

ADDIS ABABA UNIVERSITY

SCHOOL OF COMMERCE

MASTERS OF BUSINESS INFORMATION SYSTEM (EXTENSION PROGRAM)

BLOCKCHAIN FRAMEWORK TO STRENGTHEN KNOWS YOUR CUSTOMER (KYC) PROCESSES AND DATA TRANSPARENCY (IN CASE OF COOPERATIVE BANK OF OROMIA).

By: Eyob Tesfaye

ID - GSE/7305/16

Section – E1BIS1

Submitted to: -Kuribachew.G (PHD)

Submission date: - June 14, 2026

Declaration

I hereby declare that the thesis titled "BLOCKCHAIN **FRAMEWORK TO STRENGTH KNOW YOUR CUSTOMER (KYC) PROCESSES AND DATA TRANSPARENCY (IN CASE OF COOPERATIVE BANK OF OROMIA)**" Submitted to Addis Ababa University for the MBA is my only personal original work and have not been submitted for any other MBA or examination. All the information and ideas derived from other sources have been duly acknowledged in the text.

Eyob Tesfaye

ID-GSE/7305/16

Acknowledgment

I did not expect that carrying out this research was going to prove challenging, but here we are; I find myself writing this acknowledgment at 4 AM on the final day.

First and foremost, I would like to extend my deep appreciation to the One Almighty God. My foremost priority is my appreciation for my family members for their continuous support and motivation. I am sincerely grateful for the encouragement that I received from my supervisor, Dr.Kuribachew, for her motivation and prompt feedback that motivated me on numerous occasions. Special thanks are extended to Sifan Gudeta for offering meals during the research period. There cannot be enough appreciation for the peer assistance I got from those who felt like family because I would have enjoyed my college days more if it were possible. I would like to thank my workmates for offering some points of view that made the research more appealing. Lastly, I appreciate Usman Mohammed, who helped me throughout this enormous undertaking.

List of figures

Figure 1: Current KYC system and cost status 19
Figure 2: Blockchain approaches for KYC.....21
Figure 3: The Steps and Process of Transaction in the Blockchain.....22
Figure 4: Blockchain Adoption Supporting Factors 31
Figure 5: Technology Acceptance Model.....33
Figure 6: Our applied DSR process.....38
Figure 7: UML Diagram (completely New Onboarding)….....47
Figure 8: UML Diagram (Fast Onboarding)… 51

List of tables

Table 1: The test result of blockchain based KYC prototypes by KPMG 34
Table 2: Overview over the interviewed staffs 41
Table 3: Summary of the Findings 49

List of Abbreviations and Terms

AML	Anti-Money Laundering
IDASR	Identification, Authentication and trust Services Regulations
API	Application programming interface
CDD	Customer Due Diligence
CFT	Combating the Financing of terrorism
DLT	Distributed Ledger Technology
EDD	Enhanced Due Diligence
Fintech	Financial Technology
ETAM	Extended Technology Acceptance Model
EIDASR	electronic Identification, Authentication and trust Services Regulations
ETAM	Extension of Technological Acceptation Model
EU	European Union
F2F	Face To Face
FATF	Financial Action Task Force
FI	Financial Institution
FSA	Financial Supervisory Authority
FSB	Financial Stability Board
VC	Verified credential
KYC	Know your customer
VP	Verified prototype
SSI	Self-Sovereign identity
ODD	Ongoing Due Diligence
RegTech	Regulatory Technology
CRM	Customer Relation Manager
TP	Transaction Per Second
DID	Decentralized Identity

Abstract

The evolution of the KYC process has gone from a simple process to a more thorough one regulated by the regulatory authority of each country. The paper-based manual KYC process is neither cost-efficient,not fast nor customer-centered. In many countries, at least to some degree, the majority of financial institutions have to pay an estimated amount of approximately $550 million for conducting the process of KYC regulation. With the introduction of new laws and regulations concerning the process of KYC compliance in most parts of the world, there might be the chance that the cost for compliance will go up. The aim of this paper is to consider the case of Financial Institution and Cooperative Bank of Oromia through expert interviews and relevant literature analysis. As a result of the conducted analysis of the case study, factors like communication, source of information, validity of documentation, policy conformity, lengthy process, customer dissatisfaction, increased workload on the employees' side, inaccuracy, lengthy document searching process, lack of automation were identified as the main problems that arise as a result of the current process of KYC and hence render it outdated and unsuitable for business purposes. It becomes apparent that implementing blockchain technology in order to conduct KYC process would resolve all the above-mentioned problems. Some of the potential obstacles related to the implementation of blockchain could be legal risks, resistance to change, lack of trust, educating the customers, employees' training, redundancies, and energy consumption. Overcoming methods for these obstacles have been discussed in the results chapter. A number of suggestions with regard to the adoption of blockchain technology have been made including KYC automation, common KYC standards, conducting pilot projects, and linkages within the bank.

Contents

Declaration.....**I**

Acknowledgements.....**II**

List of Figures .....**III**

List of Tables.....**IV**

ListofAcronyms ..... **V**

Abstract….....**VI**

CHAPTER ONE 11

INTRODUCTION 11

1.1 Background of Study..... 11

1.2 Motivation.....12

1.3 Problem Statement.....13

1.4 Research Questions.....13

1.5 Research Objectives.....14

1.5.1 General Objective 14

1.5.2 Specific Objectives 14

1.6 Research Gap 15

1.7 Scope of the Study 15

1.8 Limitation of the Study..... 15

1.9 Organization of the study 16

CHAPTER TWO..... 17

LITERATUREREVIEW..... 17

2.1 Introduction.....17

2.2 Traditional method of KYCprocess.....19

2.2.1 Current manual structure of KYCprocess.....19

2.2.2 Challenges in existing KYC methods.....20

2.3 Blockchain Technology……..20

2.3.1 Core Components of Blockchain and how it works..... 21

2.3.2 Types and Classification of Blockchain..... 25

2.3.3 Characteristics of blockchain.....25

2.3.4 Challenges in Blockchain 27

2.4 Ethical issues in Blockchain 27

2.5 Blockchain Development in Financial Industry 28

2.6 Suitability of Blockchain in automating KYC 28

2.7 Theoretical Framework 29

2.8 Adoption issues Of Blockchain in KYC in Banking Industry.....30

2.8.1 Interoperability in Adoption of Blockchain 32

2.8.2 Issues related with Blockchain Adoption models for Theoretical Framework..... 32

2.9 Blockchain based KYC cases..... 33

2.10 Summary.....35

CHAPTER THREE..... 36

METHODOLOGY 36

3.1 Research Design..... 36

3.2 Research Approach 37

3.3 Research Analysis Approach..... 38

CHAPTER FOUR…..... 40

EVALUATION AND RESULTS 40

Introduction..... 40

4.1 Evaluation of Blockchain framework 40

4.2 Blockchain based KYC process results 41

4.3 Challenges of Implementation…….48

4.4 Findings 49

CHAPTER FIVE 53

CONCLUSION AND RECOMMENDATION 53

5.1 Introduction 53

5.2 Recommendations 53

5.2.1 Automation 53

5.3 Feasibility Study 54

5.3.1 Common Standard of KYC 54

5.4 Limitation…´´ 55

5.5 Future Reserve 55

References 57

Appendix 60

.

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

KYC (Know Your Customer) is the main procedure for the prevention of financial crimes, where it is mandatory to provide the name of the client and also an anti-money laundering procedure that is compulsory to report any suspicious transaction. There are problems like high operational cost, redundancy, and inefficiency caused by duplicate verification of client identification in different organizations. Existing systems are centralized and hence do not facilitate secure data sharing and compliance. This results in delayed compliance, fines, and poor client feedback as a result of prolonged onboarding process. Most importantly, legacy systems lack real-time monitoring capabilities that make it difficult to detect financial frauds in time. As manual KYC operations are prone to mistakes and frauds, there is a need for an effective and secure solution to this challenge. Blockchain technology presents a disruptive approach through provision of a decentralized, transparent, and secure system that is cryptographically secured and facilitates identity verification and data sharing. Through decentralization, it ensures efficiency in terms of minimal redundancy and reduced operational costs while maintaining high level of security in KYC operations. Nevertheless, there is also a problem with scaling, regulations, and integration with current systems for the technology to be adopted. In this paper, I will explore how blockchain technology can help achieve compliance by performing a business analysis approach and seeing how it impacts the financial institutions. “Blockchain technology has been regarded as a disruptive core technology” (Xu et al., 2019). In 2008, Satoshi Nakamoto, an unknown entity that introduced Bitcoin, demonstrated the potentiality of using the technology of blockchain, which is a decentralized ledger operating under a peer-to-peer architecture system, in dealing with issues concerning transaction processing and spending double time (Casino et al., 2019). Transactions in Bitcoin are stored in a fixed-size data structure known as block, whereby the blocks all have identical timestamps. Nodes within the network usually link the blocks based on chronological order in such a way that all blocks contain hash value of their previous blocks to form chains of blocks (Crosby et al., 2016). Blockchain technology does not involve an executable program; it involves a repository of transactions. A smart contract is the program required for implementing the KYC process. The method used in this research paper is a case study. There have been numerous case studies and design science research previously conducted. The key and main objective of the study is to analyze the benefits, drawbacks, and adoption strategy for using

Blockchain technology in the KYC process. The most important factor that will affect the interest of financial institutions in adopting such technology would be whether blockchain can help them reduce compliance and processing costs.

1.2 Motivation

Knowing Your Customer (KYC) is an approach used by FI, telecoms, and other businesses to authenticate the identity of their customers. KYC assists in preventing any act of identity fraud, money laundering, and various kinds of financial criminal activities. But the traditional KYC process takes time, costs more, and has room for human error, resulting in delays in establishing the account and causing inconveniences to customers. Moreover, traditional KYC requires the sharing of private customer data, thus raising privacy issues for both the clients and Cooperative Bank of Oromia. To address these challenges, Blockchain technology used in KYC processes is considered another method that can replace traditional KYC processes. The KYC process relies on electronic verification of customers' identities and therefore eliminates the need for paperwork. Nonetheless, there are issues surrounding privacy and security, which are some of the challenges faced by the KYC process.

Additionally Cooperative Bank of Oromia has announced that it has started working together with InFTF to launch a foreign remittance service based on blockchain technology in Ethiopia and the development of blockchain technology can be seen as one of the solutions for the problems regarding privacy and security in KYC systems. Blockchain is a decentralized technology that ensures the integrity of data stored in it. The KYC system designed in this paper is intended to provide a solution to the problems related to traditional KYC techniques in cooperative Bank of Oromia. The implementation of the blockchain technology will allow for enhancing the security and privacy of customer data storage. With the use of blockchain, it will be possible to provide the transparency and security of the storage of customer data and minimize the possibility of their being accessed or modified without the customer's consent. Moreover, by using the protocols of zero-knowledge proof and smart contracts, it will be possible to enhance the efficiency of KYC system design.

1.3 Statement of the Problem

In the present financial situation, KYC procedures play a vital role in ensuring that financial institutions comply with regulations, prevent fraud, and guarantee data security. Nevertheless, the conventional KYC procedures used by most financial organizations encounter various difficulties, such as inefficient manual verification procedures, data silos, lack of transparency, and poor communication between participants.

Although blockchain technology have recognition due to its capabilities to provide integrity, transparency, and enhanced data protection, little attention has been paid to the adoption of blockchain technology in the KYC process of private banks in Ethiopia. The Cooperative Bank of Oromia is one of the leading private banks in the country that faces various problems in the regulatory and operational processes. Nonetheless, little research has examined the applicability of blockchain technology to the KYC process.

Inadequate use of blockchain in banking industry is one of the problems in this study and its application in private banks. There is a lack of a detailed assessment on the role of blockchain in automating the KYC process.

1.4 Research Question

The research question that will have been answered by the research in order to understand and view the perspective of blockchain framework technology's role in financial institutions and in what ways can the blockchain technology be employed in such a way that will enhance the KYC process and improve data transparency within the financial institutions and the Cooperative Bank of Oromia.

- How can a blockchain framework be designed to strengthen KYC processes and enhance data transparency in financial institutions??
- In which way can blockchain's immutability feature enhance the integrity and reliability of KYC data Management??
- How can a blockchain framework be integrated with existing Core Banking Systems at the Cooperative Bank of Oromia to reduce KYC process times, eliminate data redundancies, and improve regulatory transparency**?**

- How can financial institutions inform the iterative design and improvement of the blockchain-based KYC framework??

The mentioned research question above is an open one because it calls for a complete investigation into the possibilities, challenges, and implementation process of the blockchain framework in the KYC process of FI and the Cooperative Bank of Oromia.

1.5 Research Objectives

1.5.1 General Objective

To design a blockchain framework that enhances the KYC process while providing data transparency and integrity within financial institutions.

1.5.2 Specific Objective

- To design a framework of the blockchain platform that encompasses identification, data transfer, and data confidentiality.
- To examine the possibilities presented by blockchain technology in mitigating the shortcoming in the KYC process such as data integrity, efficiency, traceability, and security.
- To determine the viability of adopting blockchain in the KYC process of the Cooperative Bank of Oromia based on a number of factors.
- To provide recommendations for the Cooperative Bank of Oromia and financial institutions on how to effectively adopt blockchain technology to strengthen its KYC processes and data transparency.

The stated objectives are designed to guide the research and ensure that the study contributes meaningful insights into the design of blockchain in financial institutions, particularly in the private

banking sector in Ethiopia.

1.6 Research Gap

As the importance of digitization in the field of finance becomes increasingly crucial, every financial institution does not use blockchain technology. For instance, while it is known that Cooperative Bank of Oromia has become successful in enhancing their push on the 'Know Your Customer' (KYC) practice and data gathering, little empirical research has been done about whether the use or non-use of blockchain technology impacts the security, traceability, and efficiency of the system. Even though the advantages of blockchain in contributing to financial systems have been thoroughly documented in the existing literature, very few pieces of research have discussed its impact when applied to certain cases like the KYC process in the case of cooperative Bank of Oromia. This research gap presents an opportunity to contribute to the growing part of knowledge on the design of blockchain in financial institutions, particularly in developing economies, and to provide practical insights for the Cooperative Bank of Oromia in enhancing its KYC processes and data transparency.

1.7 Scope of the Study

The study is limited to the structure of KYC processes within financial institutions and designing a blockchain framework in financial institution and Cooperative Bank of Oromia. The main focus will be on the design and artifacts of the solution including how identity is processed, verified, sharing practices, and auditing capabilities to comply with regulations.

1.8 Limitations of the Study

This suggested blockchain framework has some constraints as well. The adoption of blockchain architecture needs heavy computing capacity and that can limit the scalability of the artifacts. The adoption of zero knowledge proof of algorithms also needs computing capacity and this can affect the overall performance of the system. In terms of the scope, the research is limited to the knowledge about customer and data transparency only.

1.9 Organization of the Study

The study is organized into the multi sections to ensure clarity, coherence, and logical flow of ideas. Each part is designed to build upon the previous one and steps, leading to a comprehensive understanding of the design blockchain technology framework in strengthening the KYC process and data transparency in Cooperative Bank of Oromia and financial institutions.

CHAPTER TWO
LITERATURE REVIEW

2.1 INRODUCTION

This chapter represents a critical literature review of blockchain technology, the concept of KYC, data transparency and Design Science Research. The aim of the review is to provide a theoretical and empirical justification for the research and define the gaps that would explain the need for developing a blockchain based artifact. This chapter combines the ideas from the financial compliance regulation, transparency theory, information asymmetry theory, distributed ledger technologies and design science approach. The first step of identification will be different due to the variation in regulatory policies and regulations in different states and policies specific for each bank. Nevertheless, there is some general procedure for performing the KYC procedures (see Figure 1 below). At first, it is necessary to collect all necessary data regarding regular clients in order to identify them. Typically, the government-issued documents, including ID cards, licenses, or passports are required for this purpose. Other types of documents could be used for identification; these documents can be issued by the banks themselves, phone and utility bills could be used too (Mugarura, 2014). Once the client has been identified and personal data checked, the bank should verify if the client poses any danger to it. This means that it is necessary to check him against the list of terrorist, criminal, and politically exposed persons (Arasa and Ottichilo, 2015).

Identity verification and constant monitoring of activities will have to be undertaken separately for each client, with each client having to undertake this procedure anew while setting up accounts with a different bank. This makes the KYC process extremely lengthy and tedious for both the customer and the bank and contributes to poor experiences among the former and low account openings by the latter. Financial institutions should be capable of making necessary adjustments in order not to lose out on their clientele. In addition, there will be more room for market efficiency because of lower switching costs, due to which there will also be greater competition in the industry. Lastly, high cost of this process coupled with non-automation of some tasks increases the expenses of the institution. The main motivating factor behind the KYC regulatory measures by the financial institutions is that they need to prevent money laundering via the institution. In case of non-compliance, financial institutions may face high cost due to huge fines being imposed upon them (Moyano and Ross, 2017). One of the most important aspects of KYC process by those

financial institutions can afford. Nevertheless, there are financial institutions where KYC becomes a source of an advantage because it helps them know what their customers want, customize their services, and even develop better relationships with customers to get bigger profit from them. Financial institutions should make necessary adjustments to not only retain but gain their customers and opportunities. Market efficiency will improve due to increased competition, which will be realized by lowering switching cost. It is necessary to mention that both high level of labor intensity and non-automation of some procedures increase the cost of the KYC procedure for financial institutions. That way, one of the most important reasons behind attempts to implement regulatory KYC procedures is preventing money laundering through financial institutions. In this case, violation of regulatory procedures will raise the cost of KYC processes in financial institutions because of the imposition of serious fines for the institutions (Moyano and Ross, 2017). On the other hand, while dealing with KYC processes, financial institutions have one of the main goals to avoid being fined and getting damaged in terms of reputation, ideally, at lower costs of ownership. However, there are financial institutions where KYC processes become a source of advantage because it allows the institutions to learn customers and produce custom products for customers, as well as to develop better relationships with customers to get more profit.

Hence, the first step that has to be taken in order to increase efficiency is to implement identity management systems in an efficient manner, and this is essential because identity management systems have to handle sensitive data and therefore, they need to be secured properly. In particular, one of the reasons why centralization should not be seen as the solution here is that centralized database storing user data can serve as an attractive target for attacks since they provide access to large amounts of sensitive data. Hence, it becomes difficult to ensure proper security (Sedlmeir et al., 2021b). This concern regarding the security of centralized systems where competitive data is not at stake occurs frequently elsewhere as well.

2.2. Traditional Method of KYC Process

When it comes to such processes like account openings for clients, it is important for the bank or FI to have verifiable information about the customer that includes a passport prior to initiating KYC procedures lawfully. Next, since banks will become familiar with their customers through the data of transactions, they can do more to gather more information from the clients through payment data, insurance data, and investment data. According to (Barberis, 2018) touches are one of the most

critical ways through which banks can get to know their customers. Although the passport may give information on the identification of the individual, transaction data will give insight into which they are, including their creditworthiness.

2.2.1 Current manual structure of KYC process

The KYC protocol includes the exchange of documentation between the client and the FI on condition that the client is willing to cooperate. The protocol requires the collection of basic identity documents, which are gathered by the clients in order to check out if there are any cases of illegal and political activities undertaken by the persons involved. The procedures can only be undertaken if the client is willing to travel along with the FI in the new program. The terms and conditions within the contract should be agreed upon chronologically between the client and the financial institutions. After the KYC process starts, all the necessary documentation by the client needs to be submitted to the institutions. Once the analysis of the documents has been done, the financial institutions will prepare a document for the FI, which would act as the confirmation that the KYC process of the individual has been approved. It should be noted that if the KYC process of the individual has been validated or rejected at the center. It would simply mean that the KYC process was undertaken successfully according to the set procedures. On the other hand, if the customer wants to have a new contract with another financial institution, the same procedure will be adopted. The model makes it inefficient and costly each time the KYC process takes place and each time the customer decides to engage with another financial institution. Figure 1 below is an illustration showing an example of how a client engages in three different financial institutions at the same time and thus incurs extra costs for each KYC service.

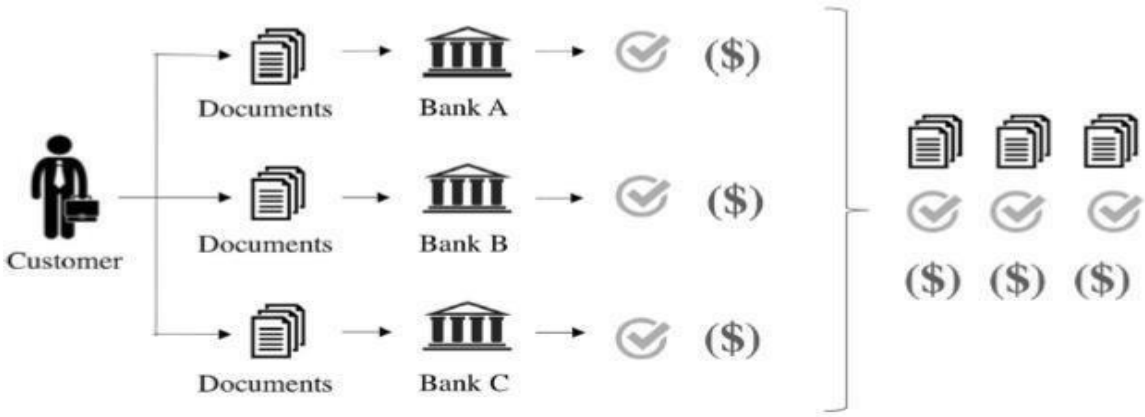


Figure 1: current KYC system and cost status

2.2.2 Challenges in Existing KYC Methods

The current and existing onboarding process methodology is quite expensive and time-consuming and requires meeting the regulatory requirements of CDD, which poses a significant problem for FIs, technology companies providing financial services, and FinTech companies. CDD information will be relevant when it is (1) accurate, (2) provided by a credible source, and (3) up-to-date (Buckley & Zetzsche, 2016). Other backups and challenges include:

- **Time consuming:** financial institutions would have intensively, thereby requiring the banks to invest more time and money into the crucial KYC procedure of their clients' information, resulting in expensive and difficult procedures for their customers.
- **Inefficient:** The process is especially unproductive in the case of Luxembourg, given its role as a cross-border international center.
- **Inconvenient, Unreliable, and Expensive:** The results are most useful outputs from the data analysis from the regulatory agencies and other firms when used in large amounts of data are those that contribute to business integrity. In regard to this output, current systems have become expensive, cumbersome, and impractical in addition to being unable to identify fraudulent acts in the financial system (Buckley & Stanley, 2016).

2.3 Blockchain Technology

Blockchain technology has gained immense popularity ever since its conception and release to the globe. These were conceived by (Satoshi Nakamoto in 2008) as a technical finding for the technology behind Bitcoin. This marked the beginning of a new era in the financial industry in the form of crypto- currencies. Blockchain is basically a distributed, immutable, cryptographically linked and continuously growing list of records where consensus among trustless entities can be achieved without involving any intermediaries. The continuously growing list of records, otherwise referred to as ledger, is distributed across the nodes of a peer-to-peer network. The ledger is a series of blocks that are linked to each other following some rules and thus the name Blockchain was derived. These blocks are generated at a fixed time interval in a decentralized fashion according to certain rules referred to as consensus algorithm. Blockchain and DLT are similar terms but have a significant difference between them. Blockchain is a type of ledger where data is stored in a specific form, while other types of ledgers are capable of storing data in another format. The concept of DLT may be realized in case of decentralization of the ledger on the network. With the aid of Blockchain technology, the smart contracts offer immutable, trustless, and transparent distributed computing and

execution of code and are used extensively in different sectors, like KYC. Thanks to smart contracts, the application logic can be saved without being interfered with because of the tamper-proof quality of blockchain technology. However, a major drawback of the blockchain technology is the fact that its transparency allows every user of the network to access it.

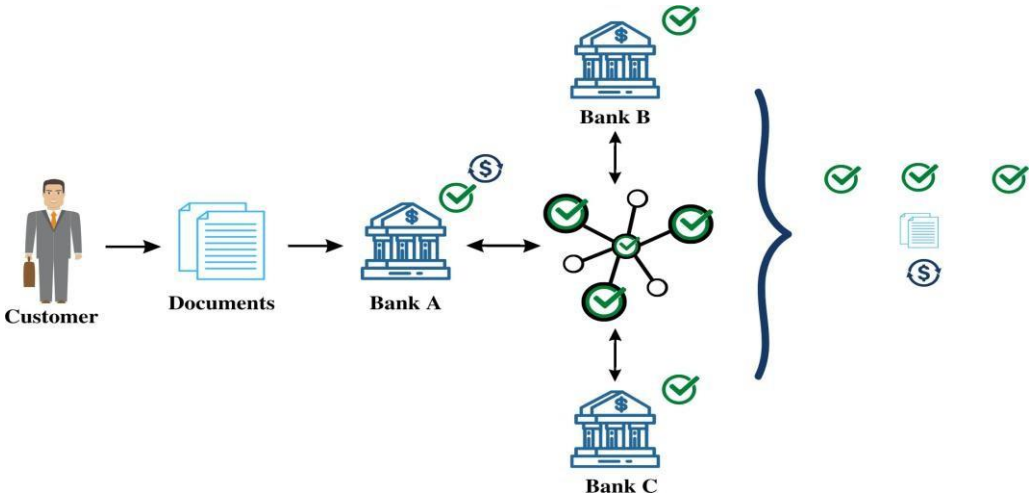


Figure 2: Blockchain Approaches for KYC

2.3.1 Core Components of blockchain and How It Works

This topic directed to discuss a deeper explanation of each of these elements and their roles is needed in order to make understanding of the whole process possible. Prior to describing the process itself, an introductory presentation is provided first. The diagram below shows some important processes starting from the creation of digital signatures. Digital signatures are generated using a signature generator, which is cryptography and data encoding. This involves the creation of cryptographic keys, such as private and public keys, and a number of rules (Geldenhuys & Hoffman, 2012). The message is encrypted using the private key before sending the message through the network. In line with the network consensus rule, when the transaction is executed, it can be verified by the nodes. Subsequently, the transaction is compiled into a block comprising only the verified transactions. After that a certain period of time elapses, the rest of the procedure is explained in other sections. In line with the network consensus rule, when the transaction is executed, it can be verified by the nodes. Subsequently, the transaction is compiled into a block comprising only the verified transactions.

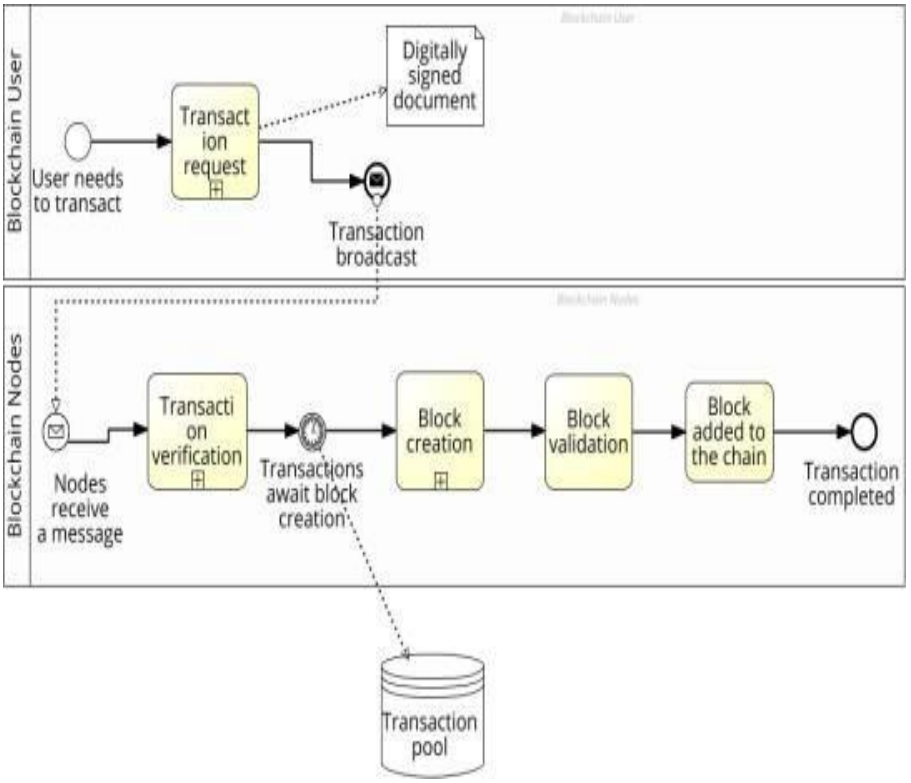


Figure 3: The steps and process of transaction in the blockchain.

Transaction Request

A transaction is referred to as any communication that is interfered into the distributed database. It may be either of the two, a message from the program or something that stimulates the program. Furthermore, the delivery may contain unencrypted data or a connection to the encrypted data. In the above figure, a collapsed sub-process is utilized in order to leave out unnecessary data which is not needed in the process diagram. The hashing, encryption and the key distribution are some of the things that are fixed standard in this stage before the distribution in the network. The next step in the chain is followed by other block holders as stated (Murphy, 2016) (Ismail et al., 2019).

Nodes

The component of the blockchain includes the use of a computerized system not owned by anyone in terms of storing events and confirming transactions referred to as node. The process involves each node having an identical copy of transactions that are included in their ledger upon reaching consensus from the other node in the network. In cases where the node consistently provides the other nodes with updates, the ledgers maintained by the node are correct as at (Alammary et al., 2019).

Transaction verification

The blockchain uses the concepts of cryptography and digital signatures to validate the transaction. The request process uses the private key to sign transactions due to the presence of both public and private keys by the user. In this case, the user's private key is kept secret and used for signing the transactions during encryption. Nevertheless, while the information is still encrypted, it is sent to the network. Several collapsed sub-processes are included in Figure 3 due to a number of peer-to-peer processes which validate the transaction through confirmation of the recipient requesting the transaction and also through the use of a public transaction key. As seen in the steps, the authentication process confirms that the information was not manipulated in any way (Zheng et al., 2017). After successful authentication and verification of the transaction, the transaction is valid and stored in the pool.

Block

Blockchain technology involves a block header and a block body, which records the transactions within the block (Yaga et al. (2018). In the header of every block there is information regarding the block, including a timeline of the transactions' times, hash of the block data, hash of the previous block header, and block size. A block operates within its own network and abides by the network's laws. Before entering the blockchain system, it checks whether the transactions' times are consistent and in their correct order. Through the reference process, each block increases the authenticity of the previous block, and hence, the whole blockchain. This technical step is immutable because it is not possible to alter it (Manav Gupta, 2017).

Chaining of the blocks

Once the blocks have been created, a transaction gets added to the block and then the decision taken by the nodes becomes that of validating the said transaction. Transaction can never get modified when there is any modification in the blockchain and it occurs very often, according to (Greg Walker, 2015). Information about the event of "completed transactions" which has occurred in the header of each subsequent block in the format of hash value links the blocks. New block continues making network by using the hash value of the prior block. Modifying any block alters the hash value of the whole network of the blocks as well as the particular block and it would never occur without

notifying all the nodes of the block network.

Hash Technique

These are a unique tag of every data in the blocks and an essential component of blockchain technology that is applied in various applications. These hashes are similar to human fingerprints; they are unique in nature. Hashing is a process that enables quick conversion of any data fed into the system into hashes by means of mathematical computations (Yaga et al., 2018). Any identical input will generate identical output, ensuring the integrity of the data; however, any change in the input generates a new hash. The output does not reveal anything about the input data. Hashes on the distributed ledger indicate the existence of the record, but only private/public key cryptography were allow one to access the content of the file (European Union, 2019).

Access to the Network

Accesses to the network are necessary for all those who want to utilize some kind of service in the network, either privately or publicly. Software applications such as desktop apps, mobile apps, and digital wallets can act as the channel connecting clients and the blockchain. In a blockchain cloud wallet, clients have the ability to safely keep their private key, public key, and address, as well as send and receive their digital currency. This software application can be installed and stored on the device or even accessed through a link address (Grech & Camilleri, 2017).

2.3.2 Types and classification of Blockchain

The types of blockchain have been identified by Fernández-Caramés & Fraga-Lamas (2018) based on the basis of data management, data usage, and user participation. The three main categories as identified by Li et al., (2019) are: Public blockchains, Private blockchains, and Consortium blockchains.

- **Permission less Public Networks:** Here is traditional blockchain network, which is completely decentralized and all the information contained in the blockchain is accessible to all the nodes within the network. The usage of such information is unlimited in all aspects. The Proof of Work algorithm is the most popular algorithm implemented on the network to achieve network security. Creation of fake blocks is prevented by the complexity of calculations involved.
- **Consortium Networks (Public & Permissioned):** As indicated by Li et al. (2019) define the consortium blockchain as one that depends on a shared network where just a few nodes are permitted to participate. They can assist with the validation process to ensure network security. Data availability is restricted.
- **Private Networks:** A limited number of individuals have the capacity to access, read, write, and audit the blockchain as it is a closed network. The verification process takes place actively and costs less compared to the use of the public network. Nevertheless, the decentralization feature of blockchain faces a threat.

2.3.3 Characteristics of Blockchain

Decentralization

Regardless of the framework used, it is important to ensure that KYC validity is established. In the case of a centralized framework, the regulator will be the third party, and he or she will be charged with the responsibility of verifying all the process or verifications, and this will entail additional costs associated with regulation and intermediation. As opposed to the technology of blockchain, the technology operates as of P2P approach whereby data in each node of the network is traced without any third-party intervention. Generally the experts agreed that blockchain technology's decentralized structure and process is a major contribution in case of ensuring and improving the data regulations in the consensus algorithm of blockchain (Yaga

etal. 2019).Neither the third party nor out of party involvement, each party in the blockchain technology may access the database and view the transaction history without any kind of involvement by the third party like regulators (Tapscott and Tapscott, 2017). The biggest advantage of the chain is the replication of the distributed network. For an abuser to go unnoticed, he has to change all copies of the blockchain simultaneously. In addition, distributed ledger technology will help in capturing all real-time transactions that limit the system from any fraudulent acts (Rennock et al., 2018). The effective management of Blockchain and its processes in relation to decentralized networks can be linked to the conditions of limitations (Pereira et al., 2019).

Tamper proof

The parties involved cannot change the record once the conditions of the transaction are set. When a condition arises whereby anything like mistake or decision needs to be reversed, then another transaction should occur in such a manner that both the transactions are known to everyone involved. Any modification of transaction will always leave its mark (Manav Gupta, 2017).

Irreversible and Immutable

Invariability indicates the idea of immutability. The process created through blockchain technology cannot be changed in practice since it is spread across the nodes located at different locations. Its usual proof of manipulation makes it immutable. An attempt by another user to manipulate the data in one node will be seen as an attack or an act and he will stop immediately (Grech & Camilleri, 2017).

Transparency

All participants with Internet connectivity will have access to the public blockchain and will be able to get access to the booklet and edit it according to the existing valuable system. From this point, there will be no transaction on participants that will be concealed or vague, and hence this can be considered reliable. Nonetheless, it should be noted that only default participants can view messages in the private blockchain (European Commission, 2019). According to Murphy et al., (2016), the degree of openness that must be achieved before utilizing this technology may become the criterion for selecting a blockchain for legal purposes.

System Security

Privacy, integrity, and accessibility in general are what constitute information system security. Privacy involves protecting most responsive information from any unauthorized access. The integrity of information ensured by the inability of any unauthorized person to make changes to the data, and the opportunity for such individuals to explain the changes will be that the data will be accessed only when needed. Such a technological advancement will allow for the protection of data privacy through e-signatures and makes sure that the records will not be modified once they are stored on the chain. Blockchain technology involves distribution of data across many nodes; therefore, attacking one node will not affect the availability of the data.

2.3.4 Challenges in Blockchain

Despite the great prospects offered by the blockchain technology, there are many problems that will impede its implementation. Blockchain technology involves the creation of a distributed ledger wherein the information regarding relations among people is stored, and new data can be added. Therefore, transparency and decentralization play an important role because such qualities lead to many disadvantages, which affect not only the chain but also the activities of users in many ways (Drescher, 2017). In spite of the security, scalability, and latency being the most significant challenges associated with the technology, banks attempt to solve the problem.

2.4 Ethical Issues in Blockchain

Furthermore, the application of blockchain technology may provide consumers with the possibility to make use of immutability option in case of keeping their data permanently. At the same time, the aspect of data privacy may become a possible risk factor for some companies (Till et al., 2017). The problem with the implementation of confidentiality in case of blockchain technology lies in the availability of information for everyone connected within the system (Staples et al., 2017). While transparency is needed to confirm ownership of the user and avoid double spending, confidentiality is required by the users themselves. As mentioned by Feng et al. (2018), the transactions in the blockchain will involve the addresses of the parties, the hash values of the transactions, timestamps and digital signatures of the senders, which make it possible for data miners to monitor transaction flows and identify user information. Since blockchain is distributed, it has no control from legislative authorities and administrators, and due to the impossibility to alter records on the blockchain, both these

factors cause several problems (Price, 2018). Crypto-currencies are used by criminals as a mode of payment. However, as per Lewis et al. (2017), blockchain technology, despite having all weaknesses, is used for satisfying AML and KYC purposes for financial institutions and public transactions using blockchain.

2.5 Blockchain Development in Financial institution

Despite the fact that the dev't of the new technology is still in its initial stages and meets numerous difficulties, the basic multinational banks and other financial institutions that provide such service institutions immediately jumped at marking their territory and investing in development and design of the technology. Transactions on blockchain allow conducting processes of big data processing and therefore will move together with the process of big data in parallel. Additionally, people will be able to determine the development process in business activities (trade). The innovation introduced by blockchain technology is that it offers unlimited opportunities. Once blockchain technology starts being widely adopted by everyone, the commercial banks become active in improving and adopting the technology in order to make the centralized banking system even more powerful. Financial institutions will no longer require middleman due to transparency and immutability (Underwood, 2016). It is mainly due to the fact that for ages banks have performed the functions of middlemen and obtained numerous benefits from their trustworthy service. Nevertheless, the role of middlemen in banks' performance is becoming increasingly difficult under blockchain technology influence.

2.6 Suitability of Blockchain in Automating KYC

Regardless of the nature of technology, it looks like some form of integration should take place within the existing financial system infrastructure for the sake of making it more convenient. Another very important consideration is preventing the development of various technology stacks. The existence of manual procedures is one of the most significant hurdles for using blockchain-based technologies. Moreover, getting rid of obsolete infrastructures and reducing the amount of expensive reconciliations becomes a requirement. According to Angela Walch, the use of blockchain technology should not be viewed as a matter of simple connection and entertainment (Wharton 2018). "Blockchain technology, at its core, is just group bookkeeping. If you want to maximize on its benefits, you have to bring all members of the group into the process of the system. That requires cooperation among and between businesses, which could

be a big hurdle and possibly the biggest" (Wharton 2018). From another side, the European Network and Information Security Agency believes that "most future distributed ledgers will require interaction between themselves in terms of data exchange and thus format and protocol translation" (ENISA 2016).

2.7 Theoretical Framework

Egelund-Muller et al. (2017) indicated and looked at the possibility of building a multi-party automated financial system using diffused financial instruments such as settlement, directly on the distributed ledger technology. The rise of regulation and the development of technology, along with the 2007 financial crisis, have created space for businesses operating in the area known as "RegTech." RegTech is a word that combines two words: "regulation" and "technology." In relation to the scope of KYC, these possibilities are of special importance (Memminger et al., 2016; Arner et al., 2016). It is essential for the consumer to undergo the KYC procedure first before dealing with any FI or NBFI. In its current form, whenever the client decides to partner with a financial institution, the KYC process procedure generates costs. At this stage, it becomes essential to distinguish b/n the "core KYC process system", which constitutes the core of KYC verification procedure that all financial institution have to conduct according to the law, and the "bank-specific processes". In order to solve the problems with efficiency of KYC process, the new concept of DLT-based KYC needs to be introduced on the following assumptions (Parra Moyano & Ross, 2017).

i. The conditions under which vital KYC verification is made available to a client are established collectively by a set of FIs that are all operating within the same country and hence fall within the purview of KYC requirements.

ii. A consensus is reached amongst the entire set of FI participating in this arrangement regarding the cost associated with the execution of a KYC procedure. Of course, this cost depends largely on the nature and specific conditions surrounding individual clients (such as size, risk level, documentation, etc.).

iii. The regulatory body must maintain the structure and allow the financial institutions to

improve their KYC procedure to be better and streamlined.

The above-mentioned three assumptions are needed in order for all of the participating financial institutions to get proper compensations.

2.8 Issues related with adoption of Blockchain in KYC in Banking Industry

The old traditional contribution has to change the path for blockchain mechanism and digital evolution, states the World Economic Forum (2015). In particular, governments will opt to take an engaging facilitator role instead of a commander role. Should monetary organizations choose to adopt blockchain technology, it will affect existing structures in place concerning pricing and exchange rates. The elements that enable blockchain adoption are viewed as opportunities of adopting blockchain technology.

As the thought by per Lang (2017), the encryption aspect of blockchain ensures security in sharing data so that banks can create an up-to-date database of identification data of their clients. This is going to enhance AML/KYC process, ensure better interoperability of banks globally, cut costs in administration and avoid data duplication, hence reducing infrastructure cost. Nevertheless, it is anticipated that blockchain-based KYC registries will fail to be adopted widely since banks would not like to rely on third party for data verification process.

As stated by The contribution of Smith (2018) was about how the consensus, encryption, security features, timestamp, and auditing associated with the use of the blockchain can be made more continuous and in real time instead of merely historical and can evaluate all transactions as compared to traditional random statistical sampling approach. Smith (2018) anticipated that audit firm will play a bigger part in data security plans and decision making. Transparency and safety of banking process would be ensured owing to the blockchain technology. Highest level of transparency is achieved through locking down the blocks and giving maximum access to historical information and right authorizations and any changes will be available publicly as well. Real time auditing, automatic preparation of financial statements, immediate actions in case of violation of any regulations and instant interaction between banks and regulator would all be possible (Hassani et al., 2018).

Intermediaries are considered outdated in view of what Lang (2017) found out and contributed to, that is the certainty that can be gained through blockchain allows both person and FIs the opportunity to make direct transaction thereby making payment process easier

and safer. The average TPS in a blockchain transaction, according to Hassani et al. (2018), is 1,000-2,000 TPS; however, no consensus in terms of blockchain transaction capability has been reached in the banking sector. In contrast, Marr (2018) argued that, because of the high levels of sophistication, encryption, and distributed functionalities of blockchain, the technology is expected to be relatively slow and inefficient, especially in larger applications. As a relatively nascent solution, he calls for improvement through engineering and speed in processing. The operational costs, according to Accenture (2017), will be reduced by half. In comparing the adoption drivers to the occurrences of the term, "improving KYC process," emerges as the winner, with 46.80% of all supporting factors. Given that the top three factors are the most relevant, it follows that the availability of systems and infrastructure plays a more crucial role in blockchain adoption in the banking environment (Kawasmi et al., 2020).

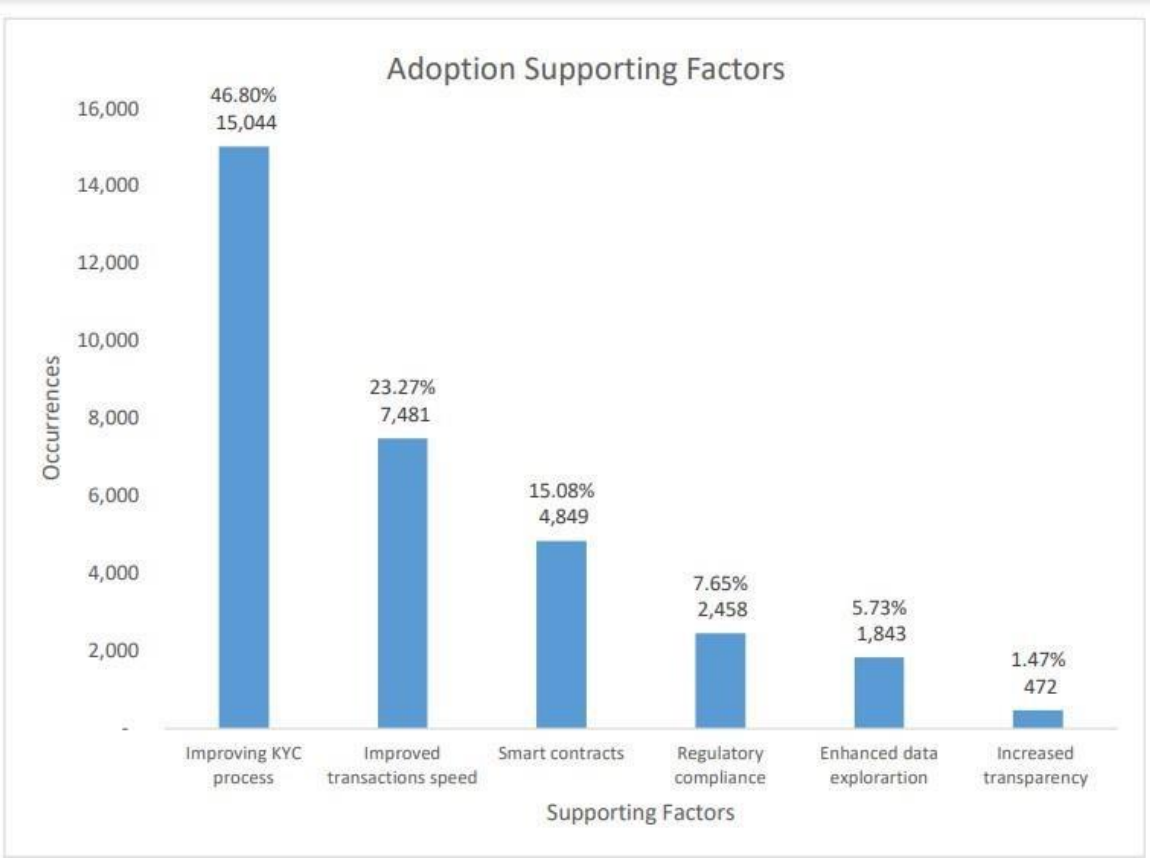


Figure 4: Blockchain Adoption Supporting Factors (Kawasmi et al., 2020)

2.8.1 Interoperability in Adoption of Blockchain

Interoperability refers to a characteristic of blockchain-based platforms that enables connections and data circulations (Courcelas & Timsit, 2019). Despite several options to make blockchain's interoperable, only two models can be distinguished, as to Courcelas and Timsit (2019). An approach to using trusted third-party authorities (Trusted Bridging) to verify transactions or data is included into the first category of interoperability. For instance, two or more blockchain's may agree to permit an off-chain entity to transfer data between them or record their states so that each blockchain would believe what had been done on another one. Moreover, multiple blockchain's may depend on a trusted third party for obtaining information such as certificates about people's or assets' identities. Another interoperability approach (Trustless Bridging) is related to explicit information transfer between blockchain without involving a third person. Although implementation of the proposed blockchain-based process along with the existing process is quite difficult, the new ideas can gain attraction.

2.8.2 Adoption of Blockchain Models for Theoretical Framework

The importance of explanations of emerging technologies for policymakers to be better prepared for the introduction of a technology. The use of new technologies in an industry such as the banking industry, which is heavily regulated, should not be determined by the acceptance of its clients but rather by new laws and guidelines (Kawasmi et al., 2020). There has been enough research done on models for the adoption of technology in the last few decades that has led to the development of several different models for technology acceptance; some examples of those are TAM, Extended Technology Acceptance Model (ETAM), and Rogers DOI (Taherdoost 2018). The most accepted and utilized model for technology adoption is TAM, as argued by Gangwar et al. (2014) and Taherdoost (2018). According to Gangwar et al. (2014) and Taherdoost (2018), the reason for the widespread acceptance of TAM model is based on the following three determinants: perceived usefulness (PU), perceived ease-of-use (PEOU), and attitude towards (A). Wang et al. (2016) proposed a Blockchain Maturity Model (BCMM), considering the need for a business to determine its maturity level before adopting the new technology.

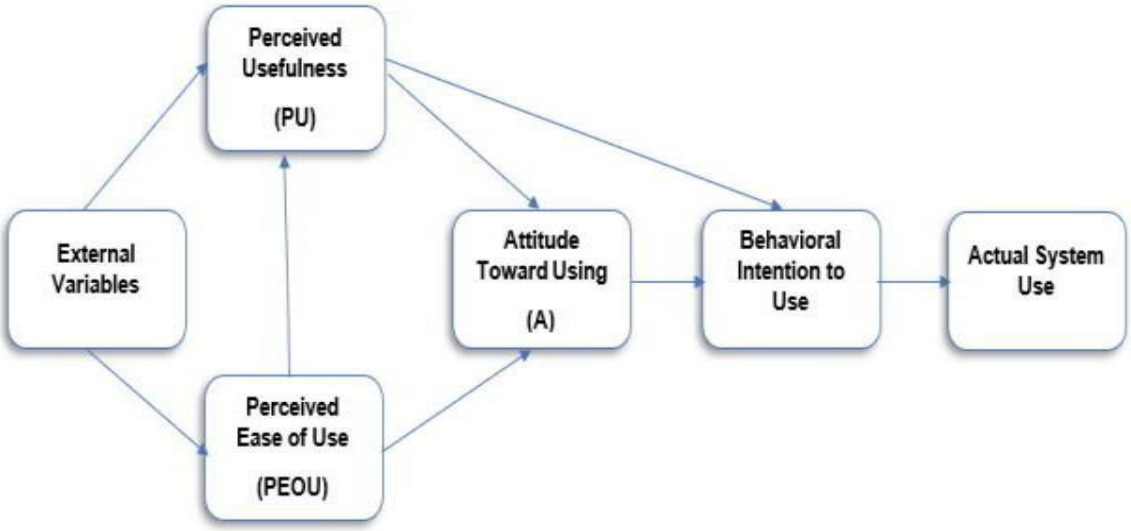


Figure 5: Technology Acceptance Model (Davis, 1989)

2.9 Blockchain Based KYC cases

While the blockchain had an apparent application potential, the feasibility of the KYC utility needed to be assessed in order to determine the actual applicability of the same. KPMG in Singapore and Bluzelle Networks developed a proof-of-concept KYC utility based on blockchain network in 2017, collaborating with three banks of Singapore including HSBC, OCBC, and Mitsubishi Financial Group (MUFG), as well as the Singapore regulator, Info-communications Media Development Authority (IMDA). In the initial phase, all the other KYC requirements were first discussed on the single network, and existing user data was exchanged with the user's consent after developing the distributed KYC system. Customer data was verified by relevant third parties, whose findings were recorded on the KYC shared ledger, increasing data depth. Customer behavior, approvals, as well as any new data supplied to each of the three banks was tracked and recorded. This proof-of-concept prototype was developed by KPMG in 2017 in order to assess the technical aspects of blockchain connections including usability, fun security, and scalability (Eamonn & Chia, 2018). The results of the test led to the following conclusions:

Table1: Result of Blockchain based KYC Prototype by KPMG

Factor	Conclusion
Responsiveness	The blockchain KYC platform remained stable and responsive even at a high volume of information flow
Performance	Platform performance was strong, with transaction times remaining swift even as transaction concurrency and complexity increased.
Security	All data was secure and confidential, with access limited only to those with the correct authentication codes.
Cost-Effectiveness	The platform could save an estimated cost of 25–50 percent by the reduction of duplication and providing a clear audit trail.
Tamperproof	The platform resisted tampering by third parties.

Clipeum

By introducing an open source financial ecosystem for collaboration in the process of handling and storing the documents relating to KYC, they attempt to solve some of the inefficiencies of the market space. It offers a multi-finance institutions platform which would greatly speed up the entire KYC process; however, the main purpose of the system is just document management. Although banks will have to go through their own KYC process independently, the task can be made easier with the help of Clipeum's APIs.

This guarantees that should a FI require access to some particular set of records, then the treasurer has the power to provide such access to the bank whenever it is required. A treasurer who wishes to end a business arrangement However, a specific FI can anytime withdraw its access to information from the particular institution's data (Patel & Ganne, 2020).

KYC-Chain

This is an automated system of processes based on blockchain technology that simplifies the KYC process and controls the whole customer lifecycle. Sanctions scanning, identity verification, OCR extraction software, API integration, and much more are elements of the solution system, which was developed as a result of dissatisfaction with the existing KYC process. Users have the ability to develop a turnkey solution that will meet the legislative requirements of various regulatory systems thanks to the completely customizable kit they offer (Bringing Digitalization to the Business World, 2020).

Shyft

Blockchain enabled public network where the user companies will be able to exchange internal data and get the consent from their customers to exchange personal documents of theirs, while being compliant with regulatory standards and requirements of FTAF. Essentially, Shyft is a public network which will allow companies within the data ecosystem to interchange encrypted data within external database. The network will never take part in any transaction or data custody; rather, it will enable users to exchange their data with other participants of the network of their choice.

2.10 Summary

From Previous years' researches and theoretical background of the analysis are the most important sections of the current chapter. Research papers of past years have been thoroughly examined in order to identify the identity process, the stages of such verification processes, including their strengths and weaknesses, traditional blockchain approaches to KYC process, and scopes and challenges of blockchain based KYC verification process. Furthermore, the components, processes, forms, and features of blockchain technology have also been examined from the previous researches and implementations. Suitability of blockchain for KYC process and the ability of blockchain technology to bring improvements to banking sector, at its best, have been investigated. Conditions regarding the adoption of blockchain technology and their implications on the KYC process have also been identified in the theoretical background section.

CHAPTER THREE
RESEARCH METHODOLOGY

3.1 Research Design

The steps we followed are DSR approach. The purpose of developing DSR was to help IS researchers find a solution to previously unsolvable problems using continuous iteration of building and evaluating. The outcomes of DSR are IT artifacts including constructs, models, methods, and instantiations. Some academics believe that the IT artifact alone can serve as a research contribution if it is novel and useful (Gregor and Hevner, 2013; Baskerville et al., 2018); however, there are still two challenges to distinguish the contributions of DSR research. First, it is difficult to identify exactly what constitutes the theoretical contribution of DSR (Gregor and Hevner, 2013). Second, it is difficult to strike a balance between practical contribution and generalizability when dealing with fast-paced technological changes in a technology context [Baskerville et al., 2018]. In order to meet these challenges, our goal is to contribute with architecture design and processes as an IT artifact. Then, to contribute theoretically with the proposed IT artifact, we will derive DPs from it (Hevner et al., 2004; Gregor and Hevner, 2013). Therefore, our goal is to make a contribution to nascent design theory in the form of operational principles. For an IT artifact to provide a significant contribution to the IS discipline, the IT artifact has to satisfy a business need (Hevner et al., 2004). Such a business need may stem from any persons, organizations or technology in a particular environment. Nevertheless, an IT artifact must also be relevant in the same environment where the business need arises (Hevner et al., 2004). For the construction of a robust IT artifact through design, the IT artifact must also be built on previous IS research knowledge [Vom Brocke et al., 2020]. Furthermore, there must be use of existing research methods in assessing the created IT artifact [Hevner et al., 2004]. In the case presented here, the proposed framework is informed by existing literature that focuses on enhancing the KYC process through the use of technological advancements in addition to the technical and theoretical background of KYC and DLT. We have used a popular and reputable (Schweizer et al., 2017; Reinecke and Bernstein, 2013] DSR process model of Peffers et al. [2007] to create

The IT artifact

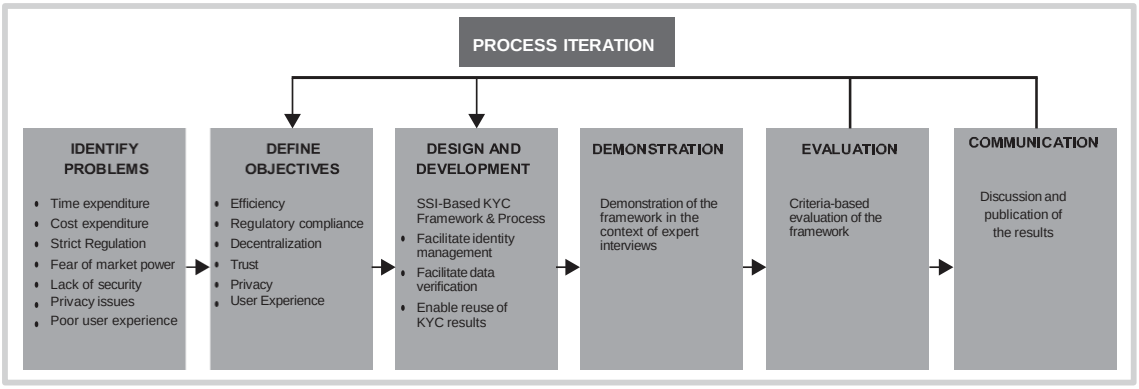


Figure 6: Our applied DSR process, following Peffers et al. [2007].

Created by a rigorous method. Our method consists of six stages ordered sequentially (please see Figure 6), including the iterative nature of research [Peffers et al., 2007]. The process begins with the formulation of a practical problem of research. For example, in Section 2.2 .1, it was revealed that the existing KYC procedure poses several challenges, such as inefficiency of the process, security problems, issues of the user experience, and confidentiality of data. At the end, we formulated solution goals.

3.2 Research Approach

As per DSR criteria, the results generated from the build and evaluate cycle should be generalizable and hence applicable to more generic situations. Furthermore, the design artifacts should create disruptive changes in the usual ways of doing things [Hevner and Gregor, 2020]. Current trends in DSR suggest that researchers should conduct studies based on previous DSR studies conducted within the same field. We generated the solution objectives after conducting a review of existing literature and compliance regulations related to the KYC process and blockchain identification and authentication, leading to six solution objectives for the KYC process and numerous requirements for each solution objective. From these objectives and theory, a blockchain-based KYC process will be designed and developed as the next stage in our research process. Phase 5 involves evaluation, which becomes essential to test if an artifact fulfills the very purpose of creating it and validating this claim through rigorous methods. Evaluation

Also assists one to comprehend the problem situation more clearly and hence generate better results.

3.3 Research Analysis Approach

Since there is no unique route with respect to the evaluation process because the optimal way to do it would vary based on the issue under study as well as the artifact being analyzed (Peffers et al., 2007), our evaluation process had several iterations, beginning with the formative evaluation of the design objectives with interviews of staffs and experts. Additional interviews followed for summative evaluation of our framework by showing it to the respondents and integrating their suggestions. The evaluation itself was intended to reveal whether our framework was functional, accurate, reliable, fit-for-use and organization-wide. Next, we used criteria-based evaluation in terms of assessing whether the solution objectives achieved were met because the evaluation criteria should be established individually for each artifact (March and Smith, 1995). In order to bring implicit contributions from IT artifacts into abstract, generalizable knowledge for the purpose of further discussion, we created nascent DPs in the field of blockchain technology since it was novel and popular while the general DPs still lacking in literature. Finally, we delivered our results to the target audience. The DSR applied was iterative and partially parallel since the results of the evaluation shaped our artifact.

Qualitative interviews, which have been applied during our evaluation cycles, are very common research tools in the field of IS studies, as they can be applied successfully to gather in-depth data. Semi-structured interviews were held in order for us to respond in an appropriate manner to the interviewee's answer and ask additional questions to get deeper into the matter. The staffs (department team) on KYC and IT department teams were used as the interviewees to represent the opinion on the topic in terms of practical applicability within existing organizations, as well as in relation to the structures of the Cooperative Bank of Oromia and opinion on technical maturity and feasibility. In addition, the interviewees were chosen to avoid an elite bias; namely, they represented the voices of executives of various management levels. Additional requirements included comprehensive knowledge and rich experience of the interviewees within their area. Open and axial coding techniques were applied for the purpose of analyzing the gathered data. Interviewing took place for 120

minutes (average duration of each interview was 15.6 minutes). Interviewing was conducted, taped, transcribed, and then content analysis was performed using the MAXQDA program. The categories are “the higher level concepts”. An outline of the participants in the interviews is presented in Table 2.

Session	Staffs	ID	Role	Background/position	Type of interview
1	KYC	A	Project Manager KYC	Strategic analysis and research	Phone Call Phone Call
1	KYC	B	Sales Director	Research, Banking	Phone Call
1	KYC	C	Identity Engineer	Innovation Consultant	Video Call
1	KYC	D	Executive Director	Banking	Phone Call
2	KYC	E	Branch Internal controller	Compliance	Physical
2	KYC	F	Senior Developer	Computer Science	Phone Call
2	KYC	G	Supervisor	Start-up CSO	Phone Call
2	KYC	H	Sales Executive	Banking	Video call
2	KYC	I	Sales Director	Banking	Phone call

Table 2: Overview over the Interviewed staffs.

We classify lower level concepts as sub-categories under it. In the first round of coding, we made 20 categories and 200 sub-categories, while in the second round, axial coding was used to make sub-categories. Therefore, all the data that were classified in open coding were reclassified into an abstract form in categories.

Chapter Four

Evaluation and Result

Introduction

The case study and title selected, as well as the collected information, have been covered in this chapter of the study. It contains all details of how the interviews were analyzed using MAXQDA software. Besides, it covers the results of the interviews in great detail.

4.1 Evaluation of the Blockchain Framework

The discussion on the existing problems in the KYC process and our identified goals for the KYC process took place with KYC staff members. Our goal for conducting these interviews was to evaluate the identified goals in terms of relevance and completeness. We chose different staff members from different departments and at different levels to gain various perspectives on the goals.

Staff A believed in the appropriateness of objectives and their prerequisites. Since the cost of people and technology is increasing, process efficiency is an important goal that the banks must achieve. Process efficiency also includes digital processing throughout the entire process and interbank coordination in the process, where there are issues of trust between the banks and also mistrust by customers about the safety of their information. The other issue is that of the importance of privacy, which was one of the important aspects highlighted by the person. In addition, he highlighted the importance of the need for regulations and their compliance. For example, customer information has to be stored for a minimum period of five years by the banks.

Additionally, process efficiency is considered the most important factor according to Staff B since it allows for saving costs and time. It appears that the amount of manual operations in the process is quite high. Thus, the automation of procedures and digitization of documents processing becomes essential. Besides, Staff B emphasizes the necessity to pay special attention to the protection of customers' privacy. The sensitive approach to handling private information is required since no third parties, including partners, are allowed to access such information.Concerning the user

experience aspect, Staff C considers it significant as users rarely pay attention to the functionality. Besides, special emphasis must be paid to usability issues when implementing the solution. With respect to the architectural aspect, Staff C highlights the importance of providing backup and recovery services within cloud storage for improving users' experience in case of data theft or data loss. In response to the question about the role of IDAS in designing a KYC system, Staff C confirms its importance. In particular, there remain some uncertainties regarding IDAS as far as the possibility of using personally identified information is concerned when such information is encrypted or hashed. Moreover, it became clear that the blockchain - based data cannot be deleted. Among other issues of using KYC documents provided by other banks, the issue of establishing a mutual trust relationship between banks was mentioned. Nonetheless, the combination of KYC architecture with the IDAS infrastructure will resolve this issue. Finally, it should be stressed that all the rest of staff mentioned all design objectives which seemed very relevant for KYC evaluation from the point of view of a bank.

4.2 Blockchain based KYC process Result

Based on the typical steps of the KYC procedure implementation, we have considered the KYC procedure implementation in three stages that include (1) Customer Identification, Data Validation and Identity Verification; (2) Name Screening, Risk Evaluation and Enhanced Due Diligence; and (3) Monitoring and Record-Keeping. The first stage has been further divided into three different scenarios based on the client’s status in relation to the KYC process.

In other words, the KYC procedure implementation starts with the client onboarding. The following three different situations are possible regarding this stage. First, the procedure of complete onboarding is implemented when the client does not have any wallet or VCs proving completion of the KYC procedure. Second, the fast onboarding procedure takes place if the client has a wallet or self-sovereign wallet along with the VCs verifying completion of the KYC procedure in the previous period. Finally, there is a “new to KYC” situation wherein clients have wallets and VCs with their identities from another environment.

Regarding the first scenario, the following figure illustrates how it is represented on a UML sequence diagram (see Figure 7 below). Let us first take a look at the situation when the

bank uses blockchain for the onboarding process. In order to make this process functional, it must complete what is called a "one-time" bootstrapping step during which it will register its own public DID and the DID document. The latter can contain all sorts of services of the bank such as customer services or Know Your Customer process. Moreover, the bank will have to create its credential definition based on a certain credential template comprising the attributes of the verifiable credential. All of this data needs to be accessible from the public and should be related to cryptography in order to enable validation of the VPs made by using the specific VC and to allow non-revocation proving for customers.

After the preparation process, the bank is ready for customer onboarding. Though the sequence diagram on [Soltani et al., 2018] gives a relatively simpler example regarding customer onboarding, it still contains too many unnecessary frequent reading operations of the blockchain and writing into it. According to the outcome of our interview, having a peer DID of the client is enough and even more confidential in this case. Also, we will describe the consequences of such architecture both for the bank and the client: binding, revocation, and backup. As for onboarding, it starts when a client visits the bank's website either through a smartphone or laptop or physically visits a bank to open a new account. Since the client doesn't have an SSI user wallet as well as the necessary KYC documents, the bank suggests downloading a wallet for the client and provides him/her with a corresponding link. Any digital wallet supporting public DID, peer DID, and VC standards can be used by the client. It will store the credentials and keys, secured with either password/biometric protection. Even a bank can provide a corresponding edge agent, encrypted in a cloud-based environment, in order to use this capability as an alternative backup/recovery method. The system will generate a new DID with keys needed for encryption and will store them in the user wallet. At first, the wallet creates a certain link secret. This function is useful for combining various credentials within one VC for the reason of not being able to selectively disclose the credential information afterwards. However, when all the credentials contain some common information like the customer's name, it becomes easy to prove their connection without the link secrets. The customer will then be able to utilize this DID to establish a secured channel of communication between themselves and the endpoint made available by the bank for carrying out the KYC procedure. In another scenario, this information can be provided to the customer through a QR code (e.g., through an email), whereby scanning the QR code by the customer enables them to connect to the endpoint provided by the bank.

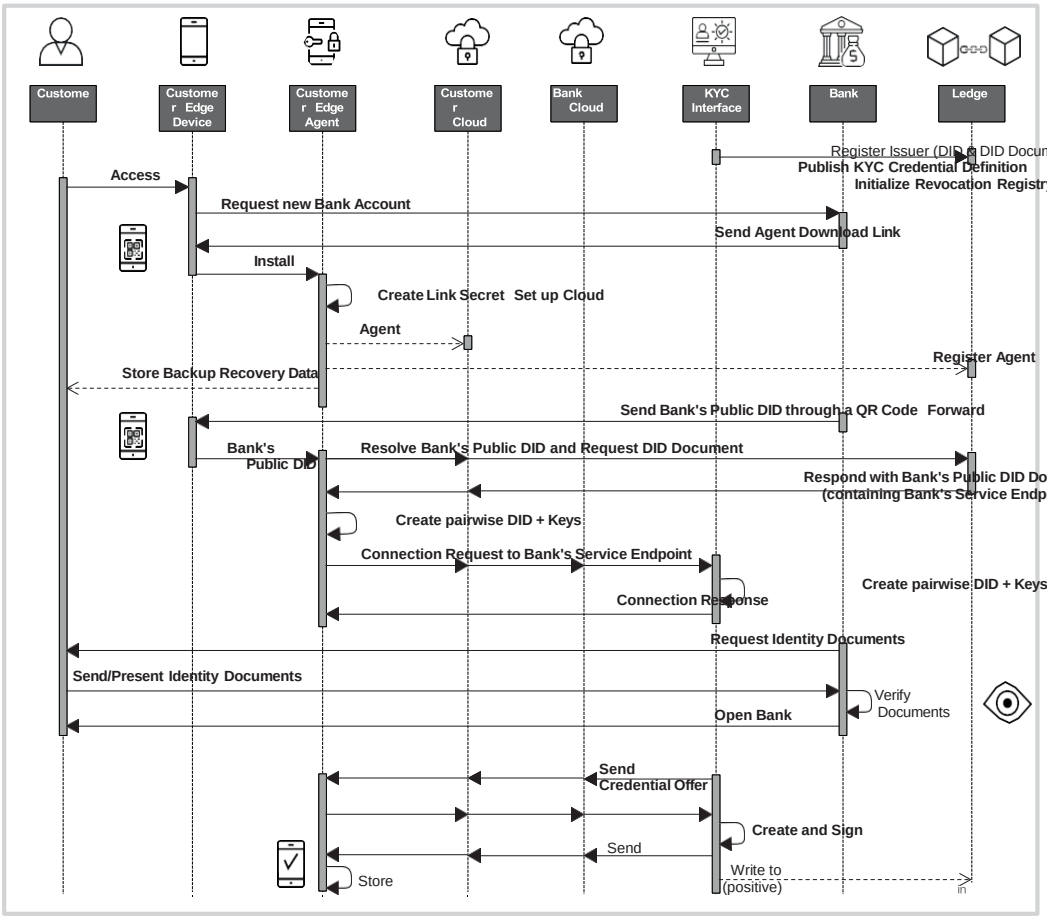


Figure 7: UML Framework: *Completely New Onboarding*

At this stage, the new pairwise DID have been created along with the bank's key pair that is unique to this particular business relationship. Moreover, the bank sends a connection request to the cloud agent of the customer's service that, in turn, forwards the message to the customer's wallet. In the connection request, the bank will provide its DID, the corresponding public key and the service endpoint at which the customer can reach out. In addition, the connection request may include the proof that the bank's DID is indeed authorized (for instance, the VP containing the proof of the identity of the bank issued and certified by the reputable public entity). As a consequence, the customer's digital wallet authenticates the connection, creates a new set of DIDs and keys for this relationship and replies to the connection request of the bank, sending the message to the cloud agent or wallet of the bank. At this stage, an end-to-end

encrypted connection has been successfully established and the customer and the bank can start exchanging messages, public keys, VCs and VPs. Since the client does not have any verifiable credentials, it needs to get verified first. In case of traditional procedure, the client will submit his or her analog identity data manually or via email transmission and uploading the scanned data to the newly established channel. Should the customer register an account in the branch office of the bank, the documents will be verified right there in the bank. Once the identity of the client is successfully confirmed and verified, the bank will send the credential offer to the edge user agent of the client that will contain the preview of the attested data, issuer details, the expiration date of the VC and credential revocation information. Following the credential request acceptance, the client sends the credential response using the link secret encoded in the blinded form. Nevertheless, the client is obligated to produce the link secret once and then use it again in future credentials. The blinded link secret appears among the attested attributes on the VC which then the bank forwards to the client. As a result, the credential may allow selective disclosures. This means that the client is able to provide the attributes that the verifier requires and attests in each VP.

If there is support for the revocation functionality and the issuer has previously bootstrapped the revocation registry, then the VC will have the information regarding whether the VC has been revoked or not. This implies that the issuer can create credentials using the revocation registry within the distributed ledger system. Additionally, the bank might take advantage of this functionality to revoke the credential in the event when it was mistakenly created. It is essential to highlight that it is because of the additional information concerning the revocation within the credential itself that the client is capable of interpreting the data contained in the public revocation registry. Since the actual credential does not get disclosed while only proofs can be generated based on it, such approach seems to be enough for meeting FTAF requirements. Such fast process gets also initiated whenever the bank customer logs into the bank's website or bank branch website to create a new account at the bank.

The channel needs to be trusted since in this situation the customer cannot possibly know the DID of the bank beforehand. The customer can follow the below-listed process for checking the validity of the communication through using the identity system known as IDAS: First of all, the customer's IDAS certification

of the public key of the bank will be checked based on the DID document. Next, the user agent of the customer will determine the distributed ledger on which the necessary DID document will reside. Then, the DID document gets obtained by the customer's user agent. The user agent determines where they can find the endpoint for obtaining the KYC services offered by the bank. The connection request gets sent together with the customer's Pairwise DID and its public key. Finally, the bank generates the Pairwise DID and its keys and answers back with the connection request.

After establishing the secure channel between the bank and the customer, a proof request to carry out quick KYC onboarding process will be made by the bank. The proof request will contain the nonce to stop any attacks on the channel. The proof request will specify what the bank needs from the cu stomer. The proof request will also indicate the conditions for accepting the proof from the client. For example, it will mention the issuers (credential definition) and schemas that have been used for issuing VCs and also any condition regarding non-revocation of VCs, together with the revocation registry timestamp if it exists. The agent at the client will look for VCs in the wallet that matches the condition specified in the proof request and will update the revocation registry locally and generate a proof that will be submitted to the bank. The bank will be able to cryptographically prove the validity of the claims, which may also involve verifying revocation registries and other information concerning the credentials.

It is also capable of cryptographically verifying the validity of the proof. The bank will verify that the digital signatures of the issuer are valid for all the attribute attestations that are in the VP; no attested attributes in the VP have been signed using a revoked VC; all the VCs that were used in the VP were issued for the same,

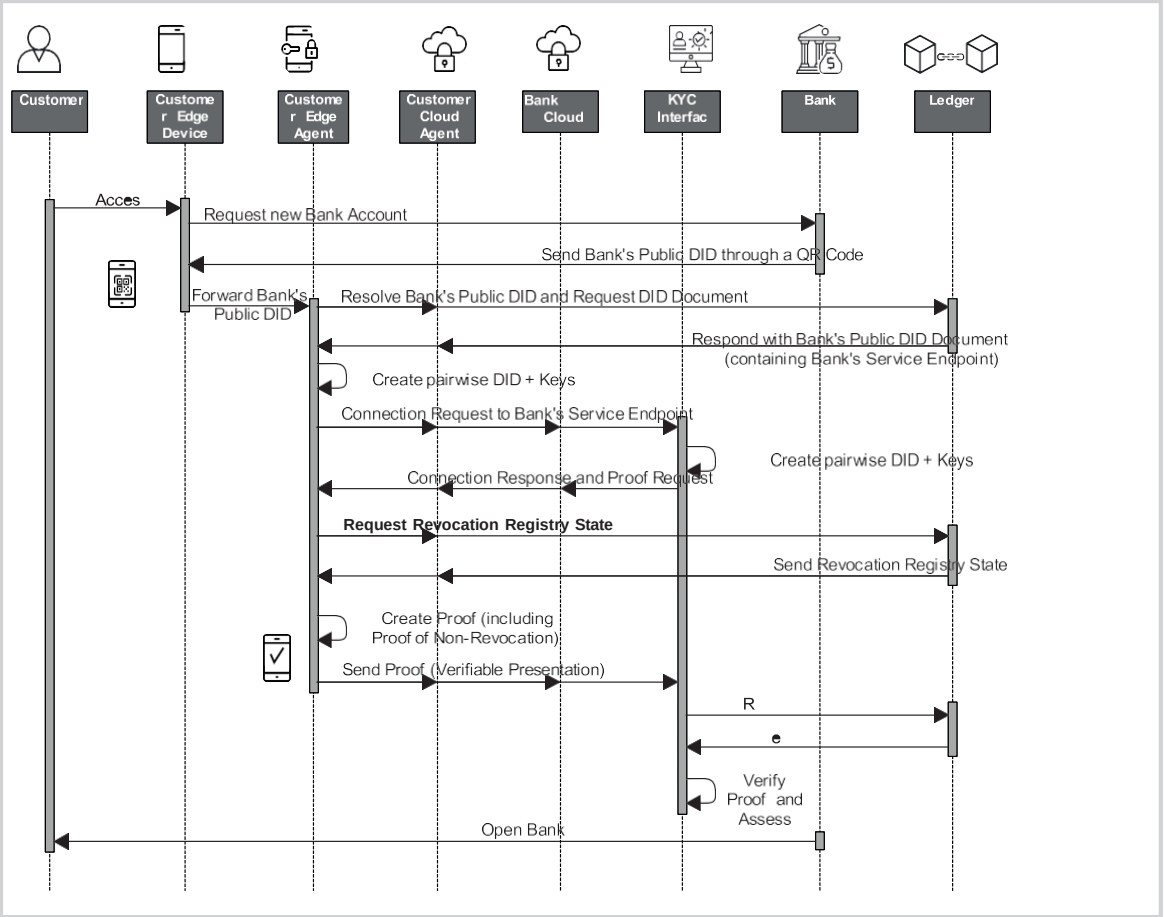


Figure8: UML Framework: *Fast Onboarding*

Common secret of the link. After the verification process is completed, the bank account will be successfully opened. All the processes mentioned above can be automated and would require just a few seconds of time. Secure connection, built on the basis of pairwise DIDs, may be employed for sharing documents in the future. The verification of all participants will be conducted with the help of the keys that were shared previously. The use of the keys is critical for the communication with digital identities as the bank should communicate with the same person in the future [Jessel et al., 2018]. The third onboarding type is also new to the KYC process because the client possesses their cloud user agent and VCs related to their identity in the case, but no credentials that are provided as a result of conducting the KYC process by the bank. Therefore, new to KYC includes both completely new and fast onboarding types of the procedure (see Figures 8)

and 8). Should the fast onboarding be accompanied by establishing the pairwise DID relationship, receiving analog identity documents, and obtaining KYC credentials will constitute the completely new onboarding procedure. However, prior to obtaining the analog IDs of the client, the latter may use a proof request to determine whether some of the documents will suffice as they are partially verified. Along with the opportunity to open the bank account online, one may visit the bank personally to establish the account via the QR code and get service endpoints. Once all the necessary data exchange and identity validation through cryptographic means have been done, then the name screening service is applied in the context of the bank's IT environment to analyze whether the acquired data matches some known public blacklists concerning terrorists, money launderers, politically exposed persons, or any negative publicity. Name screening results serve as inputs for the risk engine that will do the classification based on the acquired risk class. Through various parameters, including the outcome of the name screening, the risk engine will generate a score that will help classify the applicant as low, medium, or high-risk client. In case additional verification measures become necessary due to the risk class, other verifications will be conducted before allowing the new customer to open an account. The forging of the VCs is highly complex than that of the analog IDs; thus, only a limited amount of data is required for the initial screening process. To mitigate risks, the bank can use the secured communication channel to ask for more documents and data, such as the statement of income or purpose of the opening of an account. As demonstrated above, other documents could either be in paper form or VC forms that the user possesses, such as the income statement from the trusted employer. The corresponding VP can also be delivered. After verification of the client, the account can be opened.

Ongoing monitoring

After opening the account, the risk engine will continuously monitor all activities done by the customer as well as the number of transactions made by them during the tenure of the business relationship in relation to their expected number, and whether there is any indication that these transactions involve unusual transaction activities.

Record keeping

It is because of the concept of blockchain technology that the bank will not hold any personal information about the customer at all. This data will be located only in the wallet of the user, and it will be relatively easy to ask the data when required. At the same time, according to regulatory bodies, it may be important to keep the data on customers for a longer period of time, just in case it will be required to prove their identity in case of frauds and other criminal activities. Therefore, the bank will have to maintain a copy of the information in its local database within the redesigned system as well. However, there will be possibilities of manipulation with the data by the bank. The greatest benefit of using VCs that focus on ZKPs is that VP would be either non-repudiable or repudiable in order to create tamper-proof documents and ensure privacy in case of any hacking without the need for audits with sensitive information such as income included.

4.3 Challenges of Implementation

Trust Issue: Most of the respondents said that they trust the blockchain but not completely. There are still some confusions and a lack of confidence in the technology among some of them. Two respondents said they trust the public blockchain, not the private one. The technology is still not widely used; thus, it is not widely accepted by the stakeholders.

Resistance to Change: Change does not happen overnight; it takes a lot of time and practice from different levels. While perceived from a range of opinions, the interpretation of the findings indicates that many respondents perceive this phenomenon as a challenge to the blockchain's adoption. Among the reasons identified in the findings is an inability to abandon manual control and oversight, as well as a fear of displacement if they become redundant. Also, it would be hard to motivate the customer to be accustomed to a new process.

Training of the Employees: To shed light into this matter, some respondents said, to implement a new process, training is a must. The interviews revealed a profound lack of knowledge about technology. Training for the employees requires time and money. Not all banks or fintechs would like to pay for the training. The time needed for training is also the time of unproductiveness.

Educating Customer: Most of the respondents shared this challenge to implement blockchain technology. The majority of the customers, including individual or business entities, do not want to be bothered by new processes or systems once they are comfortable in an old system. Banks would have to educate all the customers about the new process, which will require money and time; also, it might cause customer discomfort because they are very busy people. One respondent said, "*This technology is very new to us, so it can cause operational risk. So we need to educate ourselves, and we need to educate our customers regarding this new process."*

Interoperability: Most of the respondents said there would not be a big interoperability issue. Interoperability is a property of a product or system that enables it to communicate freely with other products or systems, either now or in the future, in terms of implementation or access. However, few of them shared their concern about it because all the banks have different core systems provided by different software manufacturing companies.

Legal Risk: Legal risk associated with the public blockchain was considered a huge deal by the respondents. Public blockchain might pose a GDPR risk for the banks that would end in a colossal fine. One respondent said, *"There are risks involved in the public blockchain. If I store some personal information related to some specific customer, which can be accessed by the person who shouldn't have access to this information that is a huge legal risk.Because we cannot expose customer personal information to the world."*

4.4 Findings

This chapter began with the presentation of information regarding the study case and the research topic. After that came a description of the background of the interviewees whose data was gathered for the justification of their contribution.

Lastly, the result from the interviews is presented. The tables below show the results that have been derived through answering sub-research questions.

Table 3: summary of the findings

Research Questions	Findings from the Interviews
Output or implication of blockchain technology on the KYC process of FI?	
What is the status of the KYC process before the emergence of the blockchain?	• It is a very timely process. • The validity of the document is time bound. • Compliance standards vary from country to country. • The sources of information are public as well as private. • The communication process includes more layers. • The customer dissatisfaction depends on contact frequency.
Improvement in the KYC process can be described as?	• Time Effectiveness • Regulation • Automation • Customer Convenient • Data Sharing • Data Security • Privacy • Trust • Efficiency

What would be considered an improved KYC process?	• Fast process • Hard to tamper with • Automation • Convenience for the client • Reduced workload • Easy access to documents • Accurate • Efficient

Research Questions	Findings from the Interviews
How to determine the benchmark to measure the performance of the blockchain based KYC process?	
What are the key criteria for assessing the success of the KYC process?	• Cheaper • Reliability • Accuracy
What are the major indicators of efficiency in the KYC process?	• Number of case • Lead time • Quality Assurance
What would be deemed as convenient KYC procedures?	• Customer account • Customer response
What would be the operational and legal hurdles to the implementation of blockchain-based KYC?	
What are the major hurdles in respect of legal and regulatory frameworks?	• Legal risk • Different legal criteria
What are the main issues with operational procedures and interoperability?	• Change resistance • Client education • Employee training • Redundant Jobs • Interoperability • Trust issues • Energy consumption

What are the solutions for overcoming such hurdles?	• Standard KYC Practice • Skills-based awareness • Customer driven • Consciousness • Reception from the authorities • Approving process

Chapter Five
Conclusion and Recommendations

5.1 Introduction

As discussed in the previous chapter, Findings of the study have been presented. In this regard, the summary of the findings and recommendations are to be provided once general information is obtained through document analysis and interviews based on the research questions. In addition, implications of the findings, limitations of the study, and future research ideas are also discussed in this chapter.

5.2 Recommendation

Several aspects of Blockchain such as decentralization and immutability are some of the factors that make it an appropriate and safe method for conducting the Know Your Customer (KYC) process. However, there are several precautions that need to be taken for the implementation of this technology to take place effectively. Hence, the recommendations for the application and adoption of blockchain technology in the KYC process are as followed some steps in FI and Cooperative Bank of Oromia.

5.2.1 Automation

As per the respondents and earlier studies, there would be one bank who would initiate the steps of the core KYC process for the new client, and then the client would send the needed documents for the KYC process through customer portal networks to the bank through the interface of an advanced KYC system. The said documents that would be allowed by the permissioned ledger and with the digital signature would be entered into a set of documents, which includes the acceptance or rejection of the said documents. After the basic KYC process is completed, then the consumer would be provided a new account having both the public and private keys.

5.3 Feasibility Study

The feasibility study is very essential in evaluating the feasibility of the project (Mintzberg et al., 1976). As our findings from the interview regarding feasibility mechanism shows that despite the public ledger holding the hash code and key to the document packages, there is not a bank that will hold customer information on the public ledger since it is very easy for frauds or financial hackers to retrieve the document packages using the transaction history through hash codes and keys. Data retrieval efficiency can improve when customer document packages are held by the financial institutions in their local servers. Therefore, it was recommended that each FI should have at least one unique account for each customer in the permissioned ledger.The bank needs to carry out a survey data of the customers (personal banking and business banking) to ensure that their expectations are met.

5.3.1 Common Standard of KYC

It can be seen from the result analysis that lack of properly designed KYC laws complicates the whole process and renders it tough. Most countries tend to use the US Patriotic Act 2001 as the core KYC laws. However, the ID verifying procedure and other identity information vary in many ways compared to many other countries. They include whether the ID copies should be legally acceptable, urgency of the document as well as the extra information about beneficial owners of the business among many others. Besides, there is an existence of difference in data privacy laws when it comes to Ethiopia as compared to the US because of the existence of FTAF Ethiopia. In the rest of Asia and Africa, the KYC laws are said to not be strict and practiced enough. Though it may seem unrealistic for all countries to adopt the same KYC laws, it would be expected for financial centers to adopt one KYC law. This makes the whole KYC verification process easy regardless of the method of application.

5.4 Limitation

It is impossible to deny the flawlessness of qualitative data analysis since it involves subjective evaluation and interpretation on the part of the researcher, unlike quantitative research, which presupposes following certain rules and formulas (Patton, 1999). As for the research at hand, there is also some probability of biased interpretation of the obtained results. Speaking about generalizability of the conclusions drawn based on qualitative research; one cannot point out only a single opinion concerning it. Positivist scientists have difficulty generalizing the conclusions they arrive at while conducting a qualitative study (Shenton. 2004). However, this does not mean that it is impossible to make certain conclusions regarding the possibility of such a generalization. Some scholars think that generalizability depends on how the reader perceives the presented analysis. Despite the fact that this research provides all necessary information required for its adoption, such generalization is possible, to put it mildly.

Since the discussion of issues was conducted in a confidential manner and the information discussed could be regarded as sensitive, it was necessary for the author to assure the participants of complete anonymity. This is why the discussion itself has been omitted from the transcription of the interviews, despite it being recorded on tape. However, the audio recording does include the names of the participants, place of work, as well as several pieces of information that should be considered private within the framework of the corporate code of ethics.

5.5 Future Research

It is important that further research be conducted to be able to understand the output and consequences of the blockchain implementation process. FIs and Cooperative Bank of Oromia require knowledge regarding the impact of the blockchain adoption on the confidentiality of their data. The knowledge obtained will help them decide which strategies should be implemented so as to ensure their privacy will not be violated. Since these studies were carried out in specific geographical locations, results cannot be generalized to other locations.

The primary purpose of carrying out the research was creating a framework of adoption of the technology in strengthening the KYC system. However, the adoption

part did not include any implementation plan. It is advised that researchers conduct a new form of research in order to simplify the development and implementation of the solution. Where the adoption research discusses the adoption and integration of the technology by financial institutions and Cooperative Bank of Oromia in order to offer better services, the implementation research will focus on configuration, management, and training of employees on the usage of the technology.

REFERENCES

1. Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. MIS Quarterly, 28(1), 75–105.

2. Dierksmeier, C., & Seele, P. (2016). Cryptocurrencies and business ethics. Journal of Business Ethics, 152(1), 1-14.

3. Drew, J. (2017). How blockchain is revolutionizing KYC. Journal of Digital Banking, 2(2), 123-131.

4. Hevner, A. R. (2007). A three cycle view of design science research. Scandinavian Journal of Information Systems, 19(2), 87–92.

5 .World Bank. (2022). Financial consumer protection and fraud prevention in digital finance. World Bank Publications.

6. Kshetri, N. (2017). Can blockchain strengthen the internet of things? IT Professional, 19(4), 68–72..

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

8. Rabah, K. (2021). Challenges & opportunities for blockchain powered financial systems in developing economies. International Journal of Advanced Research in Computer Science and Software Engineering, 11(4), 1-15.

9. World Bank Group. (2021). Blockchain for development: Emerging opportunities for developing countries. Finance, Competitiveness & Innovation Global Practice.

10. Zetzsche, D. A., Arner, D. W., & Buckley, R. P. (2020). Decentralized finance (DeFi). Journal of Financial Regulation, 6(2), 172-203.

11. McKinsey & Company (2020), blockchain can reduce the time required for KYC by up to 70%, while also improving data accuracy and reducing fraud. Alammary, A., Alhazmi, S., Almasri, M., & Gillani, S. (2019). Blockchain-Based Applications in Education: *A Systematic Review. Applied Sciences*, 9(2400), 18.

12. Bhatia, S., & Wright de Hernandez, A. D. (2019). Blockchain Is Already Here. What Does That Mean for Records Management and Archives? Journal of Archival Organization, 16(1), 75–84. https://doi.org/10.1080/15332748.2019.1655614

13. Brew, T. (2020, October 8). *Blockchain in KYC Verification(Know Your Customer)*. Medium. https://medium.com/techskill-brew/blockchain-in-kyc-verification-know-your-customer- 67aeb57984e7

Bringing digitalization to the business world: A DLT adoption outlook. (2020). Cointelegraph. https://cointelegraph.com/news/bringing-digitalization-to-the-business-world-a-dlt-adoption- outlook

14. Budhiraja, S., & Rani, R. (2019). TUDocChain-Securing Academic Certificate Digitally on Blockchain. In S. 15.Smys, R. Bestak, & Á. Rocha (Eds.), Inventive Computation Technologies (98th ed., pp. 150–160). Springer Nature Switzerland AG.

16. Callahan, J. (2018, July 10). *Know Your Customer (KYC) Will Be A Great Thing When It Works* [News Paper]. Forbes. https://www.forbes.com/sites/forbestechcouncil/2018/07/10/know-your-customer-kyc-will-be-a-great-thing-when-it-works/

17. Casino, F., Dasaklis, T. K., & Patsakis, C. (2019). A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telematics and Informatics*, *36*, 55–

18. https://doi.org/10.1016/j.tele.2018.11.006

Consumer financial services action plan. (2017). Retrieved 14 April 2021, from https://ec.europa.eu/info/publications/consumer-financial-services-action-plan_en

19. Courcelas, L., & Timsit, K. (2019). Scalibility Interoperability and Sustainability of Blockchains. The European Union Blockchain Observatory and Forum. https://www.eublockchainforum.eu/sites/default/files/reports/report_scalaibility_06_03_2019.pd f

Creating a GovPass digital identity. (2017). Retrieved 13 April 2021, from https://www.dta.gov.au/blogs/creating-govpass-digital-identity

20. Crosby, M., Pradan, P., Sanjeev, V., & Vignesh, K. (2016). *BlockChain Technology: Beyond Bitcoin*.

Davis, F. D. (1989). Perceived Usefulness, Perceived Ease of Use, and User Acceptance of Information Technology. *MIS Quarterly*, *13*(3), 319–340. https://doi.org/10.2307/249008

Denney, A. S., & Tewksbury, R. (2013). How to Write a Literature Review. Journal of Criminal Justice Education, 24(2), 218–234. https://doi.org/10.1080/10511253.2012.730617

21. Draheim, D., Koosapoeg, K., Lauk, M., Pappel, I., Pappel, I., & Tepandi, J. (2016). The Design of the Estonian Governmental Document Exchange Classification Framework. In A. Kő & E. Francesconi (Eds.), *Electronic Government and the Information Systems Perspective* (pp. 33–47). Springer International Publishing. https://doi.org/10.1007/978-3-319-44159-7_3

22. Drescher, D., 2017. Blockchain basics: a non-technical introduction in 25 steps, Apress, [2017], viewed November 23rd 2018, ISBN-10: 1484226038.

23. Duch-Brown, N., & Martens, B. (2014). Consumer Benefits from the EU Digital Single Market: Evidence from Household Appliances Markets. SSRN Electronic Journal. doi: 10.2139/ssrn.2446964

24. Dumortier, J. (2016). Regulation (EU) No 910/2014 on Electronic Identification and Trust Services for Electronic Transactions in the Internal Market (eIDAS Regulation). SSRN Electronic Journal. doi: 10.2139/ssrn.2855484

Eamonn, M., & Chia, T. Y. (2018). Could blockchain be the foundation of a viable KYC utility? KPMG International. https://assets.kpmg/content/dam/kpmg/xx/pdf/2018/03/kpmg-blockchain-kyc- utility.pdf

25. Ecosystem, A., & Model, O. (2021). Operation Model - Unique Identification Authority of India | Government ofIndia. Retrieved 12 April 2021, from https://uidai.gov.in/ecosystem/authentication-ecosystem/operation-model.html

26. Effiong, M. (2020). *A FRAMEWORK FOR THE ADOPTION OF BLOCKCHAIN TECHNOLOGY IN ACADEMIC CERTIFICATE-VERIFICATION SYSTEMS: A CASE STUDY OF NIGERIA*.

EKYC Landscape in Austria and Germany. (2020, October 3). Fintech Schweiz Digital Finance News - FintechNewsCH. https://fintechnews.ch/fintechgermany/ekyc-landscape-in-austria-and-germany/36650/

27. European Commission. (2019). Blockchain Now and Tomorrow. In European Commission. Science for Policy report by the Joint Research Centre (JRC). https://doi.org/10.2760/29919

28. Feng, Q., He, D., Zeadally, S., Khan, M.K., Kumar, N., 2018. Review: A survey on privacy protection in Blockchain system. J. Netw. Comput. Appl. 126, 45–58. https://doi.org/10.1016/j.jnca.2018.10.020.

29. Fernández-Caramés, T., & Fraga-Lamas, P. (2018). A Review on the Use of Blockchain for the Internet of Things. IEEE Access, 6, 32979–33001. https://doi.org/10.1109/ACCESS.2018.2842685

Four major banks and Isabel Group join forces to streamline business services with KUBE. (2020, January 22).

30. Isabel Group. https://www.isabelgroup.eu/en/four-major-banks-and-isabel-group- join-forces-to-streamline-business-services-with-kube/

Appendices

Appendix 1: Interview Questions

Section 1: Introduction

1. Kindly provide a brief introduction about yourself.

2. What is your position in this unit?

3. For how long have you been in your position?

Section 2: Question about the processes followed in the existing system of KYC process?

1. How do you obtain or receive information for the purpose of CDD/ODD?

2. How do you make contacts with the client?

3. Can you complete the ODD/CDD even when you fail to validate the document? Yes or No. Why?

4. How do you access other databases? What kind of database do you use? Are they reliable?

Section 3: Question about automation process

1. What can you say about your computer skill? Basic, average or highly skilled.

2. What type of automation process do you use at present?

3. What is your understanding about centralized database sharing?

4. Do you feel that centralized database sharing will help in improving the KYC process?

Section 4: Issues on difficulties encountered in the present system

1. Which challenges are emphasized by you about the present system of verification and data sharing?

2. What are your strategies for addressing these challenges in the present system?

3. Which aspect of the present system do you feel needs improvement for better effectiveness?

4. Do you think that the present system is effective and efficient? What criteria do you use to determine its effectiveness?

5. Are your customers usually satisfied with the present system?

A. Yes, what are the indicators that show their satisfaction?

B. No, what causes their dissatisfaction?

Section 5: Knowing respondents' understanding of the blockchain

1. How much do you understand about the blockchain technology? Do you believe in this technology? (In case the respondent does not know about the blockchain, I would make an attempt to explain about it briefly, after which further discussion will follow.)

2. Will the implementation of the blockchain be advantageous to the document and identity verification in your department?

3. Can there be any significant risks in operational or legal terms of applying blockchain in the present system?

4. How do you think the challenges may be dealt with?

Section 6: Questions regarding issues with adoption.

1. How do you feel about issues with various legal requirements for other countries?

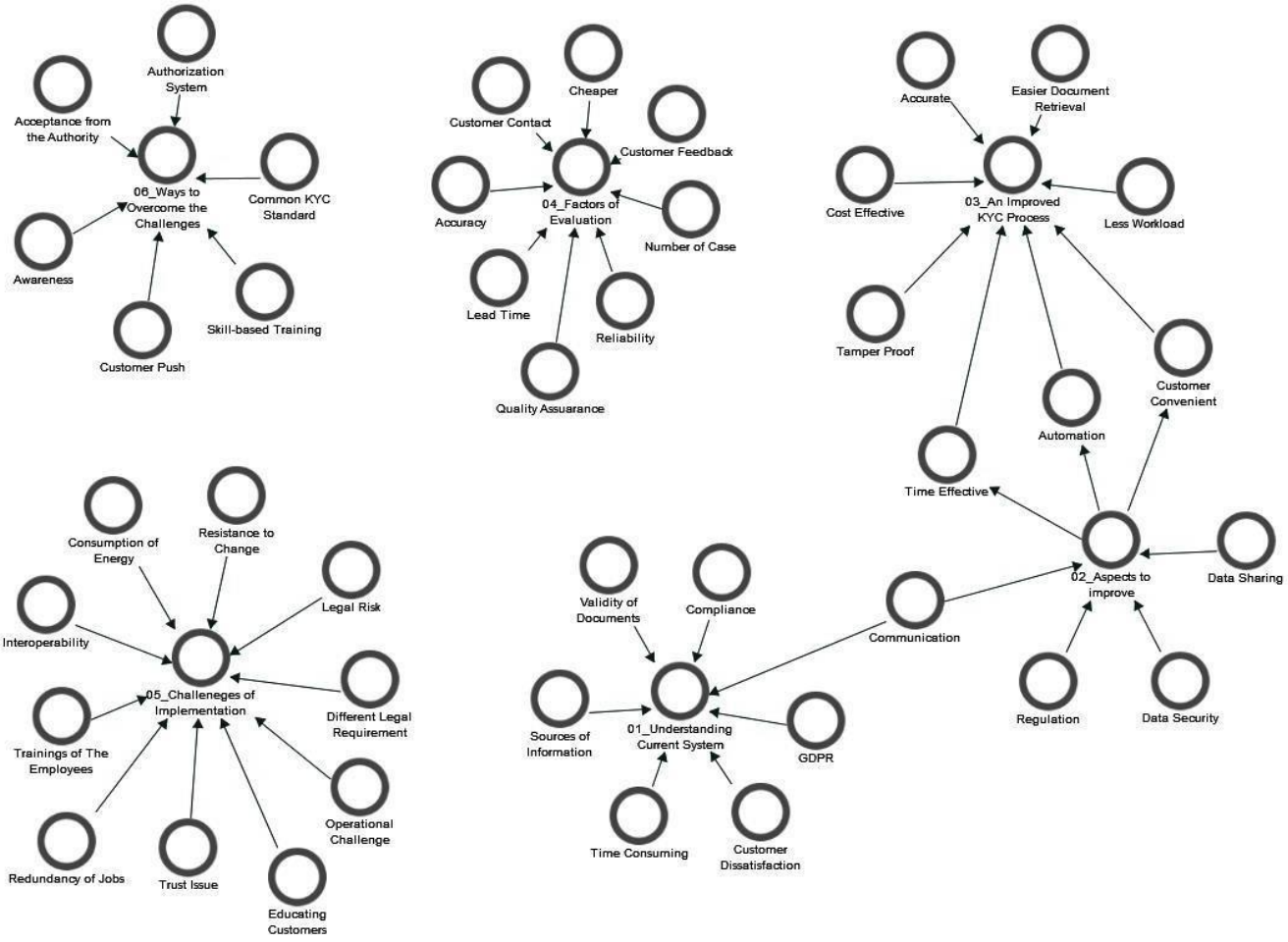
2. Do you think Internal QA and Government Audit will become less attentive when verifying the truthfulness of the data provided?

3. Do you think that banks will exchange their data with each other? If yes, would there be any problem with interoperability? If not, explain why.

4. Will you be at ease with the new procedure?

5. Do you think that your function in the existing system will be impacted because of the shift to blockchain technology?

Appendix 2: Thematic Plotting of Code Categories



Appendix 3 – Non-exclusive license for reproduction and publication of a graduation thesis

Eyob Tesfaye

1. Non-exclusive license for the reproduction of my thesis "BLOCKCHAIN FRAMEWORK TO STRENGTH KNOW YOUR CUSTOMER (KYC) PROCESS DATA TRANSPARENCY (INCASE OF COOPERATIVE BANK OF OROMIA)" By the Addis Ababa University, School of Commerce under the terms of its own license (free license).

1.1. Reproduction of the graduation thesis to make it available for preservation and electronic publishing, including reproduction in the digital collection of the library of Addis Ababa University, School of Commerce up to expiration of the term of copyright protection;

1.2. Publication of the thesis on the website of Addis Ababa University, School of Commerce, including reproduction in the digital collection of the library of Addis Ababa University up to expiration of the term of copyright protection.

2. The author is aware that he/she retains the rights set forth in paragraph 1 of this non-exclusive license.

3. I confirm that granting non-exclusive license will not violate the intellectual property rights of other parties, rights established by the Personal Data Protection Act or other legal acts.