes SSI to improve the efficiency of the KYC process. By using SSI on top of the blockchain layer, their framework leveraged the advantages typically associated with blockchain technology while avoiding its well-known issues with scalability and privacy. Additionally, Fugkeaw (2022) demonstrated a blockchain-based privacy-preserving KYC system that used a secure and decentralized authentication and verification mechanism for KYC processes with the user's consent enforcement feature. They observed great improvement in efficiency and scalability in terms of policy cost, encryption and decryption operations, registration and verification process with features to support transaction traceability. Sinha and Kaul (2018) proposed an integrated system of IPFS and blockchain KYC system, which among other benefits is cost-effective, fault-tolerant, attack resistant and immutable. They demonstrated that using their system increases the overall efficiency of KYC processes by 183.77%.

Kapsoulis et al. (2020) also proposed an enterprise blockchain KYC architecture based on InterPlanetary File System (IPFS) and Quorum blockchain with special emphasis on user privacy protection. As one of the few such systems to emphasize privacy, it used two types of smart contracts, namely public KYC smart contracts and private KYC smart contracts for customer onboarding and CRUD (Create, Read, Update, Delete) operations respectively. Cost-effectiveness and efficiency of operations of the architecture were achieved through smart integration of the different technological components. Finally, using Distributed Ledger Technology (DLT), cryptography and the consensus mechanism of blockchain, Yadav and Bajpai (2020) proposed a model for a KYC system that optimized storing, updating, sharing of data and accessing operations along with enhanced security, transparency and privacy, with an added advantage of enhancing customer ownership and experience.

Methodologies for Assessing Technology Maturity

Technology maturity of an organization is described simply as the organization's state of being fully developed (Leem et al., 2008). Maturity also generally refers to the state of being complete, perfect and ready, while implying the measured progress in the development of a system, which is captured qualitatively or quantitatively in a discrete or continuous manner (Schumacher et al., 2016). Competitive organizations brace themselves for new technologies and create comprehensive concepts and goals around the evolution of any new technology, while at the same time systematically identifying organizational objectives and aligning them to the technology (Bazaee et al., 2020; Leem et al., 2008).

Maturity models are commonly used as tools to conceptualize and measure an organization's maturity in the adoption of new technology (Schumacher et al., 2016). Maturity models can be assessed using methods and factors of development such as scope, design, etc. (Lees, 2016). Some of the most common methodologies for assessing technology readiness include but not limited to The Connected Enterprise Maturity Model (Rockwell Automation, 2014), the Industry 4.0 Maturity Model (Schumacher et al., 2016), The L&K model (Leem et al., 2008) and The Blockchain Maturity Model (Wang et al., 2016).

The Connected Enterprise Maturity Model has four (4) dimensions of interest, which focus on the entirety of the system, from hardware and software to the smaller controls and devices of the system as well as security and privacy. Even though it's a comprehensive model (consisting of 5 levels) that focuses on the information technology capabilities of the implementing institutions, it lacks organizational and operational dimensions, and appropriate assessment tools, as well as has undefined criteria for maturity (Ustundag & Cevikcan, 2017).

On the other hand, the Industry 4.0 Maturity Model is focused on having a significant impact on supply chains, business models, and business processes by providing benefits such as standardization in development, higher quality, flexibility, continuous benchmarking, and global competitiveness among strong businesses (Gökalp et al., 2017). Although the model is very comprehensive, it has a limited application area, mainly focusing on the manufacturing industry (Lees, 2016).

The L&K model is one of the latest maturity models that overcame the shortcomings of previous models. Unlike The Connected Enterprise Maturity Model, The L&K model supports practical evaluation tools and comprehensively expands its framework into 345 measurable items covering several organizational items that need to be assessed for readiness (Leem & Kin, 2004). A noticeable shortcoming however is the sheer size and complexity, requiring extensive tweaking and customization to suit the various business scopes, characteristics, and cultures.

The Blockchain Maturity Model

The Blockchain Maturity Model (BCMM) provides a framework that adopts the Association of Computer Machinery (ACM) Computing Classification System (CCS) (ACM, 2014) for the assessment of four critical components necessary for organizations to adopt blockchain technology namely, Networks, Information systems, Computing methodologies, and Security and Privacy (Wang et al., 2016). The significance of this model lies in its use of the Capability Maturity Model (CMM), which according to Paulk et al (1995), describes key performance areas from an initial level of maturity to an optimization maturity, to measure the maturity of each of the CCS components. The model determines maturity by assessing each of the components, placing them into one of the five (5) levels of maturity, namely Initial, Repeatable, Defined, Managed, and Optimized.

According to Wang, Chen, and Xu (2016), the 'Initial' stage is a chaotic period that usually involves the emergence of new technologies or new processes and as such generates a general lack of understanding in the organization. The 'Repeatable' stage is a reactive stage that has its methodologies established, controlled, and coordinated, with the tendency of reproducing successes from previous encounters. At the 'Defined' stage, there is a proactive approach to documenting all established methodologies and maintaining standards for future tests, developments, or maintenance. The 'Managed' stage involves the establishment of quality metrics for measuring the performance of the organization's methodologies or systems. By the 'Optimized' stage, an organization can continuously improve its process by adopting technological innovations and also share the knowledge of its practices with the wider community. The stages in the CMM and how they are applied in the BCMM are shown in Table 1.

In assessing Computing Methodologies Wang, Chen, and Xu (2016) looked at the Standardization and Computational complexity of the technology itself. In this paper, however, we instead looked at the Policy and Regulatory Frameworks within the country that will govern the adoption and use of blockchain, since the subject of study is the maturity of the financial sector and not the blockchain

Table 1.
The Blockchain maturity model

	Initial (stage 1)	Repeatable (stage 2)	Defined (stage 3)	Managed (stage 4)	Optimizing (stage 5)
Networks		Network load	Reliability		
Information Systems	Architecture Upgrading Integration	Maintenance Storage Scalability		Business efficiency	
Computing Methodologies	Standardization	Computational complexity			
Security and Privacy			Privacy	Data security Transaction security	

Source: Wang, Chen, and Xu (2016)

technology itself. Also, Hassani et al. (2008) strongly link the success of blockchain-based KYC of financial institutions to cross-bank policies standardization, with Kawasmi et al. (2020) confirming that the lack of such policies and industry standards could seriously hinder the adoption of blockchain technology across the sector.

The choice of BCMM for this study is based on the fact that it represents a simple taxonomy of maturity assessment using very few assessable indicators. Additionally, all the individual indicators are clearly defined, requiring very little tweaking and customization to suit the business scopes, characteristics, and cultures of the financial industry.

Blockchain Adoption in Financial Institutions

According to UNCTAD (2021), the finance industry is one of the earliest adopters of innovative technologies such as big data and blockchain. Within this sector, these technologies are actively being used to improve operational and transactional processes such as credit decisions, risk management, fraud prevention, trading, personalized banking, and process automation. Adopting blockchain technology in the financial sector takes into consideration obstacles that might hinder or affect its success and requires further agreement on the implementation standards across institutions, including technology scalability and interoperability (Morabito, 2017). Various researchers have conducted studies into technology adoption in different sectors of the economy, with varying conclusions.

In assessing the readiness of the Korean Financial Industry in adopting blockchain technology, Gokhale (2016) concluded that blockchain technology would have to be thoroughly tested for its robustness, security, and data integrity before there can be a mass integration of the technology into the Korean financial markets. The study also opined that the Korean government regulation at the time was not abreast with the advancement in blockchain technology and as such any such implementation would involve the input of regulatory bodies.

Using the L&K Model, Leem et al (2008) analyzed the behavior of South Korean enterprises towards IT adoption and usage, revealing that even though a majority of the small enterprises were in stage 2 (IT Infrastructure Stage) maturity, a few of the large enterprises fell in stage 3 (IT Organization and Rules Stage). They attributed the unpreparedness of the small enterprises to suboptimal infrastructure implementation caused by a lack of education and improper organizational change, creating dissatisfaction in IT investments. Given that South Korea in terms of technology and innovation is many steps ahead of Ghana (UNCTAD, 2021), it is of great interest to determine how the Ghanaian financial sector will perform over a decade later.

METHODOLOGY

Research Design

According to Pandey and Pandey (2015), a good research design is significant in facilitating the smooth scaling of research operations, by applying appropriate data collection techniques and providing a suitable guide for the research. The descriptive research design was adopted for this study since according to (Kothari, 2004), it allows the researchers to clearly define what must be measured and provides adequate methods for the measurement.

Research Population

The population of research describes the complete collection of data that contains the data points of interest and whose properties or characteristics are analyzed and studied (Bartolucci et al., 2016). The financial sector in Ghana is made up of financial institutions including banks and regulators that supervise KYC processes in the financial sector as well as third parties that play a role in the process. A total of twenty-four thousand, three hundred (24,300) people are employed in the twenty-three (23) commercial banks that are regulated by Ghana's central bank (Ankrah, 2018). The population of this

study is limited to commercial banks for two reasons: (1) commercial banks will be the initiators of KYC processes if blockchain is adopted. This is because other transactions within the sector such as insurance brokerage, investments, etc., must involve these banks at a certain point in their lifetime. Thus, all payments and transfers must pass through a bank that should already have performed KYC for the parties involved. (2) Compared to other deposit-taking institutions such as rural banks and micro finances, commercial banks are the leaders in technological innovation (Dahl et al., 2017).

Sample Selection

A purposive sampling technique was employed for this study with the following criteria: (1) Respondents were conversant or involved with the KYC processes of banks. (2) Respondents had sufficient knowledge in information and communication technology (ICT), and (3) Respondents were knowledgeable in blockchain technologies. According to Etikan et al., (2016), purposive sampling, also called judgment sampling, involves the deliberate selection of participants due to their qualities such as knowledge in a field of work and/or interest in a particular matter. Its strength lies in its intentional bias and despite this inherent bias, it is known to provide robust and reliable data (Tongco, 2007).

Since Hair et al., (2010) recommend a rule of thumb of 5-10 sampled respondents per every measurement variable, a representative sample size of one hundred and thirty (130) respondents (13 variables x 10) was selected for the survey. Out of which hundred and twenty (120) were employees of the banks and third parties, while ten (10) were industry experts.

Data Collection Method

The study employed a structured self-administered questionnaire (for the 120 sampled bank and third-party employees) and semi-structured interviews (for the 10 sampled industry experts/practitioners) as the data collection instruments to obtain the primary data. Questionnaires and interviews were based on the BCMM and adopted a mix of close-ended and open-ended questions to glean enough information from respondents that were truly representative of their opinions.

Twelve (12) respondents were used to pretest the questionnaire, with the data collection process commencing only after all amendments have been effected.

The four (4) components of the BCMM, namely, Networks, Information System Architecture (hardware, software, and people), Computing Methodologies, and Security and Privacy, were assessed. The network component was measured by two measurement variables namely, bandwidth and causes of latency. The information systems component, on the other hand, was measured by eight measurement variables namely, Possibility of Extending Storage Capacity, Reasons for System Upgrade, Reasons for System Replacement, Mode of Communication with Third-Party Systems, Processes of Applying Updates and System Integration Implementation Methods, as well as Frequency of staff training on new systems and Frequency of External staff training. Lastly, the security and privacy component was measured by three measurement variables namely, Mechanisms for Ensuring the Privacy of Customer Information, Frequency of Penetration Testing, and Mechanisms for Ensuring Data Packet Security. Altogether, thirteen (13) Measurable variables were used.

During the data collecting process, 116 out of the 120 questionnaires sent out were returned, out of which six (6) questionnaires were rejected because they contained more than 25% blanks per Sekaran (2006), which stipulates that a questionnaire can be scrapped and not added to the data set for analysis if blank spaces account for over 25% of the entire questionnaire. Also, one (1) industry expert could not be available for most of the scheduled interviews leading to his exclusion from the sample. This subsequently, brings the valid questionnaires to 110 and the valid industry experts interviewed to 9.

The survey data was cleaned, coded, and analyzed using Microsoft Excel 2016. Also, after transcribing the interview files, the data were coded and analyzed in MS Excel after identifying the themes for categorization. Data analysis was both descriptive and inferential as the collected data is represented using measures of central tendencies as well as visually shown as frequency distribution tables. The demographics of the respondents for both the questionnaire and interview are shown in table 2.

Table 2.
Demographics of respondents

Demographic	Item	Frequency	Percentage (%)
Age	25 - 35	67	56.30
	35 - 45	45	37.82
	Above 45	7	5.56
Education	Diploma	9	7.56
	Bachelors	81	68.07
	Masters	27	22.69
	Doctorate	2	1.68
Gender	Male	73	61.34
	Female	46	38.66
Role	Top Management	16	13.45
	Mid-Level Management	38	31.93
	Non-Management	65	54.62

RESEARCH FINDINGS

In the assessment of blockchain maturity of Ghanaian financial institutions and their readiness to adopt Blockchain technology for KYC processes, the maturity of the institutions' information systems, security and privacy methods, and regulatory framework were assessed using the Blockchain Maturity Model.

Information systems architecture of financial institutions

Wang, Chen, and Xu (2016) considered information systems components to be made up of the requirements of the blockchain which are the Network, Hardware, Software, and People. The states of each of these components were assessed and the results are presented as follows.

Network Component

The efficiency and reliability of the network are very crucial for the success of any blockchain project since the technology is mostly controlled by the network infrastructure. In assessing the maturity of the network, the bandwidth and latency of the institutions' network were assessed. A summary of the findings is presented in table 3.

It was revealed that most financial institutions (as indicated by 85 percent of respondents) operate with a download bandwidth below 10Mb/s (table 3), with no institution registering a bandwidth above 50Mb/s.

It was also discovered that the majority of the institutions (72 percent of respondents) experience high network latency when network traffic increases, compared to other causes such as bad weather conditions (10.9%), the distance between the source and the destination (9.1%), fiber cuts (0.9%), router issues (0.9%), problems with the service providers (0.9%) and others (4.5%).

Nevertheless, the majority of the respondents (63 Percent) still considered their network to be reliable, with 37% admitting their network has not been reliable.

Hardware Component

In Assessing the hardware maturity of financial institutions, it was necessary to assess the scalability of existing storage since adopting blockchain technology requires every institution to store a duplicate

Table 3.
Summary of findings for Network component assessment

Designation	Frequency	Percentage (%)
Average Bandwidth of Office Internet – Download (Mb/s)		
Less Than 1	33	30.0
1 – 10	61	55.5
11 – 25	12	10.9
26 – 50	4	3.6
51 – 75	0	0.0
76 – 100	0	0.0
Greater Than 100	0	0.0
Causes of High Network Latency		
Increase in Network Trafic	79	71.8
Bad weather	12	10.9
Distance Destination	10	9.1
Fiber cuts	2	1.8
Router Issues	1	0.9
Service Provider Issues	1	0.9
Other issues	5	4.5

block of transactions from every other participating node leading to a voluminous transactions ledger. Additionally, in adopting blockchain for KYC processes there is a very high possibility that these organizations will be required to change or upgrade portions or their entire system. Hence, the willingness and preparedness of organizations to implement the needed upgrades are considered by assessing the availability of a testing environment as well as the reasons for a system upgrade and/or replacement. A summary of the finding is presented in Table 4.

It was revealed that all of the institutions surveyed currently have enough memory for the storage of KYC data, with a majority of institutions having the requisite hardware infrastructure to support additional memory. As shown in Table 3, a majority of the respondent (43.6%) indicated that their institutions have the necessary hardware infrastructure to support double the current storage capacity. Another 40.9% indicated that their storage capacity could be extended to more than three (3) times the current capacity. 9.1% indicated their system could support triple the current memory capacity, with only 4.5% of respondents indicating they lack the requisite infrastructure for an extension of memory capacity.

Although not all respondents (only 80%) confirmed the existence of a testing environment, all respondents unanimously confirmed upgrading and changing part of their hardware within the past 24 months, signaling the readiness of the financial institution to improve or at least maintain a stable system. According to the findings, the main reasons why these institutions upgraded their hardware were to increase efficiency (60%); stay competitive in the industry (20.9%); comply with industry standards (10.9%) and meet the demands of customers (8.2%). When it came to the total replacement of the hardware, however, the results became much more thinly spread. The main reasons indicated by respondents that necessitated a total system replacement include the need to support business strategy (46.4%); a newer version was available (16.4%); when regulators demanded it (14.5%); when the existing system had a functional defect (11.8%); when the manufacturers stopped providing support for the existing equipment (10.9%).

Table 4.
Summary of findings for hardware component assessment

Designation	Frequency	Percentage (%)
Possibility of Extending Storage Capacity		
Cannot be Extended	5	4.5
Up to Double the current capacity	48	43.6
Up to Triple the current capacity	10	9.1
More than Triple the current capacity	45	40.9
Not sure	2	1.8
Reasons for System Upgrade		
To increase efficiency	66	60.0
To stay competitive.	23	20.9
To comply with industry standards	12	10.9
To meet customer demand	9	8.2
Reasons for System Replacement		
To support business strategy	51	46.4
When a newer version is available	18	16.4
When the manufacturer no longer supports the system	12	10.9
When regulator demands	16	14.5
When the Existing system is faulty	13	11.8

Software Component

The blockchain concept is still fairly new and as such there will be a continuous release of system updates to stabilize the technology as it is with any innovation. Also, adopting blockchain technology for KYC processes will require the systems of different institutions to communicate with each other. Hence, it is critical to assess how institutions apply system updates and even how system integrations are conducted. Assessment of the software component of the information systems architecture involves investigating how the current systems of financial institutions communicate with other systems, the process of applying updates to systems, and how system integration is implemented. A summary of the findings is presented in Table 5.

The findings show that not only have most financial institutions (over 98%) in the country moved away from operating stand-alone systems (only 1.8%), but they have also employed a variety of innovative technologies to exchange information with third-party systems for KYC activities. The most popular of which was found to be API architecture (40.9%), followed by ISO protocol (28.2%), file transfer between systems (19%), EDI integration (8%), and others (2.7%).

The results also revealed that the IT departments of most of the institutions (over 77%) have been empowered to apply system updates (out-of-place – 60% and in-place – 17.3%) which will usually depend on a laid down operational standard procedure rather than a bureaucratic process. Additionally, 11.8% rely on the authority of a steering committee to apply updates whiles 10% leave the job of applying updates to third-party consultants, with 0.9% using other methods.

Regarding who leads the system integrations processes, the results show that the majority of institutions (61.8% of respondents) implement system integrations using a collaboration of the in-house IT team and external consultants. A few (20% of respondents) however, use only the In-house IT team, only external consultants (17.3% of respondents), and other methods - 0.9%.

Table 5.
Summary of software component assessment findings

Designation	Frequency	Percentage
Mode of Communication with Third-Party Systems		
API architecture	45	40.9
ISO protocol	31	28.2
File Transfer	21	19.1
EDI Integration	8	7.3
Other	3	2.7
None	2	1.8
Processes of Applying Updates		
IT team (out-of-place update)	66	60.0
IT team (in-place update)	19	17.3
Steering committee	13	11.8
Third-party consultants.	11	10.0
Other	1	0.9
System Integration Implementation Methods		
IT Team and Third Party Consultant	68	61.8
IT Team (In-house)	22	20.0
Third-party consultants (Outsourced)	19	17.3
Other	1	0.9

The People Component

Assessing the people component of the information systems architecture involves the assessment of how institutions currently train their staff on cyber-security issues, how often institutions train their staff on the use of new systems and how often external training sessions are organized for staff. The people component is necessary for assessing the readiness of staff to work with blockchain technology, as well as the willingness of the institution to support existing staff to acquire the requisite knowledge and skill to use new technologies. A summary of the findings is presented in table 6.

Like any other innovative technology, all respondents unanimously agreed that adopting blockchain for KYC processes will require a significant upgrade in their technical knowledge and expertise in the area. However, it was discovered that most institutions do not keep a regular staff training regime. When it comes to the readiness of institutions to provide training to staff when new systems are implemented in the organizations, a majority of the respondents (40%) indicated that they mostly learn on the job without any special in-house training. Another 25.5% only receive training when resource persons are available in-house. Only 34.6% keep a regular training regime, receiving training at least once a year in-house. Institutions are rather more willing to send staff out to attend external training programs to enhance their skill. A majority (60%) of employees received external training when their role required a particular new skill. Additionally, 36.4% of employees attended external training at least once a year. Only 3.6% of employees have never received any external training.

Table 6.
Summary of People component assessment findings

Designation	Frequency	Percentage
Frequency of staff training on new systems		
Quarterly	18	16.4
Twice a year	10	9.1
Once a year	10	9.1
Based on the availability of the resource persons.	28	25.5
Staff learn on the job.	44	40.0
Frequency of External training for staff		
Quarterly	7	6.4
Twice a year	13	11.8
Once a year	20	18.2
When your role requires it	66	60.0
Never	4	3.6

Security and privacy concerns regarding the use of blockchain technology

In the BCMM, the privacy and security category stands on its own and is measured to determine the maturity level of an organization for adopting blockchain or any technology for that matter (Wang et al., 2016). Security and privacy readiness were measured through the assessment of the following three areas, namely, mechanisms used by organizations for ensuring the privacy of customer information; the frequency of which penetration testing is carried out at each of the assessed institutions; and the mechanisms employed by institutions to ensure data packet security across the network. The findings are presented in table 7.

The results reveal that financial institutions have adopted a combination of reactive and proactive mechanisms to ensure customer data is secure. Data encryption was found to be the most dominant technology used to ensure privacy in the sector as 44.5% of respondents confirm its use in their institutions. Followed by access level mechanisms, 39%, and multifactor authentication, 13.6%. Security tokens (2.7%) were found to be the least adopted measure to ensure the privacy of customers' data.

In ensuring the security of the network, however, antivirus technologies were found to be the most popular mechanism as 73.6% of respondents confirmed its use in their institution. Followed closely by Internet Protocol Security (IPsec) 61.8% and DMZ, 39.1% as a form of defensive mechanism against external attacks. Only 12.7% of the respondents opted for Pretty Good Privacy, while 0.9 opted for each of the remaining including utilizing tunneling technologies (such as DMVPN, IPSEC Tunnels, and GRE Tunnels), firewalls technologies, and DDOS.

Additionally, it was revealed that most institutions (63.6%) perform penetration tests at least once every year, which is consistent with the guidelines in (Kionga, 2020). However, 28.2% of the institutions perform these tests when there is an opportunity or resources become available. While some 8.2% are yet to conduct any such tests.

Policy and Regulatory Requirements for Blockchain Adoption

In assessing the policy and regulation component of the model, qualitative data was gathered by interviewing nine (9) industry experts (including IT experts, consultants, software developers, and blockchain Industry practitioners) to help gauge the complete sentiment across the industry.

Table 7.
Summary of Security and privacy component assessment findings

Designation	Frequency	Percentage
Mechanisms for Ensuring Privacy of Customer Information		
Data Encryption	49	44.5
Access Levels	41	37.3
Multi-Factor Authentication	15	13.6
Security Tokens	3	2.7
Other	2	1.8
Frequency of Penetration Testing		
Quarterly	38	34.5
Twice a year	16	14.5
Once a year	16	14.5
When resources become available	31	28.2
Yet to be done	9	8.2
Mechanisms for Ensuring Data Packet Security (Multiple answers allowed)		
Antivirus	81	73.6
Internet Protocol Security (IPsec)	68	61.8
DMZ	43	39.1
Pretty Good Privacy	14	12.7
Tunneling technologies (DMVPN, IPSEC and GRE)	1	0.9
Firewalls	1	0.9
DDOS	1	0.9

Adequacy of Current Laws and Policies

The sentiment was unanimous across the board that the adoption of blockchain technology would not require any significant change or amendment in the current KYC policies. One of the IT Expert/ Consultant opined that even though significant changes will not be required for the initial adoption, there need to be certain minor adjustments to ensure the sustainability of the technology:

…….. Even though changes may not be needed right away, there definitely might be a few adjustments in the future as we get to see the issues that will arise. Thus, fine-tuning may be needed in the long run. Nonetheless, I still believe the current laws are enough to adequately regulate the industry.

Another IT expert while agreeing that the laws do not need a change even proposed some of the additions that might be needed to facilitate a quick take-off, including the introduction of incentives and criminalizing certain actions of customers:

They will not change, but there could be additions. Two major possible policy additions could include those that give incentives for financial institutions that perform the initial hard work of KYC and customer due diligence and also the criminalizing of customers deliberately providing wrong information during the KYC process……..

The introduction of incentives to financial institutions that initiate KYC processes, for instance, could be a significant driver for the adoption of blockchain technology. Also criminalizing the deliberate provision of inaccurate customer information could help ensure that the information is accurate from the source since there have to be mechanisms to ensure the accuracy of the information of every new customer at the collection point before it is distributed through the network. A few however were skeptical, questioning the preparedness and willingness of the regulators to adequately enforce these regulations. As indicated by one of the software engineers:

…….Regulations in our books are robust in so many ways. The issue usually has to do with the willingness of state actors to enforce them.

Mode of Blockchain Implementation

When it came to whether blockchain adoption should be imposed by the policymakers on the financial institutions, most (89%%) of the experts disagreed, with some proposing ways to improve the adoption rate without compulsion. One of the software developers suggested that instead of forcing banks to adopt the technology, the regulator could use a bank's adoption to boost its rating:

Blockchain adoption should be optional. Instead of issuing licenses for blockchain technology, an institution's adoption of blockchain technology could be used as a means for measuring a bank's ratings to indicate the use of best practices.

It is believed that this could significantly improve participation in an already very competitive industry. This sentiment was largely confirmed by another IT consultant who believed that Banks are already aware of the potential value of technologies such as blockchain and if an enabling environment is created, they will not hesitate to adopt it:

The banks for instance are already fiercely competing in every area. If the internet and other enabling technology are available to them, they will adopt blockchain without hesitation. They already know the value of such technologies.

Another IT Consultant opined that the role of the regulators must be to ensure that the right data is captured, and checked for fraud as well as ensure the protection of data under the Data Protection Act. It was also generally implied from all the opinions that even though blockchain technology is distributed and does away with trusted third parties, there should still be some control by a regulatory entity.

However, a few who believe the technology should be imposed on the institutions feared that leaving it to the banks may delay the process because most banks may not be willing to be the first to share their data:

……..It must be compulsory for all banks, otherwise, every bank will wait to see how it will work. Since they might not want to be the first to share their data.

Who should lead?

It was almost unanimous (89%) that it is a bad idea for the regulator to try and lead since the banks are in a better position to understand what is best for their business. It was generally the opinion of the experts that the regulator is not in the position to lead since they lack the technical expertise to do so. As opined by one of the IT consultants, the Ghanaian regulators will not be willing to implement

blockchain until the regulator sees other financial institutions around the world implementing and benefiting from it:

Ghana is generally a late adopter of technology and the regulator is also showing no signs of initiative in this discovery. As a result, blockchain technology may become popularized in about five(5) years especially when leading financial institutions around the world are upholding it.

Some even believe that for fear of losing control the regulator might not be willing to lead the process:

From experience working with the regulators, I don't believe the regulators will take up the initiative to adopt the technology as they may lose some control over the financial institutions.

However, the 11% who believe the regulator must lead opined that the regulator has the muscle to compel all banks to join the network. Believing that the benefits of blockchain technology may not be realized if only a few banks join the network.

DISCUSSING OF FINDINGS

Network

Since blockchain requires a stable and reliable network to achieve a real-time update of the ledgers on all participating nodes, the reliability, and stability of the network are very crucial for its success. The results point to a general confirmation of network reliability across most institutions. However, there was also an acknowledgment of an increase in network traffic being the chief cause of high network latency. Hence, the network component was placed at the 'Repeatable' stage since the network traffic problem still exists but is controlled and coordinated to still provide a generally stable network (see table 8). This is consistent with the finding of Wang et al., (2016), who also placed the network component at the 'Repeatable' stage, identifying it as the main concern for blockchain adoption.

Hardware

The Hardware component of the Information Systems architecture was assessed based on the storage capacity, availability of a testing environment, frequency of system upgrades, and the reasons for upgrading. The results indicate that institutions are generally proactive in investing in increasing their

Table 8.
Summary of Blockchain maturity of Ghanaian financial institutions using BCMM

		1. Initial	2. Repeatable	3. Defined	4. Managed	5. Optimized
Networks	**Network**		Internet Bandwidth Network load Network reliability			
Information Systems	**Hardware**		System upgrade	Storage	Testing Environment	
	Software		System updates	System integrations	Systems communication	
	People	Staff training				
Computing Methodologies	**Policy and Regulatory requirements**	Policy and Regulation				
Security and Privacy	**Security**			System Security		
	Privacy			Data Privacy		

storage capacity. This is a crucial development since institutions most definitely will be required to invest in upgrading the hardware infrastructure to accommodate the large volumes of data they will need to store in the distributed ledger, as alluded to in Swan (2015). Nonetheless, Wang, Chen, and Xu (2016) indicated that traditional storage is not efficient for blockchain adoption. Hence, the Storage is placed at the 'Defined" stage. On the other hand, the testing environment component was placed at the 'Managed' stage since the results point to the existence of a testing environment in most (over 80%) of the institutions. Additionally, the results revealed that institutions did not keep a policy on system upgrades. Instead, these activities are reactive and only performed when it is needed to attract customers or when the strategy of the business demands it. Due to the reactive nature of the system upgrade component, it was placed at the 'Repeatable' stage (see table 8).

Software

Since the results reveal that more than half of the institutions have moved away from the use of purely stand-alone systems, suggesting that systems are getting more consolidated and reliable. Hence, communication was placed at the 'Managed' stage. As opined by Egner (2017), financial institutions have realized that using APIs to communicate with third-party systems opens up one's systems. Thus, attracting traffic to one's products and co-creating customer value for the end-user, as well as encouraging the sharing of losses and profits amongst participants involved in the API ecosystem when exploring new markets. According to Huang and Tilley (2003), the managed stage involves defined quality management strategies for the established processes employed to manage risk effectively.

The results also suggested that the various Information Technology departments have been empowered to apply system updates in the test environment and then in production which will usually depend on a laid down operational standard procedure rather than a bureaucratic process. This effectively led to the placement of the system update component at the 'Repeatable' stage, since institutions will not need significant changes with a new system (see table 8).

The presence of in-house developers working with consultants is a proactive attempt by institutions to cut down on implementation costs and also facilitate system integrations. Hence it was placed at the 'Defined' stage. At the defined stage, standards and process management procedures are not only established but properly outlined for organization-wide usage (Huang & Tilley, 2003).

People

Across the institutions, there is a general lack of initiative for skill and awareness training on new technologies. Even though institutions will usually train staff at least annually, the availability of resource persons for specific subject areas is still a determining factor for taking up training for most institutions. Skills level and expertise in blockchain and other advanced technologies in Africa are relatively low, posing a challenge for projects and initiatives in their quest to find and attract adequate talent for solution development (Smart Africa, 2021). This is because blockchain technology is still not fully emerged and providing training sessions for institutions will be fully dependent on the availability of an expert, which in most cases will be nonexistent. The people aspect of the Information Systems architecture is therefore placed at the 'Initial' stage (see table 8).

Security and Privacy

The results revealed that financial institutions are very concerned about security and data privacy and have adopted multiple methods to ensure their systems are secure and the privacy of customer information is guaranteed. The privacy concern of blockchain technology for the Ghanaian financial industry is how the blockchain seeks to keep customers' information private, especially from competitors and the general public. Security-wise also, financial institutions are concerned about how their systems are secured from external threats and attacks from fraudsters. A major concern is whether the blockchain truly provides a more robust system compared to the traditional methods

concerning security and privacy since there may be less confidence in newer systems. Generally, the results revealed that financial institutions are proactive with regard to security during the setting up of their systems for operations thereby placing the security component at the 'Defined' stage (see table 8).

Also, the results showed that institutions will want to first hide sensitive data by encryption which signifies the priority put on the privacy of its information and that of its customers. Financial institutions have documented standards when it comes to the privacy of information putting it under the 'Defined' stage. As indicated by Mattila (2016), for permissioned blockchains such as what is being discussed in this research, there is increased security and more privacy with people's financial assets since blockchain allows records of ownership to be created and afterward made immutable. Additionally, blockchain provides a solution that offers a human-centric solution to access, share and manage personal data but with strict adherence to security and privacy standards (Baars, 2016).

Policy and Regulatory Requirements

The results suggest a lack of concrete solutions on how to seamlessly merge the policy and regulatory requirements with the use of blockchain technology for KYC. Even though policies already exist for the traditional KYC method, there seems not to be a straightforward approach to simply translating the policy and regulatory requirements to the blockchain implementation roadmap. As posited by Patel, Bothra, and Patel (2017), the uncertain regulatory status of the subject matter compared to other regulated technologies hinders the proliferation of blockchain awareness in the financial industry. According to Mattila (2016), factors that could affect the adoption of blockchain technology could include the rise of competing disruptive technologies and also changes in regulations. It is revealed that there is supposed to be some control of some sort over the blockchain technology especially as it is being used for KYC but it is also uncertain whether the regulator will embrace the technology and assume that control.

Since the technology is still unclear both to regulators and financial institutions, measuring the readiness of policy and regulatory requirements regarding the adoption, it is appropriate to place this at the 'Initial' stage (see table 8). This is because there is still a lack of understanding of the role of regulations and policies in blockchain technology for KYC which in itself is an emerging trend.

As concluded by Wang, Chen, and Xu (2016), the blockchain system itself has not attained optimum maturity but has very promising potential. By extension, in adopting blockchain technology for KYC, financial institutions will eventually be fully ready in all the aspects under investigation. Ghanaian financial institutions are late adopters of new technology but warm up to it eventually, especially when there is enough evidence of its usage and there is sufficient understanding and appreciation of the technology.

CONCLUSION

There are currently numerous applications for blockchain technology, which will only continue to grow. The use of blockchain technology in the financial sector allows financial institutions and regulators to access reliable customer KYC information in near real-time. Blockchain technology also increases the ability of regulators as well as banks to track customers across the industry to enforce compliance and reduce fraud within the sector. However, the Ghanaian financial sector was largely found to be in the very early stage of maturity and unready to adopt blockchain for KYC in its current state, since within the framework of the BCMM, the information system architecture, the security and privacy management levels, and policy and regulatory requirements of blockchain adoption in the financial sector were found to be in Repeatable, Define and Initial stages respectively.

Even though the information system architecture is at the repeatable stage of maturity, there is a sense of proactiveness for possible changes and investment in systems if blockchain technology is truly seen to guarantee operational and overall efficiency. Also, given that security and privacy are reactive actions from financial institutions (Ahram et al., 2017), it presupposes that maturity in this

area will improve if blockchain technology is introduced especially since blockchain provides in-built security controls that adopt big data and data management services in masking and auditing data. Additionally, The central bank has a role to play at least in setting clear and concise standards. Even if the bank does not lead the process, it must at least facilitate and coordinate the adoption process. Alternatively, in creating standards and compliance measures for financial institutions, the regulators could experiment with a few banks to build confidence before attempting any large-scale adoption. There is also the need for working collaboration between technocrats in the financial, technology, and regulatory sectors to bring out the full potential of blockchain technology as it pertains to our Ghanaian markets.

This paper gives relevant insights for academics on a number of levels. To the scientific community, it demonstrates the feasibility and applicability of the BCMM in a real-world scenario to assess the maturity of a significant economic sector of a developing economy. Also, it paints a comprehensive picture of the state of technological maturity and exposes some of the major limitations that currently hinder the adoption of blockchain for KYC in the Ghanaian financial sector, pointing to the specific areas that need improvement and the specific type of improvement and investment need. These findings serve as a reference for practitioners and researchers in the field of blockchain adoption in developing countries.

The limitations of this research include the relatively low sample size of both bank employees and blockchain experts, as well as the chosen sub-sector (only commercial banks were used). Even though the chosen sample was representative of the current research, generalization of the finding may become problematic, since apart from banks, the financial sector is made up of diverse institutions, such as insurance brokers, credit unions, etc., with variable structures and needs.

Future research should therefore expand the research population and sample size to cover the other sub-sectors of the industry. Other areas of future research may include developing and studying methods and frameworks for the integration and migration of existing customer KYC information to the blockchain platform since the efficiency of this transition including the integration and migration is equally paramount to the adoption of the technology. By extension, frameworks, documentation, or software libraries must be developed to guide the setup of blockchain technology and provide guidelines for integration with other third-party systems.

ACKNOWLEDGMENT

Conflict of Interest

The authors of this publication declare there is no conflict of interest.

Funding Agency

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors.

REFERENCES

ACM. (2014). *ACM Computing Classification System (CCS)*. Retrieved Aug. 6, 2022, from https://www.acm.org/publications/class-2012

AFI. (2019). AFI Special Report: KYC Innovations, Financial Inclusion and Integrity. In *Selected AFI Member Countries*. Alliance for Financial Inclusion.

Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., & Amaba, B. (2017). *Blockchain technology innovations. In 2017 IEEE technology & engineering management conference (TEMSCON)*. IEEE. doi:10.1109/TEMSCON.2017.7998367

Alexandre, C., Mas, I., & Radcliff, D. (2011). Regulating New Banking Models that Can Bring Financial Services to All. *Challenge*, *54*(3), 116–134. doi:10.2753/0577-5132540306

Ankrah, N. O. (2018). *Over 70% bank staff want to quit over low salaries, unrealistic targets Report.* Citi News. Retrieved Dec. 21, 2021, from https://citinewsroom.com/2018/09/24/over-70-bank-staff-want-to-quit-over-low-salaries-unrealistic-targets-report/

Baars, D. (2016). *Towards self-sovereign identity using blockchain technology* [Master's thesis]. University of Twente. Retrieved from https://essay.utwente.nl/71274/1/Baars_MA_BMS.pdf

Bank of Ghana. (2022). *Know Your Customer Policy.* Retrieved July 25, 2022, from https://www.bog.gov.gh/supervision-regulation/know-your-customer-policy/

Bartolucci, A. A., Singh, K. P., & Bae, S. (2016). *Introduction to Statistical Analysis of Laboratory Data*. John Wiley & Sons. doi:10.1002/9781118736890

Bataev, A., Koroleva, E., Lukin, G., & Sviridenko, M. (2020). Evaluation of the Economic Efficiency of Blockchain for Customer Identification by Financial Institutions. In *IOP Conference Series Materials Science and Engineering.* OP Publishing. doi:10.1088/1757-899X/940/1/012038

Bazaee, G., Hassani, M., & Shahmansouri, A. (2020). Identifying Blockchain Technology Maturity's Levels in the Oil and Gas Industry. *Petroleum Business Review*, *4*(3), 43–61.

Bukola, A. (2014). *AML De-Risking: An Effective Method of Plugging AML Control Failures?* Association of Certified Anti-Money Laundering Specialists. Retrieved from https://www.acams.org/wp-content/uploads/2015/08/AML-De-Risking-An-effective-method-of-plugging-AML-controlfailures-B-Adisa.pdf

Cai, Y., & Zhu, D. (2016). Fraud detections for online businesses: A perspective from blockchain technology. *Financial Innovation*, *2*(1), 10. doi:10.1186/s40854-016-0039-4

Chang, V., Baudier, P., Zhang, H., Xu, Q. A., Zhang, J., & Arami, M. (2020). How Blockchain can impact financial services – The overview, challenges and recommendations from expert interviewees. *Technological Forecasting and Social Change*, *158*(6), 120166. doi:10.1016/j.techfore.2020.120166 PMID:32834134

Chorafas, D. N. (2006). Know your customer and his or her profile. In Wealth Management: Private Banking, Investment Decisions and Structured Financial Products (pp. 24-45). Elsevier Ltd. doi:10.1016/B978-075066855-2.50002-7

Christidis, K., & Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. *IEEE Access: Practical Innovations, Open Solutions*, *4*, 2292–2303. doi:10.1109/ACCESS.2016.2566339

Dahl, D., Meyer, A. P., & Wiggins, N. (2017). *How Fast Will Banks Adopt New Technology This Time?* Federal Reserve Bank of St. Louis. Retrieved Jul. 24, 2022, from https://www.stlouisfed.org/publications/regional-economist/fourth-quarter-2017/banks-adoption-fintech

De Kruijff, J., & Weigand, H. (2017). *Towards a Blockchain Ontology.* Research report Tillburg University. Retrieved from https://www.list.lu/fileadmin/files/Event/sites/tudor/files/Training_Center/OTHERS/VMBO2017_paper_5.pdf

Deloitte. (2016). *Blockchain applications in banking*. Deloitte LLP.

Dicuonzo, G., Donofrio, F., Fusco, A., & Dell'Atti, V. (2021). Blockchain Technology: Opportunities and Challenges for Small and Large Banks During COVID-19. *International Journal of Innovation and Technology Management*, *8*(4), 2140001. doi:10.1142/S0219877021400010

Egner, T. (2017). Open APIs and Open Banking:Assessing the Impact on the European Payments Industry and Seizing the Opportunities. *The Capco Institute Journal of Financial Transformation*, *45*, 8–13.

Etikan, I., Musa, S. A., & Alkassim, R. S. (2016). Comparison of Convenience Sampling and Purposive Sampling. *American Journal of Theoretical and Applied Statistics*, *5*(1), 1–4. doi:10.11648/j.ajtas.20160501.11

FinTech Network. (2016). *Four Blockchain Use Cases for Banks.* FinTech Network. Retrieved from https://germanyfintech.org/wp-content/uploads/2018/01/fintech_blockchain_report_fintech_network.pdf

Fitzgerald, M., Kruschwitz, N., Bonnet, D., & Welch, M. (2013). Embracing Digital Technology: A New Strategic Imperative. *MIT Sloan Management Review*.

Folkinshteyn, D., Lennon, M. M., & Reilly, T. (2015). A Tale of Twin Tech: Bitcoin and the WWW. *Journal of Strategic and International Studies*, *X*(2), 82–90.

Frøystad, P., & Holm, J. (2015). *Blockchain: Powering the Internet of Value.* Evry. Retrieved Sept. 25, 2020, from https://www.finyear.com/attachment/637653/

Fu, D., & Fang, L. (2016). Blockchain-based trusted computing in social network. *2016 2nd IEEE International Conference on Computer and Communications (ICCC).* doi:10.1109/CompComm.2016.7924656

Fugkeaw, S. (2022). Enabling Trust and Privacy-Preserving e-KYC System Using Blockchain. *IEEE Access: Practical Innovations, Open Solutions*, *10*, 49028–49039. doi:10.1109/ACCESS.2022.3172973

Gökalp, E., Sener, U., & Eren, P. E. (2017). Development of an Assessment Model for Industry 4.0: Industry 4.0-MM. In Software Process Improvement and Capability Determination (pp. 128–142). Springer International Publishing.

Gokhale, H. (2016). *Blockchain: Opportunities And Challenges For Korean Financial Industries.* Seoul National University. Retrieved from http://hdl.handle.net/10371/129092

Goodhart, C. (2011). *The Basel Committee on Banking Supervision: a history of the early years, 1974–1997*. Cambridge University Press. doi:10.1017/CBO9780511996238

Hair, J. F., Black, W. C., Babin, B. J., & Anderson, R. E. (2010). *Multivariate Data Analysis: A Global Perspective* (7th ed.). Pearson Prentice Hall.

Hassani, H., Huang, X., & Silva, E. (2008). Banking with Blockchain-ed Big Data. *Journal of Management Analytics*, *5*(4), 256–275. doi:10.1080/23270012.2018.1528900

Hong Kong Monetary Authority. (2017). *Whitepaper 2.0 on Distributed Ledger Technology.* Retrieved 5th Aug. 2022, from https://www.hkma.gov.hk/media/eng/doc/key-functions/finanicalinfrastructure/infrastructure/20171025e1a1.pdf

Huang, S., & Tilley, S. R. (2003). Towards a documentation maturity model. *SIGDOC '03: Proceedings of the 21st annual international conference on Documentation*. doi:10.1145/944868.944888

Isa, Y. M., Sanusi, Z. M., Haniff, M. N., & Barnes, P. A. (2015). Money Laundering Risk: From the Bankers' and Regulator's Perspectives. In *7th International Conference On Financial Criminology 2015* (pp. 7-13). Procedia Economics and Finance. doi:10.1016/S2212-5671(15)01075-8

Islam, H. (2021). *Adoption of blockchain in know your customer (KYC) verification process: a thematic analysis on European banking industry* [Master's thesis]. Tallinn University of Technology.

Kapsoulis, N., Psychas, A., Palaiokrassas, G., Marinakis, A., Litke, A., & Varvarigou, T. (2020). Know Your Customer (KYC) Implementation with Smart Contracts on a Privacy-Oriented Decentralized Architecture. *Future Internet, 12*(41), 1-14.

Kawasmi, Z., Gyasi, E. A., & Dadd, D. (2020). Blockchain Adoption Model for the Global Banking Industry. *Journal of International Technology and Information Management*, *28*(4), 112–154.

Kinyua, D. (2020). KYC, Client Onboarding: Leveraging Blockchain Technology. *The Paris Conference on FinTech and Cryptofinance.* doi:10.2139/ssrn.3528323

Kionga, D. (2020, February 26). *How often should companies conduct penetration tests?* Retrieved 07 24, 2020, from https://www.cloudcape.de/en/how-often-should-companies-conduct-penetration-tests/

Kirss, K. K., & Milani, F. (2021). *Using Blockchain Technology to Redesign Know-Your-Customer Processes Within the Banking Industry. In International Conference on Business Process Management*. Springer. doi:10.1007/978-3-030-66498-5_19

Kothari, C. R. (2004). *Research Methodology: Methods and Techniques*. New Age International.

Leem, C. S., Kim, B. W., Yu, E. J., & Paek, M. H. (2008). Information technology maturity stages and enterprise benchmarking: An empirical study. *Industrial Management & Data Systems*, *108*(9), 1200–1218. doi:10.1108/02635570810914892

Leem, C. S., & Kin, I. (2004). An integrated evaluation system based on the continuous improvement model of IS performance. *Industrial Management & Data Systems*, *104*(2), 115–128. doi:10.1108/02635570410522080

Lees, M. (2016). A maturity model for Control and Automation in environmental impact. In *Australian Control Conference (AuCC)* (pp. 299-304). Australian Control Conference (AuCC). doi:10.1109/AUCC.2016.7868206

Lempogo, F., Yeboah-Boateng, E. O., & Brown-Acquaye, W. L. (2021). Big Data Analytics in Developing Economies:Harnessing Insights and Creating Value. In Digital Technology Advancements in Knowledge Management (pp. 149-166). IGI Global.

Luu, L., Chu, D., Olickel, H., Saxena, P., & Hobor, A. (2016). Making Smart Contracts Smarter. *2016 ACM SIGSAC Conference on Computer and Communications Security*, 254–269. doi:10.1145/2976749.2978309

Mattila, J. (2016). *The Blockchain Phenomenon – The Disruptive Potential of Distributed Consensus Architectures.* ETLA Working Papers, No. 38, The Research Institute of the Finnish Economy (ETLA).

Morabito, V. (2017). Blockchain Practices. In V. Morabito (Ed.), *Business Innovation Through Blockchain: The B3 Perspective* (pp. 145–166). Springer International Publishing.

Nguyen, Q. K. (2016). Blockchain - A Financial Technology for Future Sustainable Development. *2016 3rd International Conference on Green Technology and Sustainable Development (GTSD)*.

Norvill, R., Cassanges, C., Shbair, W., Hilger, J., Cullen, A., & State, R. (2020). *A Security and Privacy Focused KYC Data Sharing Platform. In 2nd ACM International Symposium on Blockchain and Secure Critical Infrastructure (BSCI '20)*. Association for Computing Machinery.

Norvill, R., Steichen, M., Shbair, W. M., & State, R. (2019). Demo: Blockchain for the Simplification and Automation of KYC Result Sharing. In *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)* (pp. 9-10). IEEE. 10.1109/BLOC.2019.8751480

Pandey, P., & Pandey, M. M. (2015). Research Methodology: Tools and Techniques. Bridge Center.

Parra-Moyano, J., & Ross, O. (2017). KYC optimization using distributed ledger technology. *Business & Information Systems Engineering*, *59*(6), 411–423. doi:10.1007/s12599-017-0504-2

Parra-Moyano, J., Thoroddsen, T., & Ross, O. (2019). Optimized and Dynamic KYC System Based on Blockchain Technology. *International Journal of Blockchains and Cryptocurrencies*, *1*(1), 85–106. doi:10.1504/IJBC.2019.101854

Patel, D., Bothra, J., & Patel, V. (2017). Blockchain Exhumed. 2017 ISEA Asia Security and Privacy (ISEASP), 1–12.

Paulk, M. C., Weber, C. V., Curtis, B., & Chrissis, M. B. (1995). *The Capability Maturity Model: Guidelines for Improving the Software Process*. Addison-Wesley.

Rockwell Automation. (2014). *The Connected Enterprise Maturity Model: How ready is your company to connect people, processes, and technologies for bigger profits?* Rockwell Automation, Inc.

Schlatt, V., Sedlmeir, J., Feulner, S., & Urbach, N. (2022). Designing a Framework for Digital KYC Processes Built on Blockchain-Based Self-Sovereign Identity. *Information & Management*, *59*(7), 103553. doi:10.1016/j.im.2021.103553

Schumacher, A., Erol, S., & Sihn, W. (2016). A Maturity Model for Assessing Industry 4.0 Readiness and Maturity of Manufacturing Enterprises. *Procedia CIRP*, *52*, 161–166. doi:10.1016/j.procir.2016.07.040

Sekaran, U. (2006). *Research Methods For Business: A Skill Building Approach* (4th ed.). John Wiley & Sons.

Singh, R., Bansal, R., & Singh, V. P. (2022). Industry 4.0: Driving the Digital Transformation in Banking Sector. In M. Niranjanamurthy, S.-L. Peng, E. Naresh, S. R. Jayasimha, & V. E. Balas (Eds.), *Advances in Industry 4.0: Concepts and Applications* (pp. 51–64). De Gruyter. doi:10.1515/9783110725490-003

Sinha, P., & Kaul, A. (2018). Decentralized KYC System. *International Research Journal of Engineering and Technology*, *5*(8), 1206–1211.

Smart Africa. (2021). *Blockchain in Africa: Opportunities and Challenges for the Next Decade*. Smart Africa.

Srinivasan, N. (2007). Policy Issues and Role of Banking System in Financial Inclusion. *Economic and Political Weekly*, *42*(30), 3091–3093.

Sullivan, K. (2015). Know Your Customer and Customer Identification Program. In K. Sullivan (Ed.), *Anti–Money Laundering in a Nutshell* (pp. 69–100). CA Press. doi:10.1007/978-1-4302-6161-2_5

Sun, N., Zhang, Y., & Liu, Y. (2022). A Privacy-Preserving KYC-Compliant Identity Scheme for Accounts on All Public Blockchains. *Sustainability*, *14*(21), 14584. doi:10.3390/su142114584

Swan, M. (2015). Blockchain: Blueprint for a New Economy. O'Reilly Media, Inc.

Tongco, M. D. (2007). Purposive sampling as a tool for informant selection. *Ethnobotany Research and Applications*, *5*, 147–158. doi:10.17348/era.5.0.147-158

Üçoğlu, D. (2022). Blockchain Technology and Future Banking: Opportunities and Challenges. In Applications, Challenges, and Opportunities of Blockchain Technology in Banking and Insurance (p. 26). IGI Global. doi:10.4018/978-1-6684-4133-6.ch003

UNCTAD. (2021). *Technology and innovation report 2021: Catching Technological Waves - Innovation with equity.* United Nations. Retrieved from https://unctad.org/system/files/official-document/tir2020_en.pdf

Ustundag, A., & Cevikcan, E. (2017). *Industry 4.0: Managing The Digital Transformation*. Springer.

Wang, H., Chen, K., & Xu, D. (2016). A maturity model for blockchain adoption. *Financial Innovation*, *2*(1), 5. doi:10.1186/s40854-016-0031-z

Wright, A., & De Filippi, P. (2015). Decentralized Blockchain Technology and the Rise of Lex Cryptographia. SSRN *Electronic Journal*, 58. 10.2139/ssrn.2580664

Wüst, K., & Gervais, A. (2018). Do you Need a Blockchain? *2018 Crypto Valley Conference on Blockchain Technology (CVCBT)*. doi:10.1109/CVCBT.2018.00011

Xu, X., Pautasso, C., Zhu, L., Gramoli, V., Ponomarev, A., Tran, A. B., & Chen, S. (2016). The Blockchain as a Software Connector. In *2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA)* (pp. 182–191). IEEE.

Yadav, A. K., & Bajpai, R. K. (2020). KYC Optimization using Blockchain Smart Contract Technology. *International Journal of Innovative Research in Applied Sciences and Engineering*, *4*(3), 669–674. doi:10.29027/IJIRASE.v4.i3.2020.669-674

Yang, Y., Shi, Y., & Wang, T. (2022). Blockchain Technology Application Maturity Assessment Model for Digital Government Public Service Projects. *International Journal of Crowd Science*, *6*(4), 184–194. doi:10.26599/IJCS.2022.9100025

Yu, L., Tsai, W.-T., Li, G., Yao, Y., Hu, C., & Deng, E. (2017). Smart-Contract Execution with Concurrent Block Building. *2017 IEEE Symposium on Service-Oriented System Engineering (SOSE)*, 160-167. doi:10.1109/SOSE.2017.33

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *2017 IEEE International Congress on Big Data (BigData Congress)*.

Zhu, Y., & Chen, Z. (2017). RealID: Building A Secure Anonymous Yet Transparent Immutable ID Service. *2017 IEEE 3rd International Conference on Big Data Security on Cloud (BigDataSecurity), IEEE International Conference on High Performance and Smart Computing, (HPSC) and IEEE International Conference on Intelligent Data and Security (IDS).* 10.1109/BigDataSecurity.2017.44

Forgor Lempogo is a Senior Lecturer and currently the Head of the Department of Mobile and Pervasive Computing, Ghana Communication Technology University, Accra Ghana. He obtained his MSc. in Information Systems and Technology as well as his PhD in Automation and Control from the Tver State Technical University in the Russian Federation. His main research interest is in the area of control systems and emerging computing technologies such as Big Data, IoT and Blockchain.

William Leslie Brown-Acquaye is a senior Lecturer at the Information Technology department of the Ghana Communication Technology University in Accra, Ghana. Additionally, he is the head of the above department. He has a PhD in Automation and control from the Tambov state technical university in the Russian federation. His main research interest is in the area of control systems, Pervasive computing and Human-Robot Interaction.

Millicent Agangiba is a lecturer at the Department of Computer Science and Engineering in the University of Mines and Technology, Tarkwa. She obtained her PhD in Information Systems from the University of Cape Town and MSc from Tver State Technical University in Russia. She is a senior member of the Institute of Electrical and Electronics Engineering (IEEE), Association of Information Systems (AIS), Association of Computing Machines (ACM), Internet Society Chapter (ISOC), Ghana, International Association of Engineers (IAENG) and Women in Science without Borders (WISWB). Her research interest is in Human-Computer Interaction, Digital Accessibility for Persons with Disabilities, Information and Communication Technologies for Development.

Daniel Selassie Kwasi Twumasi is currently a Senior Software Engineer at IT Consortium based in Accra, Ghana. He has an MSc. Management information Systems from Ghana Communication Technology University. His research interests include software development approaches for distributed ledger and Big Data.