TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technologies

Hafizul Islam
194293IVGM

ADOPTION OF BLOCKCHAIN IN KNOW YOUR CUSTOMER (KYC) VERIFICATION PROCESS: A THEMATIC ANALYSIS ON EUROPEAN BANKING INDUSTRY

Master's thesis

Supervisor: Alexander Horst Norta

PhD

Associate Professor

Tallinn 2021

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia teaduskond

Hafizul Islam
194295IVGM

BLOKIAHELA KASUTUSELEVÕTT KONTROLLIPROTSESSIS (TUNNE OMA KLIENTI) (KYC): TEMAATILINE ANALÜÜS EUROOPA PANGANDUSSEKTORI KOHTA

Magistritöö

Juhendaja:	Alexander Horst Norta
	PhD
	Associate Professor

Author’s declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Hafizul Islam

10.05.2021

Abstract

KYC operations have matured from an elementary process into a rigorous and meticulous practice supervised by the regulatory authority of each country. The manual paper-based KYC process and digital KYC process both are not cheap, swift, and client-friendly; to some extent, major financial institutions expend close to $500 million for the KYC process. KYC regulations are becoming stricter all over the world so, this expenditure might increase gradually. The core objective of the paper was to figure out how the blockchain adoption might improve the KYC verification process by making it more secure, cheaper, faster, and convenient. A thematic analysis was done based on the European banking and Fintech industry using expert interviews and previous study reviews. The study revealed that aspects like communication, source of information, the validity of the document, compliance, GDPR, time consumption, customer dissatisfaction, heavy workload, inaccuracy, long document retrieval process, and lack of automation make the current process obsolete and not business-friendly. The study showed how an improved blockchain-based KYC verification process could remove all the constraints of the current system. The hindrances of the implementation like legal risk, resistance to change, trust issues, educating customers, training of the employees, redundancy of the jobs, consumption of energy were also identified and discussed. Major ways to overcome the challenges were stated in the result part as well. Finally, several recommendations regarding the adoption process were provided like, the use of automation, common KYC standard, running pilot project, collaboration among the banks, educating customers and employees, and research & development.

Keywords: KYC, Compliance, European Banks, Blockchain, Smart Contract, Distributed Ledger Technology

This thesis is written in English and is 92 pages long, including 5 chapters, 6 figures and 4 tables.

Acknowledgment

Before starting the thesis, I thought it was going to be a piece of cake, but here I am, writing my acknowledgment at 3 AM on the submission date!

Greatest thanks to the Almighty. I would want to thank my family first for the supports they have provided me throughout the years. A sincere appreciation to my supervisor Alexandar Norta for his kind guidance regularly; his prompt responses really amazed me. Friends from my student dorm Sidiisaba, will always be in my heart; the way we worked together for the thesis was remarkable. Thanks to Momin Reja and Umme Sayma Bushra for continuously treating me with food during the thesis time. The support of my E-Governance classmates, whom I am proud to call family, has been tremendous throughout the journey though I wish I could have enjoyed my university life more (thanks to Covid 19). Appreciation to my colleagues from the workplace who shared their insight to enrich my thesis. Last but not least, I am indebted to Nuzhat Naeema, who was always there for me when I needed the motivation and support for this enormous work.

Hafizul Islam
10.05.2021
Tallinn

List of abbreviations and terms

AML	Anti-Money Laundering
API	Application Programming Interface
CCAF	Cambridge Centre for Alternative Finance
CDD	Customer Due Diligence
CFT	Combating the Financing of Terrorism
DOI	Diffusion of innovations
DLT	Distributed Ledger Technology
EDD	Enhanced Due Diligence
Fintech	Financial Technology
eIDAS	electronic IDentification, Authentication and trust Services
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
GDPR	General Data Protection Regulation
KYC	Know Your Customer
NBFI	Non-Bank Financial Institution
OCR	Optical Character Recognition
ODD	Ongoing Due Diligence
RegTech	Regulatory Technology
RM	Relationship Manager
TPS	Transaction Per Second
UN	United Nation

Table of contents

List of figures

List of tables

1 Introduction

Back in the 80s or 90s, it was facile to launder or send money, even by regulated banks. Banks or Non-Bank Financial Institutions (NBFIs) did not need deep authentication of the clients or the purpose of the fund. As a result of the absence of this regulatory framework, criminals around the globe took the benefit of the loophole and financed all types of terrorism, and finally, 9/11 happened in the USA. The world changed after 9/11, and like many sectors, major restrictions and regulations were introduced in response to that horrific incident. KYC or know your customer is one of them. KYC regulations were implemented as a part of the Patriot act signed in 2001 in the USA; later, it was introduced all over the world. Banks, NBFI, Fintech, or any kind of financial institution (FIs) are obliged to conduct KYC procedures in order to operate with the compliance of the USA and the European Union. FIs are compelled to know the person or the business in detail with whom they are commencing the commercial partnership to eradicate the possibility of involvement of the clients with any types of illegal or illicit activities. Know Your Customer (KYC) has been emerged to encounter this need of the FIs, and it has become an essential part of the overall FIs processes.

“Blockchain is considered by many to be a disruptive core technology” (Xu et al., 2019). In 2008, Satoshi Nakamoto, an anonymous person/group who invented bitcoin, illustrated how the technology of blockchain, a distributed ledger that works on a peer-to-peer basis structure, could be of use in addressing the aspects of transaction maintenance and spending double time (Casino et al., 2019). Bitcoin organizes transactions into a constrained-size structure that is called block, all of which share the same timestamp. The nodes of the network usually connect the blocks in the chronological order where all the blocks contain the hash values of their immediate previous blocks to create a chain of blocks (Crosby et al., 2016). Blockchain is not an executable program but is a storage of transactions. For KYC verification, a smart contract would be the program needed for the execution of verification. For this research paper, the case study methodology has been selected. Previously, a good number of design science and case study-based research have been done. The main purpose of the study would be to find a framework of implementation, advantages, and challenges of blockchain in KYC verification by analyzing the case. The audiences who will be benefitted from the study are financial institutions and blockchain specialists. Especially, financial institutions would be more interested in investing their fund and effort in this technology if it could be used to lessen the compliance costs.

1.1 Problem Statement

Customer Due Diligence (CDD) / Enhanced Due Diligence (EDD), Ongoing Due Diligence (ODD) both have matured from an elementary process into a rigorous and meticulous practice supervised by the regulatory authority of each country. The FATF (Financial Action Task Force) is an organization that is inter-governmental with the task of AML and terrorist financing. It sets the standards internationally for KYC (Parra-Moyano et al., 2019). KYC process starts with relevant documents receiving, and from that, the necessary data are retrieved. A lot of fintechs have moved to AI-powered documentation system, but most of the bank still depend on the paper-based processes due to auditing. For personal accounts, the due diligence process might be done only one time, but for a business account, due diligence is done several times based on the risk severity of the business client. For example, oil, gold, e-commerce are high-risk businesses, whereas government offices (Army, Navy) are low-risk businesses. After the submission of all documents, officials of the bank check and verify all the documents. Sometimes, for high-risk business, they perform enhanced due diligence that is the investigation of the background of the business. After verifying all the information, if the business or person is a compliant candidate, an account might be opened. This is a costly and sometimes long process which has to be done in regular interval for risky clients. And most importantly, every bank finishes this verification on its own. So, if someone opens an account in three banks, all three need to perform KYC verification.

The manual paper-based KYC process, digital KYC process, both are not cheap and swift. To some extent, major FIs expend close to $500 million for KYC process, enhanced due diligence (EDD), and customer due diligence (CDD) annually while world's top 10% of the FIs expend $100 million per year (Callahan, 2018). Fines imposed on financial institutions for violating the regulations of AML and KYC would add to this expense (Moyano & Ross, 2017). Since the partnership establishment is lengthy, the starting point frequently gets delayed with the larger corporation. Therefore, companies need to look at all their affiliated corporations and operationally autonomous subsidiaries before they are accepted for KYC certification. According to a survey conducted by Thompson Reuters in 2016, 89 percent of users did not have a positive KYC experience. In order to perform On-going Due Diligence (ODD), customers need to be contacted again according to FATF rules after 1 or 3 or 5 years, depending on the risk level to receive their information. This task also costs a significant amount of money to the banks, and it is a burden to ensure a smooth customer experience.

Forrester Consulting's analysis (Legget, 2012) noted that poor data quality was a third of the consumer experience issues standing in the way of smooth customer onboarding, where they found it in the top three ranks alongside cost and complexity. Knowledge also is stored in silos and is much more difficult to process when it is found on various channels. This helps the retention of consumers in this time period, in particular, because customers are already aware of the operation. In yet another Forrester study in 2014, it was found that more than 64% of firms lost deals and sales due to issues in the onboarding phase, and approximately 20% of clients reported having to abandon up to 50% of their new opportunities as a result.

Since several companies are using an improved approach to KYC, this number is now likely to be smaller but static processes like corporations have an effect on the onboarding process clients must consider onboarding as an opportunity rather than a routine activity. Customer satisfaction may not be over-emphasized in the modern age; it is imperative when customers have the impression that they have alternatives. Customer onboarding must be seamless; it may not be done by using manual KYC procedures. According to Reuters, the onboarding time has increased over the past year. Registrations of new customers were taking about 24 days by 2015 to rise by 18% in 2016. It's easy to see how much of a hassle this will be for customers who wait on hold before being transferred. The company will be incurring increased operational costs, too, as the number of necessary onboarding activities is rising (Thomson Reuters, 2017).

For organizations, particularly those of large size, this is a difficult issue. Most companies aren't making the KYC implementation simple for end-to-end customer onboarding. They need a robust, continuously updated KYC platform to assist with customer lifecycle management. It is worth mentioning that automating the client onboarding process gobbles up much of all the problems that companies face.

1.2 Research Objective

This research here aims to describe how KYC is completed in order to understand its challenges, difficulties, and problem and then create a structure for its improvements by employing blockchain. Below mentioned objectives have been outlined:

- Describing the current KYC verification process for European banks and fintech.
- Identifying factors that prevent the effectiveness, efficiency, and convenience of the current process.
- Providing a substantial overview of how blockchain could bring positive changes for KYC verification.
- Figuring out the challenges of implementation of blockchain-based process.
- Suggesting means of overcoming the challenges of the implementation of blockchain.
- Construct a recommendation list to adopt the blockchain-based KYC verification process.

Understanding how technology can be used to develop the system requires looking into the causes of the problems listed in Section 1.1. There would be no justification for adopting an alternative approach if there is insufficient understanding. As a result, blockchain technology would improve KYC verification process by saving time, lowering costs, and streamlining the process. Furthermore, the variables that could hinder the mechanism must be investigated and correctly understood before possible improvements could be considered. Finally, we should understand the stakeholders' perspectives on how technology would affect their responsibilities. An approach like this is critical to the technology's growth and reception.

1.3 Context

To avoid dealing with clients who participate in any of the above criminal activities, regulators require financial institutions to onboard their customers before participating in any transaction with them. The KYC procedure entails the consumer and financial institutions exchanging information. To search for illegal activity and "politically exposed individuals," the procedure involves gathering basic identification information from all beneficiaries. Risk management for new client onboarding, transaction monitoring, and relevant customer policies for banks are also part of the process (Parra Moyano & Ross, 2017). Knowing who they are dealing with is one of the most important roles of FIs and NBFIs. These financial institutions perform the KYC (Know Your Customer) process for having a sense of authenticity and security. The legitimacy of the counterparty is ensured through KYC verification.

A business process model has been drawn based on the current onboarding (CDD, EDD) and ongoing due diligence (ODD) process. It illustrates the interaction between counterparties (Specialist, Relationship Managers, and Customers). Bizagi has been used to draw the BPMN. A BPMN diagram is a graphical representation of a process's activities from start to finish. It is used to visually communicate a basic interpretation of complex and technical operations. A start event initiates a process that results in the first intervention, and it takes us through a series of events to the end event, that marks the end of all potential activity sequences and the process's target. A sequence flow is split into many directions by the inclusive gateway. Figure 1 and Figure 2 describes the KYC verification process for CDD and ODD based on the above-mentioned understanding of BPMN.

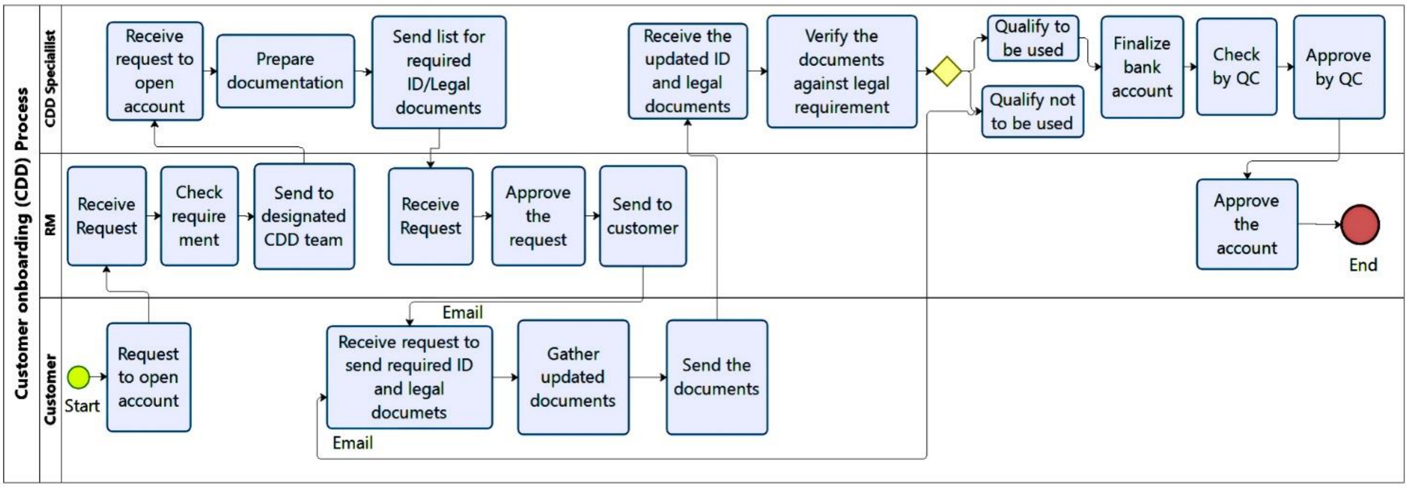


Figure 1: KYC Process for Customer onboarding (CDD). (Source: Author)

For onboarding (CDD), the customer (Personal/Business) initiates the process by contacting the relationship managers. The relationship managers receive the request and analyze the customer requirement. The latter commences with sending the account opening request to KYC specialists, where they prepare the required documentation (e.g., KYC form). Every KYC form requires several documents (for business account) like IDs (Passport, National ID, Address proof) of beneficial owners / authorized representative, article of association, certificate of incorporation, ownership information, and so on.

Usually, these are provided by the customer, but these documents are provided after they have been asked to provide. The request to provide the updated document is conveyed by the relationship managers. After receiving the document, KYC specialists start to verify the documents, and if they are not legally compliant, the request to resubmit the documents is sent back to the customer again. Finally, after receiving all the necessary documents, the KYC specialist is able to finish CDD/EDD and submit the case for QC (Quality Check). If the case passes the quality check, it is sent to RM (Relationship Managers) for final approval. This is how the process ends.

For the ODD, the process is initiated by the KYC specialist, and later they communicate with the Relationship Managers for necessary ID documents or legal documents. RM initiates communication with the customers and instructs the customer to submit the required documents within the deadline. After receiving and validating the documents, the KYC specialists finalize the case and send it to the QC. As soon as QC approves the case, the cases are sent to RM for final approval.

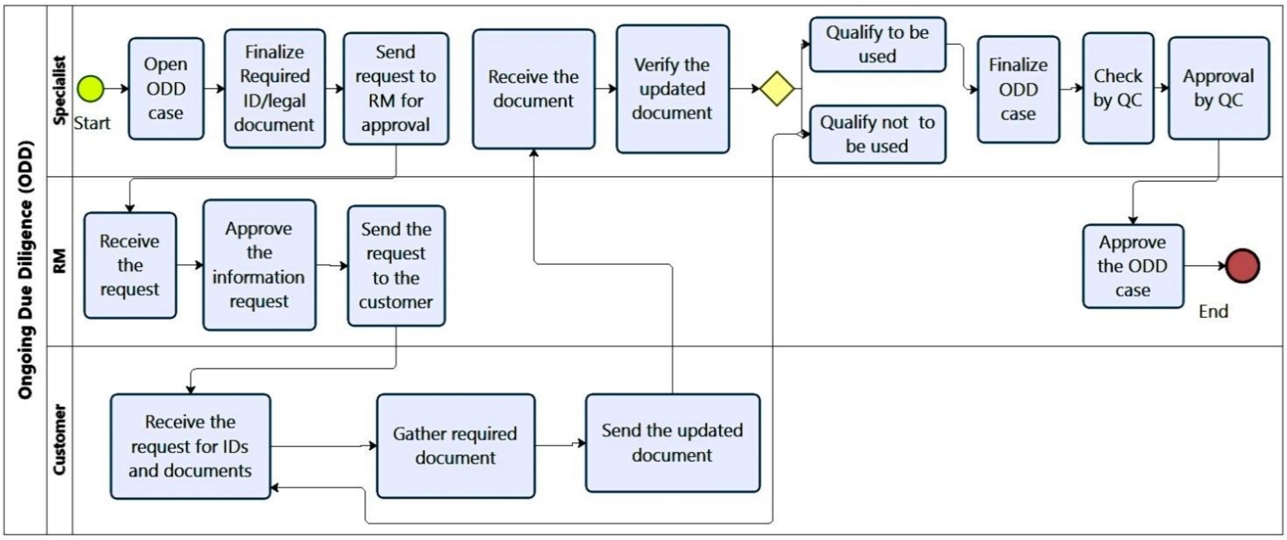

Ongoing Due Diligence (ODD)
Specialist
RM
Customer
Start
Open ODD case
Finalize Required ID/legal document
Send request to RM for approval
Receive the document
Verify the updated document
Qualify to be used
Qualify not to be used
Finalize ODD case
Check by QC
Approval by QC
Receive the request
Approve the information request
Send the request to the customer
Approve the ODD case
End
Receive the request for IDs and documents
Gather required document
Send the updated document

Figure 2: KYC Process for ongoing due diligence (ODD). (Source: Author)

Both of the processes require a long lead time and workforce. The customer is reluctant to send the document most of the time, especially for ODD. Asking the same thing over and over again hampers smooth customer relationship as well.

To open an account with bank X, one must exchange documents and complete the bank's Know Your Customer (KYC) procedure. Bank X will check his documents after obtaining them, and he will be able to open an account with them. However, if he intends to collaborate with additional banks, for example, bank Y and bank Z, he must share his documents and finish the KYC verification process again with the respective banks Y and Z. It takes time to perform several validations and result in an unnecessarily high cost of KYC validation (Brew, 2020).

Information sharing among the banks and FIs could provide a solution that would make this process more user-friendly and cheaper. Document sharing among business and government entities to smooth the process and reduce cost is becoming all over the world. For example, 71% of the total documents (45 million) among 400 government authorities, city authorities, and corporate authorities were shared by X-Road in Estonia in 2014 (Draheim et al., 2016). KYC documents could be shared between banks and fintechs, but that might not fulfill the criteria of recent updated documents. In this case, blockchain technology could be able to offer the alternative process and act as a centralized point of validity. A consumer/business would only have to go through the KYC phase once after blockchain is implemented. This information and verification of KYC will be stored on the blockchain, and the client would be able to share the outcomes of the KYC verification with FIs/NBFIs with whom the client intends to collaborate in the future.

A distributed ledger technology could be loosely described as blockchain technology (DLT). The distributed ledger technology encourages the decentralized recording of transactions, asset monitoring, and asset sharing within a network (Manav Gupta, 2017). Both tangible and intangible assets are referred to as assets. This implies that blockchain can be used to track something of value. A blockchain is a decentralized ledger that is constructed of blocks that are sequentially linked together. Holbl et al. (2018) mentioned that blockchain is a means of securely storing and distributing data among transacting parties, with complete transparency and no centralized control. To promote its inherent immutability and adaptability, blockchain's functionality draws on both of these fields. This protects digital assets and decentralizes the network of participants. This protects digital assets and decentralizes the network of participants. This protects digital assets and decentralizes the whole network (Sultan et al., 2018).

1.4 Summary

The chapter has briefly discussed the significance of KYC verification, how time-consuming and costly it is, and how blockchain technology can effectively solve this problem. Concerns about the current framework were addressed. The goals were stated, and the context in which the concepts in the following chapters should be understood was defined.

2 Related Work

To establish the foundation for the ensuing investigations, understanding of related studies is critical. Such expertise fosters awareness of what has already been accomplished as well as the knowledge gap that current research can address. This chapter aims to provide context studies as well as to delve further into the reviews that are specifically relevant to the paper's goals. This context research is divided into four parts. The first section of this thesis, Section 2.1, would outline the basic studies fundamental to this case, the second section being Section 2.2, would discuss the technology of blockchain, and the last section that is Section 2.3, would discuss the theoretical framework to create a base for the study.

2.1 Earlier Studies

Previous studies will discuss the topics around the identity verification process of Know-Your-Customer (KYC) Process in the first segment as verification exists inside the KYC ecosystem and blockchain technology in the second segment as the whole framework will be based on the impact of this technology on the KYC process. The subjects covered in the first segment include the previous studies and fundamentals of identity verification. On the other hand, KYC, from analogue to digital to eKYC and lastly to eIDAS, is part of the following segment of this section of earlier studies which discusses the main technology of KYC with its regulatory and compliance concerns. The concept, components, operation, types, function of blockchain technology and its suitability to Know-Your-Customer verification are discussed in the final segment.

2.1.1 Identity Verification

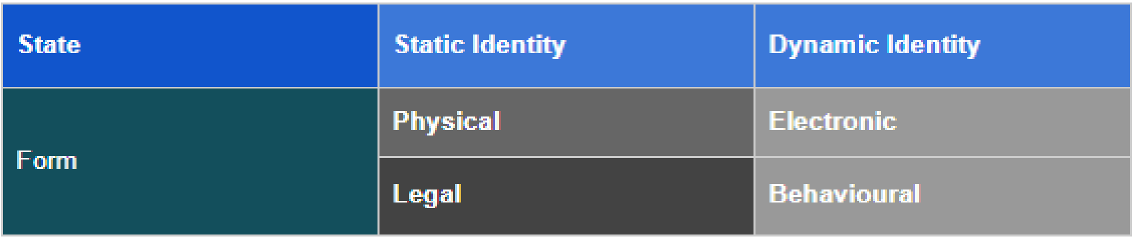
In the last three decades, technological development is both challenging and fast-paced. This is seen especially around the identity verification of people. Analogue (paper-based), digitalized (ID scanning), and digital (such as online footprints) could be the form of verification in the present time. Though they are not globally acceptable, these are mostly used for identification purposes (for instance accessing the accounts of banks or social media). The internet has a feature of securing anonymity, which does not necessarily fail, and this conflicts directly with different requirements for client identification (Arner, Zetzsche, Buckley & Barberis, 2018). A digitized form of KYC, or a digital accumulation of a person's online footprint, or any identity is converted to the electronic form of identity in both digitized way and digital way. Entities often collect and validate identities like social media credentials regularly and exchange the information among other entities for instances like bank account maintenance. Here is the table below that represents the four kinds of identity that have been familiar in the industry:

Table 1: Types of Identity (Source: Author)

Identity Type	Example
1. Physical	Fingerprint, IRIS, or DNA.
2. Document	Passports, national ID cards, and driver's licenses can serve as proof of legal identification.
3. Electronic	Accounts from social media like Facebook, Instagram etc.
4. Behavioural	Pattern of one's talking, walking, or communicating.

Below is the representation of the topology of identities:

Table 2: Topology of Identity (Source: Author)



State	Static Identity	Dynamic Identity
Form	Physical	Electronic
	Legal	Behavioural

2.1.2 Forms of Identification

The idea of identity has developed over time, much like services in the financial sector have altered dramatically by the impacts of technological adoption since 1970. By the time, it has been noticed that there are evolutions in the forms of identity and the evolution continued from the analogue form to the digitized form ("A brief history of the passport", 2021).

- **Analogue Form**: Static identity has been used to prove an individual's identity in the past usually in the banks. Analogue forms of identity generally include any kind of physical data record or any type of physical marker like fingerprint or footprint. These analogues usually used and utilized for determining a certain identity of a person.

- **Digitized Form:** Identities that are digitized are usually as same as the types of the analogue identities but the only difference is in the storing format that is digital. These digital forms of identities could be more easily used in different aspects like bank account opening by using various analogue type of documents online in the scanned form. This transition towards the new types of digital identity is the next step in the evolution in the types of identities where the identity definition is widened to integrate and incorporate all kinds of behavioural traits of a person in the identity to distinguish the person’s unique personality. International Bar Association Legal Practice Division Working Group (2015) stated that these information can be collected and analysed easily from the social media accounts of the users and from the patterns of browsing internet and interests in different areas of a person.

2.1.3 Traditional Method of KYC Verification

On an occasion like opening an account for a client, the bank or the financial institution is provided with documents of the identity of the client, such as a passport, and only then the financial-service institution conducts the legal KYC process. Following that, as banks gain a better understanding of their customers through transactional data, they can broaden their understanding by collecting payment, insurance, and investment data. (Arner, Zetzsche, Buckley & Barberis, 2018) These touch points are the most important ways for the bank to learn more about their customers. Although the passport contains information of a person's identity, transaction data aids in the development of the person's profile, which includes creditworthiness – an identity that is more than just identification.

2.1.4 Non-Traditional KYC

Banks are seen as being at a distinct disadvantage in comparison to other firms, such as FinTechs or TechFins (Arner, Barberis, & Buckley, 2016), despite the fact that the technology they use is cutting-edge. These businesses collect both behavioural and general business data, as well as employ more reliable authentication methods. A datafied company, for example, might use an in-built gyroscope to record the pattern of a person's way of holding a phone or picking it up on ear, or the person's type and frequency of entering a password on the phone. These objects may be used as a second authentication factor.

2.1.5 Traditional KYC vs Non-Traditional KYC

When compared to tech companies, financial institutions or banks are at stake in terms of ensuring their customers' clear understanding unless they have an account and frequently conduct transactions (Arner, Barberis & Buckley 2016). The average person, for example, usually checks up on their bank account's status online less than even ten times in every month compared against the hundredth of times of check-ups on any social media account or thousandth of times of sending messages over any messenger app within the same period of time. Lesser documents or information always leads to poorly informed decisions in case of loan provisions. This part is usually referred to in the industry as having a "thin credit file," which would limit the ability of the bank to assess its client's credit profile and thus would also limit the ability of the bank to sell any financial product like loans.

2.1.6 Analogue to Digital Transformation

Legal identity is something that others can see and that depicts the details of someone and distinguishes that person’s personalities. On the other hand, the identities that are physical or behavioural are internal and generally define the identity of a person. An individual's electronic identity is not a natural characteristic, but it is becoming more internalized as people are spending more time than usual online and kind of revealing a complete image of their personalities and interests of choices. During resolving the identity challenge found in financial markets, most of the evolution of identity occurred in the context of these two approaches:

- **Adoption of Digitization:** Developed markets will almost certainly digitize existing infrastructure, whereas emerging markets may leapfrog and adopt full digital identities (Arner, Barberis & Buckley 2016). However, from a wide perspective (political, legal, personal, and technological), the course of least resistance is to emphasize on the digitization of analogue identities.
- **Copyright to the Data:** This second move, on the other hand, will necessitate a broad debate to require privacy standards that are recreated thoughtfully, and to find a consensus on established concepts worldwide like sovereignty of data (Weigegnd, 2017), and to create a new mechanism that would know how to use the data rightfully in an economy (Lanier, 2014). Such an undertaking could be unlikely in the current political environment.

2.1.7 Digital Identification

Financial technology, particularly "regulatory technology" (RegTech) (Arner, Barberis, & Buckley, 2017), offers the chances to the market and the economy to reimagine the existing structures, also to develop a structural form that is required to have a balanced integrity in the market, inclusion in finance, and finally growth in the economy, adhering to the financial standards set internationally by the FATF, FSB, Basel Committee and UN.

2.1.8 Identity Verification in Finance

As Arner, Zetzsche, Buckley & Barberis (2018) said, customer identity verification and ongoing “know your customer” (KYC) due diligence are critical for consumer integrity because of their help for preserving the faith in the system of finance as well as for reducing the risk of access in the services of finance by the financial terrorists. Based on internationally negotiated approaches, rules for the abovementioned factors are expressed broadly in a variety of AML, CDD, and CFT standards. Furthermore, CDD is critical to understanding consumer needs and delivering adequate financial services, a feature that is often summarized under the umbrella of suitability.

2.1.9 Current Manual Structure of KYC Verification

According to Parra Moyano & Ross (2017), the protocols in the KYC verification generally includes the feature of exchanging papers between the client and the FI where the client is willing to cooperate. The protocol involves collecting the identity documents that are basic, from the clients for checking the criminal activities and political involvement of the people. The process usually begins only when a client plans to begin a journey with an FI in a new program. The terms of the contracts are agreed upon chronologically between the client and the FI. The KYC verification then starts to process once the client provides all the necessary documents to the FI. The FI would review the documents and then create an internal document for the FI that would additionally serve as the certificate of approval to the regulators, that would confirm the KYC verification of that client showing the result of being either validated or rejected. This would also confirm that the procedure of KYC verification was conducted correctly. The same process is repeated if the consumer wishes to join in another program with another FI. The current method generates costs every time the process of KYC verification occurs and every time the client is willing to form a new relationship with an FI. Figure 2 shows an example of what happens when a client wants to work with three FIs at a time. The following case of the example represents the occurrence of additional cost that is three times the cost of the single service that includes the exchange of the necessary documents and the core KYC verification.

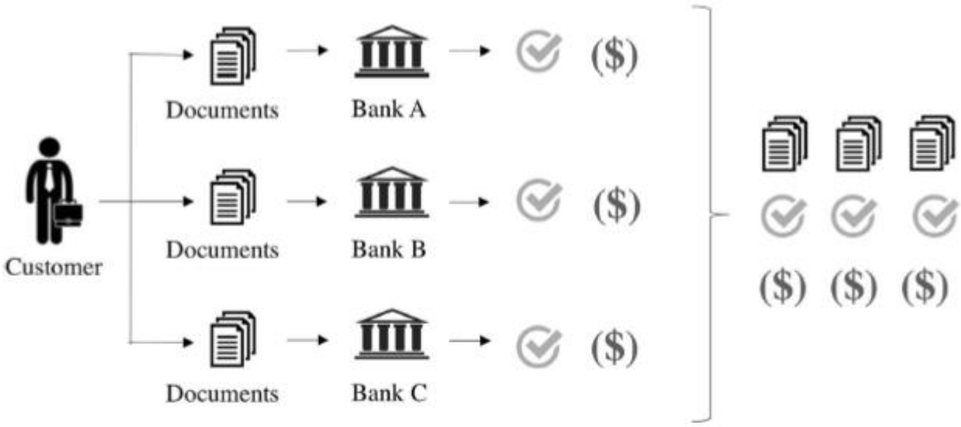


Figure 3: Current KYC system and cost structure (Parra Moyano & Ross, 2017)

2.1.10 Integrating Electronic Identification in the EU

In 2014, European regulators adopted the regulation (eIDASR) for electronic Identification, Authentication, and trust Services (eIDAS) for the reduction of expenses of online transactions, be it in the e-Commerce or in the financial services, as well as for having the competition increased in the market (Dumortier, 2016). This eIDASR is designed to ensure that the clients and the companies would be able to use their national e-IDs for accessing the public services in any country of EU that avail the usage of e-IDs. The cases of usages include the filing of tax returns, enrolment in a foreign university, remote bank-account opening, company creation in a member state, bidding on the tenders, and the authentication of internet payment.

2.1.11 Electronic Identification in KYC of European Banks

The European Commission's Consumer Financial Services Action Plan (2017) pledged that the commission would work in and with the private sector for making the users understand the use of electronic identification better to verify the identities of the users aiming more better products and more open choices for the clients in Europe. The Commission designed the action plan to allow the application of cross-border electronic identification and portability of KYC based on eIDASR to allow the banks to identify the customers digitally. European Commission (2017) stated that the electronic identity would allow the clients to open a bank account online, maintaining the stringent criteria for KYC verification or CDD tasks.

2.1.12 Challenges in Existing KYC Methods

The current method of client onboarding process is hectic and time-consuming that needs to satisfy the regulatory demands of CDD, presenting a major challenge for FIs, tech firms that provide financial services, and FinTech institutions. CDD data is only useful if it (1) is accurate, (2) comes from a reliable source, and (3) is current (Arner, Buckley & Zetzsche, 2016). More Challenges being:

- **Time Consuming:** FIs should intensely focus and contribute ample amount of time as well as funds to conduct the core KYC verification of their customers' records, leading to very costly transactions and inconvenient services for the customers.
- **Inefficient:** This is particularly inefficient in the case of Luxembourg, which serves as an international cross-border center.
- **Mutual investment schemes**: The same client is often reviewed by many Luxembourg organizations at the same time and later when the client would purchase various units of Luxembourg-based investment funds.
- **Expensive, Unreliable, and Inconvenient:** The findings from the data analytics of the regulatory agencies and other organizations are the most valuable while applied to a large group of data, in terms of overall business integrity. As a result, existing systems are not only costly, inefficient, and inconvenient, but they also fail to deter fraudulent in the financial system. Buckley & Stanley, 2016).

2.1.13 Factors in Current KYC Regulations

A Thomson Reuters survey received responses from nearly 800 financial institutions (2016) in responses to the effects of global shifts on KYC regulations. In the survey, one of their corporate clients revealed the idea that 89% of them were not pleased with their KYC experiences, and 13% of them had to change their KYC provider (*Thomson Reuters 2017 Global KYC Surveys Attest to Even Greater Compliance Pain Points,* 2017).

- **Regulatory and Legislative Reform**: According to the majority, a top KYC hurdle is ongoing regulatory reform. 87 percent of the banks and 75 percent of the investment managers conclude the change in the regulatory and legislative system very if not the most important factor in their know your customer processes

(*Thomson Reuters 2017 Global KYC Surveys Attest to Even Greater Compliance Pain Points,* 2017).

- **Constantly Evolving KYC laws:** It is posing problems for both the financial institutions as well as for the customers. Almost 70 percent of the FIs agree with the fact that majority of the customers are diligent in case of disclosing the adjustment materials for their KYC statuses, like for the change in the beneficial ownership. But almost a 30 percent of respondents from the industrial sector revealed that they would keep the FIs informed on a regular basis (*Thomson Reuters 2017 Global KYC Surveys Attest to Even Greater Compliance Pain Points,* 2017).

- **Interactions by Regulators** The interaction level with the entities by regulators has been increased in cases of KYC and CDD, according to a substantial 69 % of banks who responded. 70% of the executives from C-suite at FIs replied that they had spent more than usual amount of time and attention on KYC improvements in the previous year (*Thomson Reuters 2017 Global KYC Surveys Attest to Even Greater Compliance Pain Points*, 2017).

2.1.14 Distributed Ledger Technology (DLT) in KYC Verification

The e-KYC solution provides reliability, cost savings, and enhanced confidence through increased transparency and throughput to replace existing KYC, which is redundant, time-consuming, and expensive. The prerequisites of banks' Know-Your-Client (KYC) is labor and cost-intensive; Thus, Hanbar et al. (2020) proposed e-KYC to improve productivity and allow Anti-Money Laundering (AML) alerts, which KYC might not provide due to its labor and cost-intensive nature. The main tools for allowing e-KYC are the technology of distributed ledger and smart contracts, according to the study. Customers' certificates of approval and e-signed documents for the certificates of transactions are validated by the smart contract, ensuring that this data is not transmitted across the network without their consent.

2.1.15 KYC Optimization for Improved Customers' Experience

The aim of the e-KYC solution proposed by H. Hanbar et al. (2020) is to improve the e-KYC process with DLT and smart contracts to meet the objectives; (1) *Relationship* *anonymity*: must maintain confidential relations between the customer and the bank. However, when exchanging data from one bank to another, the identity of the bank should be secret. For the sharing of data between banks, the customer's consent is needed. (2) *KYC cost reduction*: Both banks that intend to carry out a KYC verification for a given customer must share the expenditure of the KYC proceeding. (3) *Creditability*: Each client must have a lending standard that helps banks create consumer trust. (4) *Fast flow rate and low latency*: a high number of transactions with low latency should be carried out in the given period. H. Hanbar et al. (2020) used a permitted blockchain-Hyperledger fabric. Various organizations must interact through smart contracts, and customers must connect through the customer portal to the network, which is their entrance point. When a customer signs up for the customer portal, a single but unique identification number is provided by the regulators or the identity provider (e.g., Certification authority) to the customer. Banks use APIs for their websites to connect with customers.

2.1.16 Factors Measuring the Performance of a DLT based e-KYC Process

H. Hanbar et al. (2020) created a prototype using *Hyperledger Fabric* to test the efficiency of the DLT based e-KYC solution. Hyperledger Fabric is a permissioned technology of the distributed ledger (DLT) with the ability of accessing that could be utilized in a variety of applications including banking, healthcare, and supply chain management. Smart contracts developed in general-purpose programming languages are supported in the technology. H. Hanbar et al. (2020) evaluated the optimized performance of the improved KYC structure by figuring out the number of transactions served by and in the network of blockchain through chaincode, with a lot of variations in the transaction rates. On average, the maximum level of throughput for a single transaction on the blockchain is 5 tps. It was found that throughput would increase with the rate of sent transactions in the beginning, but later would saturate around 5 tps. Again, as the number of transaction requests increases due to a high send rate, the latency increases. On average, the transactions of banks on blockchain a maximum throughput of 9 tps. It was again found that the throughput would increase with the rate of sent transactions at first, but then would saturates around 9 tps. Furthermore, when transactions begin to queue up, latency increases as the sent rate increases. (Hanbar et al., 2020).

2.1.17 Scopes of Implementations with the Redefined e-KYC Process

It is worth understanding that the use of DLT exceeds others. According to J. Parra et al. (2017):

i. Auditing and surveillance will be strengthened in the first place for the technology. The national regulator will be benefiting from that because it has a constant record of the facts checked before the accounts were opened and may serve as a unique point of fact in case of a dispute. And no other technology can match the immutability of DLT solutions' records.
ii. The scheme promotes the cooperation of FIs that do not inherently trust one another. FIs can only support an anonymous communications system – including anonymous payments and anonymous documents sharing – because they are competing for the assets and accounts of their customers.
iii. One of the major scopes of the improved KYC tech is that an organisation's attempts to validate a customer are paid anonymously and proportionately. This is only possible due to the dispersed leader characteristics, which make it possible for organisations to collaborate without revealing their identities and ensuring all relevant regulations are always complied with.
iv. It is needed to keep in mind that this system, regardless of the technological framework used, is an interbank co-operation system at its core. Since a clearing instance will be required to settle compensation for such a new scheme, DLT removes the need for high central authority fees.

In general, for the following reasons, the DLT solution is preferred because: (1) it allows for process automation, (2) increases the amount of information available in a conflict, (3) reduces mediation time in relation to other technologies and lowering business costs (Parra Moyano & Ross, 2017).

2.2 Blockchain Technology

Before Satoshi Nakamoto, the cryptocurrency blockchain had remained virtually unheard of, even though it was found to enhance the accessibility of electronic cash by an unknown peer-to-to-peer system that he named as Bitcoin in the year prior. He set out to address the problems that the electronic transfer of money poses for financial institutions. A tamper-proof payment system was offered, as it made transactions immune to fraud and minimized the total cost of each transaction (Nakamoto, 2008). In the first place, Bitcoin pioneered the idea of using a blockchain. Thus, Bitcoin should not be confused with applications like Ethereum and Smart Contracts, as it is the structure on which they are all built. Decentralization and immutability have made it a lot more versatile. Blockchain is becoming much more popular due to its permanence and adaptability (Budhiraja & Rani, 2019). Some examples of places where Cryptocurrencies have already been used include: the healthcare industry, with medical records, and becoming more common in public sector procurement. Major banks have also started using blockchain for trade finance. The advent of blockchain has been a major change in the world of industry.

The blockchain, also familiar as Distributed Ledger Technologies (DTLs), would enable different entities that might not trust one another for sharing the documents digitally (European Commission, 2019). This data could constitute money, personal information, images, records, transactions. Since the 1990s, Distributed Ledger Technology has been proposed and is applicable to any framework that can be operated through a distributed platform (Yang et al.,2018). Generally, DLTs are a class of databases – of which blockchain is one which stores, exchanges, and synchronizes data among a set of computers or participants that could be very diverse. Although not all the DLTs are blockchains, the blockchain is distinguished from other distributed ledger technology DLTs by the way it uses cryptography to archive and synchronize data in a chain of blocks (European Commission, 2019). This information is updated in accordance with the underlying principles, which are identified by the stakeholders (Bhatia & Wright de Hernandez, 2019).

2.2.1 Components of Blockchain and How It Works

This paragraph aims to discuss an in-depth interpretation of blockchain components and their functions in order to facilitate comprehension of the entire mechanism. Before delving into the specifics of the blockchain's workflow, an overview is given. The chart beneath summarizes main processes, beginning with signature generation. Digital signatures are generated using a signature generator that combines Cryptography and Data Encoding. It necessitates the use of cryptographic keys, such as private and public keys, and is governed by a set of rules (Geldenhuys & Hoffman, 2012). A message is encrypted using the private key before it is sent over the network. In accordance with the network consensus rule, when this transaction is processed, the nodes can validate it. Then, the transaction is compiled and used to construct a block that contains only those transactions that have been authenticated. After a considerable time has elapsed, the process is described in subsequent parts. In accordance with the network consensus rule, when this transaction is processed, the nodes can validate it. Then, the transaction is compiled and used to construct a block that contains only those transactions that have been authenticated. The process is described in subsequent parts.

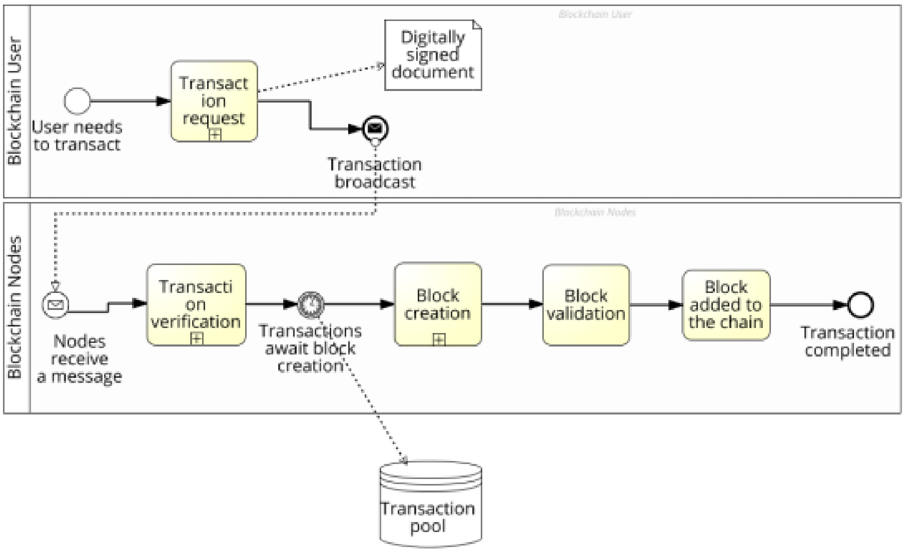


Figure 4: Process of a transaction in the blockchain (Effiong, 2020)

Transaction Request

A transaction is described as any communication that is entered into the distributed database. It may be one or the other: a warning from a program, or a stimulus for a program. Also, the message can contain unencrypted information or be a connection to information that is encrypted elsewhere. In above shown figure, a collapsed subprocess is used to omit unnecessary information that is unneeded for drawing the process. A key in this phase is often uses hashing, encryption, and spreading the key distribution, after which it is propagated across the network. The next move is following in the chain is taken by other block holders (Murphy, 2016) (Ismail et al., 2019).

Nodes

A participant in a blockchain uses a decentralized computer system to record events and confirm transactions known as a node. Each node in the network maintains a replica of transactions and records them in its ledger after obtaining consensus from another node in the network. If a node provides to the other members and continuously confirms that information, the ledger that it provides to the rest of the network must be correct (Alammary et al., 2019).

Transaction Verification

Blockchain technology utilizes digital signatures and cryptography to verify the authenticity of a transaction. The request method uses a private key to sign transactions, as users own private and public keys. While the user's private key remains private and is used to sign transactions during the encrypting process, the encrypted data is broadcast to the entire network. It is a collapsed subprocess in Figure 3 since it entails a series of peer-to-peer operations that verify the recipient who submits a transaction request and verifies the transaction using the public transaction key. The authentication process verifies that the message has not been altered in any way (Zheng et al., 2017). A successfully authenticated transaction is genuine and is retained in the transaction pool until it is added to the ledger on the block. As a result, it is depicted in Figure 3 as an intermediate timer event.

Algorithm of Consensus

A network contains several nodes, all of which are considered to be unstable. Consensus algorithms ensure network stability by ensuring that subsequent nodes are still the original version, as well as protecting the device from being hacked and forked by malicious parties. Until every transaction is registered in the blockchain, Yang et al. pointed out that it is subjected to decentralized inspection to ensure that no unauthorized transactions can take place (Yang et al., 2018). Consensus mechanism is a set of rules that guide participants in validating, verifying, and adding blocks to the blockchain (European Commission, 2019). Proof of Work, Proof of Stake, Round Robin, Proof of Authority/Proof of Identity, and Proof of Elapsed Time are just some of the different types of consensus models available (Yaga et al., 2018).

What is Block?

According to Yaga et al. (2018), each block in the blockchain network contains a block header and a block body that registers the transactions in the block. The header of each block contains information about the block, such as a time timeline, a hash representing the block data, the hash of the previous block's header, and the block size. The crypto-nonce can also contain information if a hash-puzzle is cracked in order to publish a node (Yaga et al., 2018). A block operates in its own network and adheres to the network's rules. Prior to being added to the blockchain, it ensures the consistency of transaction times and order. With the Hash function, each block enhances the validity of the preceding block and, by extension, the entire blockchain. The method is immutable since it is tamper-proof (Manav Gupta, 2017).

Chaining the Blocks

After a block has been created, a transaction is added to it, and all nodes agree to validate it. The transaction cannot be changed when blockchain updates are made – which occurs very often (Greg Walker, 2015). The information in the header of each subsequent block – in the form of a hash value – links the blocks to an event called "completed transactions". The new block continues to form the entire network with the previous block hash. Any block change updates the hash value of the block and changes the entire block network, which will not take place without notifying all the block nodes. The blocks can be rejected once a modifying message is detected (Yaga et al., 2018).

Hash Technique

A hash is a unique identifier for each digital data on the blocks and a vital part of blockchain technology, which is used in a variety of operations. They are like human fingerprints, unique in nature. Hashing is a technique for quickly converting any data input into a collection of hash values using mathematical computation (Yaga et al., 2018). The same input will still produce the same output, confirming the data's authenticity, but any slight variation in the input will result in a different hash value. The output provides no information about the data that was entered. The hash on the distributed ledger proves that a record exists, but only public/private key functions can access the document's content (European Commission, 2019).

Validating a Block Creation

According to Yaga et al. (2018), node-authenticated transactions are stored in a memory cache until they are inserted into the block. When there are a large number of distrusted participants, only one participant can add transactions to a block, which is difficult to determine. As a consequence, the collection of rules that usually govern participants, such as Proof of Stake and Proof of Work, are used to make this decision. After a transaction is made, it is added to a block, which is then validated by all nodes. The transaction cannot be changed until the blockchain is modified, which happens regularly (Greg Walker, 2015). According to Yaga et al. (2018), node-authenticated transactions are stored in a memory cache until they are inserted into the block.

Access to the Network

Network access is required for anyone who wishes to engage in some form of network service, whether private or public. Desktop apps, smartphone apps, and digital wallets are examples of software applications that serve as a conduit between users and blockchain technology. In a blockchain wallet, users can securely (1) store private keys, public keys, and associated addresses, as well as (2) send and receive digital assets. It can be downloaded and uploaded on a device, or it could be accessed through a web browser (Grech & Camilleri, 2017).

2.2.2 Classification of Blockchain

Blockchains are classified by Fernández-Caramés & Fraga-Lamas (2018) based on data management, data usability, and user engagement. (1) Public networks, (2) Private networks, and (3) Consortium networks with varying degrees of decentralization are the three major categories given by Li et al., (2019).

- **Permissionless Public Networks:** This is a traditional blockchain network, which is totally decentralized and makes all data stored in the blockchain publicly available to all nodes. The use of data is unrestricted in every way. Proof of Work is the consensus protocol most commonly used on this network to ensure network security. Counterfeit blocks are discouraged due to the computational complexity.
- **Consortium Networks (Public & Permissioned):** A consortium blockchain, according to Li et al,. (2019), is based on a shared network, but only a limited number of nodes are allowed to participate. Although not all nodes can engage in

transaction validation, they can all contribute to network security. Availability of data is limited.

- **Private Networks:** Only a limited number of people can enter, read, write, and audit the blockchain since it is a closed network. Transaction authentication is quicker and less expensive than using the public network. However, blockchain's decentralization function is jeopardized.

2.2.3 Differentiating the Forms of Blockchain

To differentiate the various forms of blockchain, Zheng et al., (2017) took a somewhat different approach. According to Zheng et al. (2017), it is a distinctive factor to decide what rule the network operates by, e.g., the private blockchain involves only organizational participants. Furthermore, not all blockchain forms have the same permission to read. Similarly, whether or not data are tamper-proof is dependent on the type of blockchain being used. Since access control is restricted to a few selected counterparties on whom the network's authority is vested, it could be possible to modify a private blockchain, illustrating why it is also much less decentralized. Moreover, the performance of various network types varies. The public network, which runs on a permissionless consensus, is usually slow due to the amount of mathematical computation required to publish a block in the Proof-of-Work consensus, while the consortium blockchain runs on a permissioned consensus, which requires a different model to publish a block and therefore is much more effective.

2.2.4 Key Characteristics of Blockchain

Decentralization

In any framework, the validity of transactions must be guaranteed. The regulator would be the third party in a centralized system who would be responsible for authenticating the all the transactions or verifications, which would result in the additional expenses for the regulatory work and intermediary interventions. The technology of blockchain, on the other hand, would operate on a peer-to-peer basis that keeps the data on each node of the network and that does not allow any third-party intervention (Zheng et al., 2017). The majority of the scholars agreed that blockchain technology's decentralized structure is a major advantage in case of ensuring the data regulations in the consensus algorithm of blockchain (Yaga et al., 2018). Without the involvement of a third party, each party in the blockchain technology may access the database and view the transaction history without any kind of intervention by the third party like regulators (Tapscott and Tapscott, 2017). The chain's key benefit is the distributed network replication. To remain undetected, a terrorist or abusive government agency must modify all copies of the blockchain at the same time. Furthermore, distributed ledger technology would be able to record all the real-time transactions restricting the system from all the fraud tasks (Rennock et al., 2018). The efficient management of Blockchain and related operations with decentralized networks can be demonstrated maintaining the conditions of restrictions (Pereira et al., 2019).

Tamper-Proof

No participants can alter the record once the terms of the transaction have been agreed. In cases where any situation such as inaccuracy or decision change requires reversal, a new transaction must take place in a way that both transactions exist, and all participants are aware of them. Every transaction change, therefore, leaves its way (Manav Gupta, 2017).

Immutable and Irreversible

Invariability suggests the notion of immutability. A transaction generated in blockchain cannot be altered in practical terms because it is distributed among the nodes at various locations. Its typical evidence for manipulation gives it immutability. Another user can perceive attempts to reconfigure the data of a single node as an act or an attack and will stop right there (Grech & Camilleri, 2017).

Transparency

All participants with an Internet connection can access the public blockchain to read the booklet, update it in line with the present consensus mechanism. In this respect, no transactions for participants are hidden or vague and the system can be trusted and audited accordingly. However, only default participants can access messages in a private blockchain (European Commission, 2019). Murphy et al., (2016) stated that the openness level that is required for the use of the technology might be the standard in case of selecting a blockchain type for legal and regulatory matters to consider (Murphy, 2016).

Authenticity of Origin

The ability to monitor a transaction to its origin on blockchain technology is another key feature of blockchain. If the need arises to see how property ownership has evolved over time, participants could learn that by themselves on the blockchain platform (Manav Gupta, 2017). It is claimed by Sultan et al. (2018) that the transparency of the technology would establish the authenticity of the origin.

System Security

The collection of privacy, integrity, and accessibility, in general, defines information systems security. Privacy refers to protecting most responsive information from unauthorized access. The integrity of the data also ensures that no unauthorized people are unable to modify the data, and the possibility for those persons to revoke the amendments is that the data would be accessed on a need basis. This technology would offer a way to preserve the data privacy by means of e-signatures and ensures the ability of the records being immutable on the chain. As blockchain data are distributed over a wide range of nodes, a node attack does not impact the supply of information (Fernandez-Caramés & FragaLamas, 2018).

Consensus Mechanism

Since there are no main reliable agents on the entire network, a consensus mechanism is established in the network. The aim of this mechanism to reach an agreement on a unified basis each time a record is verified. A record that is non-existent could be created throughout the network by having the control over the percentage of the accounting nodes. Distortion of any kind can therefore be easily identified (Huang et al., 2019).

Securing Anonymity of Users

On the chain of block, all the users have their own unique alphanumeric address, which they may choose to keep private or share with others (Tapscott and Tapscott, 2017). Transactions are made between Blockchain addresses. If the users want, they would communicate with the network with the help of the address provided, and no centralized authority would be available there to record the confidential data of the users (Zheng et al., 2018). This mechanism protects some of the user's privacy. Owing to its inherent limitations, however, blockchain cannot ensure perfect privacy and security.

2.2.5 Development of Blockchain

There are three generations of block in the technology that are Block 1.0, Block 2.0, and Block 3.0. Bitcoin is the popular project of Block 1.0, which is a currency. Mortgages, shares, loans, futures, and smart contracts are all covered by Block 2.0. Government, technology, wellness, culture, art, and literacy all use Block 3.0 as a universal framework and platform (Swan, 2015). Blockchain is divided into three levels, according to Feng et al. (2018): the peer-to-peer network, databases, and applications. Blocks are linked at the Global ledger level. Each block contains transactions and smart contracts, which are then connected to the block to which it is linked. Different services would ask, evaluate, and would interpret transactions' meanings in each block, smart contract, and would update the application level.

2.2.6 Challenges in Blockchain

Blockchain has a lot of promise, but it faces a lot of obstacles that might prevent it from being widely used. The technology of blockchain is designed as a distributed ledger system in which the users remaining in the network would be able to read the records of the transactions and update the database with new information. The system's cornerstone is transparency and the lack of central coordination that poses the negative effects on the chain and restricts the users in different aspects (Drescher, 2017). Some problems like security, scalability, and latency could be raised, but the FIs in the market are struggling in the search of reliable solutions (Underwood, 2016).

Scalability

The increase in the number of transactions and verification make the blockchain to become more voluminous (Zheng et al., 2018). Blockchain transactions, according to Marr (2018), generally would take more time than usual because of the complications in the process of implementation and encryption. Chen et al. (2018) implied that there are over a million active smart contracts on Ethereum network. According to Jackson (2018), Visa is able to process 24000 tps whereas PayPal processes 193 tps, and the Ethereum and Bitcoin processes only 20. It only implies that the processing ability of the market in a short period for millions of transactions is actually unsatisfactory. The reason behind this issue is that the blocks have a limited amount of space, causing delay in some transactions because usually, miners do prefer higher fees for making any transactions happen (Biais et al., 2019).

Security

Werbach (2018) stated that the system technology of blockchain is vulnerable in real. The networks of Bitcoin and Ethernet use blockchain as their underlying infrastructure since 2009 and are being hacked regularly that leads to a loss of around or over 600 million yuan. Blockchain is vulnerable to collusive self-centered miner attacks, as well as a number of other attacks, according to Zheng et al. (2018). Price (2018) in his paper argued that all the public networks in blockchain are vulnerable to the attacks of either 51 percent or 34 percent because of the way the technology of blockchain is developed. The attacks of 51 percent happen when the hackers are usually the primary source for the computational power in the blockchain. As a result, they own the entire Blockchain and hold the bulk of the network's votes. World's first and largest site for the exchange of bitcoin, Mt. Gox, had declared on the 28th of February in 2014 that a total of 850,000 bitcoins had been stolen that included the trading accounts of the users and even the own accounts of the company that led to a loss of $467 million. On June 8 of 2016, the hackers had stolen $3.6 million from Dao that is the world's largest site for crowdfunding that led to a loss of $75 million. Finally, a Japanese exchange announced a cryptocurrency scam worth $500 million in 2018 (Werbach, 2018). Despite the fact that the technology of blockchain would demonstrate the uniqueness of the system in the market, regulators continue to face challenges as a result of its infancy (Cong and He, 2019).

Privacy Breach

In order to avoid information leakage, the Blockchain would create several addresses rather than sharing the true identity of the users that is assumed to be a very secure technology. Since all transactions and balance information are open publicly, the system would not be able to prevent the leakage of the information of transactions (Meiklejohn et al., 2013; Kosba et al.,2016). The problem of privacy leakage is massive, and it jeopardizes the security of users' personal information. Despite the fact that many ways have been proposed to improve Blockchain's anonymity, the problem remains unresolved (Cong and He, 2019).

Consumption of Energy

Big data systems can have higher execution and still have a higher cost of storage than the cost of e-money transfers and long-term storage for the transactional data (Staples et al., 2017). Price (2018) had elaborated that the power needed for computation to run the system in the blockchain is growing increasingly. Bitcoin would consume energy at a massive rate, and a single transaction in the network of bitcoin would use thousands of terawatt-hours of energy.

2.2.7 Ethical Issues in Blockchain

Blockchain technology can provide participants the ability to store data permanently with the feature of immutability. Then again, it could also raise the concern for the risks of data privacy for certain organizations (Till et al., 2017). On the other hand, integrating the feature of confidentiality into the public networks of Blockchain-based systems is difficult since knowledge is open to all network users automatically (Staples et al., 2017). Transparency in this technology is required to explain and define the ownership of a user and avoid the problem of double-spending, whereas users in the network require for their data privacy (Drescher, 2017). According to Feng et al. (2018), the transactions in the blockchain would include the addresses of the participants, the hash values of the transactions, the timestamps, and the e-signatures of the senders, allowing data miners to track transaction flows and extract user details. As blockchain is distributed, it lacks the oversight of the legislative authorities and the administrators, and as record altering is almost impossible on the blockchain, both of the factors would trigger several issues (Price, 2018). Criminals use cryptocurrency as a payment tool. Though Lewis et al. (2017), among all the vulnerabilities, stated that the blockchain is used to fulfill the AML and KYC criteria for the FIs and for the public transaction over blockchain.

2.2.8 Blockchain Development in Financial Industry

Despite the fact that the advancement in the new technology is in its infancy still now and is impeded by numerous obstacles, the major multinational banks and other conglomerates that provide financial services have immediately run to stake the territory out and invest the money in the development and experimentation of the technology. Blockchain transactions can be used for big data processing, so they can coexist with big data. Users may also forecast the future of development in the activities of trading. The advancement in the blockchain technology is that it has the potential to open up a plethora of new opportunities. When Blockchain technology becomes more prevalent, commercial banks aggressively build and implement the technology to strengthen the centralized framework for banking. FIs would eliminate or discard the use of a middleman by leveraging the chain’s stability, transparency immutability (Underwood, 2016). According to Hassani et al. (2018), the attitudes of the banks towards the technology of blockchain are almost confusing and conflicting. The main reason behind this attitude is that banks have been playing the role of middleman since forever and have been receiving all the incentives for their trustworthy services for years, whereas blockchain is now posing a threat towards banks of seizing the role of the central party and all the incentives.

2.2.9 Suitability of Blockchain in Automating e-KYC

Regardless of technology, it appears that the financial system's current infrastructure must be integrated to ease the transition and to avoid mainly the development of multiple technology stacks. Accommodating manual processes is a major challenge for a DLT-based solution. If the elements in the technology could not be automated or coded, the system would fail to store the updates in the ledger of its distributed technology. Furthermore, the data sources are allowed to communicate with the systems that are very secured like Oracles, and generally work as the bridge between the inputs of different FIs that are on-chain and off-chain. These sources make sure that all the transactions are e-signed and a minimum degree of transparency is ensured. Since it can only access data that is stored on the chain, a distributed ledger's data sources are inherently restricted. Moreover, removing obsolete infrastructures and reducing costly reconciliation processes are crucial to improving. Angela Walch had figured the idea that the use of the technology of blockchain is not as same as the concept of plug-and-play (Wharton 2018). “Blockchain technology is, at the core, group recordkeeping. To reap its full benefits, one needs all the relevant members of the group to join the system. This requires collaboration with and across businesses, which is a potentially big hurdle and may be the hurdle that most limits adoption” (Wharton 2018). On the other hand, ENISA (2016) had analyzed that most distributed ledgers that are rising must engage in the network with each other information sharing purpose for the requirement of translating the exchanged formats and especially the protocols.

2.3 Theoretical Framework

Egelund-Muller et al. (2017) investigated the creation of a multi-counterparty automated financial system operating several complex financial instruments, like settlement, directly on distributed ledger technology. Regulation's growth and technological advancements, combined with the 2007 financial crisis, have created an opening for firms operating in the field of "RegTech," which aims to use the technology to facilitate the application of regulations. RegTech is a term that combines the terms "regulation" and "technology". Within the scope of KYC, these prospects are particularly important (Memminger et al., 2016; Arner et al., 2016). A consumer must first go through the KYC process before working with a FI or NBFI. Currently, when a client forms a partnership with a FI/NBFI, the KYC verification process incurs costs every time. At this point, it is necessary to differentiate between the "core KYC verification system", and which is the foundation of KYC verification that all FIs/NBFIs are required by law to conduct, and the "bank-specific processes". To resolve the KYC method's present inefficiencies, a redefined and improved DLT based KYC should be proposed based on three assumptions (Parra Moyano & Ross, 2017):

i. The conditions for providing vital KYC verification to a client are determined by a group of FIs/NBFIs operating in the same country and therefore bound by KYC regulations.

ii. All FIs/NBFIs involved in the framework settle on the approximate expenditure of performing a core KYC verification procedure. Naturally, costs vary depending on the complexity and default conditions of individual customers (e.g., size of the client, the risk level of the client, the volume of documents exchanged, etc.).

iii. The government regulatory authority shall preserve the structure and authorize financial institutions to make the KYC verification process more efficient and consistent.

These three assumptions are necessary so that all participating financial institutions have the correct compensation arrangements. In addition, the improved KYC process must fulfill four conditions to meet the desired effectiveness for a DLT based system (Parra Moyano & Ross, 2017):

1. *Proportionality Condition:* It needs to ensure that the costs of performing the core KYC verification procedure are shared in proportion. The criterion for proportionality guarantees an equal distribution of costs.

2. *Irrelevance Condition:* The confidentiality benchmarks governing the KYC process are to be met as they currently exist. The condition guarantees that no excuse should exist for a FI/NBFI to perform the core KYC verification procedure.

3. *Privacy Condition:* This one will guarantee that no institution will be eligible for reimbursement or compensatory damages unless and until the core KYC process is completed. Until the information is disclosed, the Privacy Policy ensures that the FIs/NBFIs operating on the framework are unaware of the customer's other FIs/NBFIs.

4. *No-minting Condition:* This must ensure that a core KYC verification method is not intended by a financial institution to be compensated for the work it does not perform. It should also ensure that no FI becomes a free-rider by refusing to pay for the use of data provided by other member institutions.

2.3.1 Adoption Issues of Blockchain in KYC in Banking Industry

Traditional roles would have to alter the course of blockchain technical and digital developments, according to the World Economic Forum (2015). Governments, in particular, will pursue an engaging facilitator role rather than a commander role. If monetary institutions embrace blockchain technology, they will disrupt established pricing and exchange rate structures. The key factors that contribute to blockchain adoption are regarded as opportunities or advantages of utilizing blockchain technology.

According to Lang (2017), blockchain cryptography secures shared data, allowing banks to create an updated core “repository” of customer identification data. This will improve the AML and KYC processes, enhance the interoperability of banks across borders, lower expenditure in administration, and reduce data duplication, lowering infrastructure costs. However, it is believed that blockchain-based KYC registries will not likely gain widespread acceptance because Banks would be reluctant to depend on third-party verification of data.

Smith (2018) showed how using the blockchain’s consensus, encryption, security elements, timestamp, and auditing could be improved to be continuous in real-time rather than just historical and could review all of the transactions rather than the conventional, random, statistical sampling. He forecasted the auditors playing a bigger role in data protection strategies and decision-making. Banking procedures could become more transparent and secure as a result of blockchain technology. High levels of unparalleled openness are achieved by locking the blocks, granting maximum historical data access and authorization rights, and making all alterations publicly available. Real-time auditing, automatic financial statements, prompt action in the event of a regulatory breach, and real-time contact among banks and regulators would all be possible (Hassani et al.,2018).

Traditional positions such as intermediaries would be questioned, according to Smith (2018), but new advisory functions will emerge. Because of the certainty that blockchain provides, Lang (2017) found that both person and FIs could have the option of transacting directly, allowing for quicker, easier, and more safe payments. The average blockchain transaction rate, according to Hassani et al. (2018), is 1,000-2,000 transactions per second (TPS), but the banking industry has yet to agree on blockchain transaction ability. Marr (2018), on the other hand, believed that due to its sophistication, encryption, and distributed functionality, blockchain would be slow and cumbersome, particularly as it grows in scale. As a still-to-be-developed approach, he suggests advances in engineering and processing speed. According to Accentrue (2017), operating processes will be cut by 50%.

When the adoption supporting factors were compared to the term occurrences after categorization, the “improving KYC process” factor came out on top, accounting for 46.80% of the total supporting factors. Since the top three variables are the most important, this means that the degree of offered systems and infrastructure has a greater impact on blockchain adoption in the banking arena (Kawasmi et al., 2020).

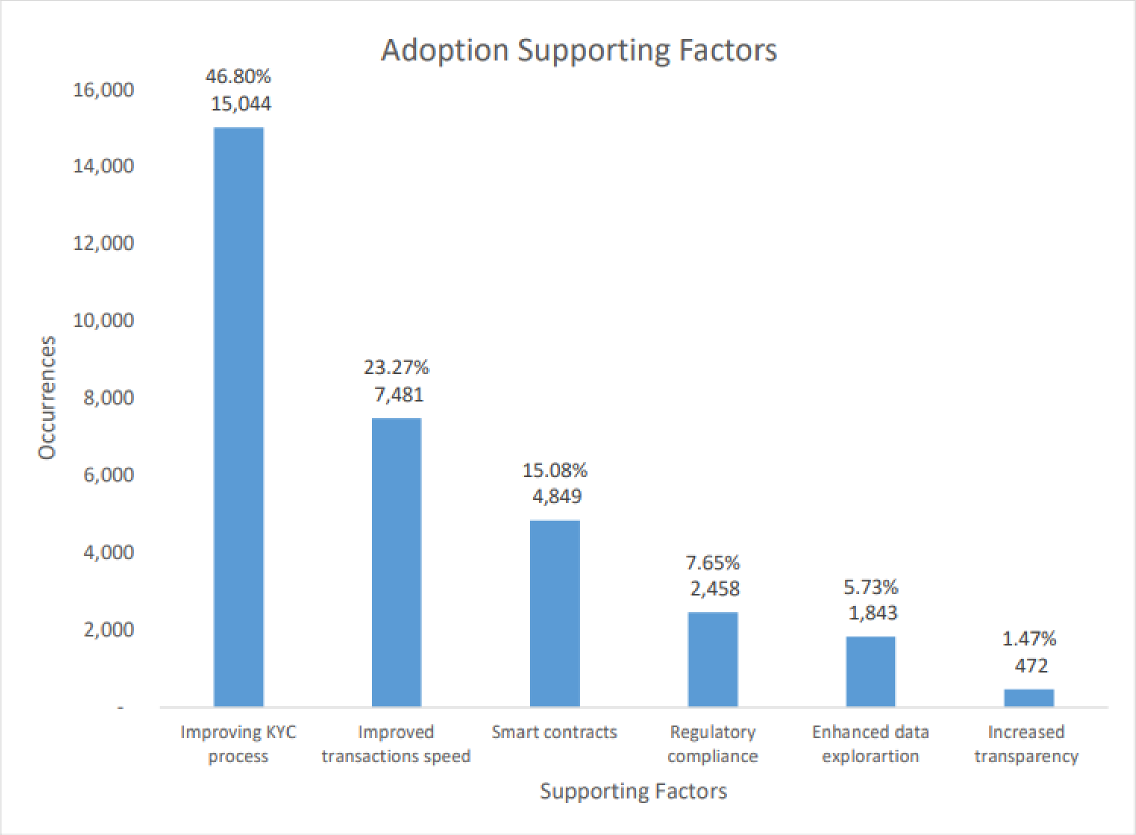


Figure 5: Adoption Supporting Factors (Kawasmi et al., 2020)

2.3.2 Change Management in Adoption of the Blockchain Technology

According to Beck and Müller-Bloch (2017), developments in transaction speed, security, and accountability, lower transaction expense with revolutionary projections to reshape structures and modify the existing economy's cardinal premise are among the potential advantages of utilizing blockchain technology in the banking industry. However, Tapscott and Tapscott (2017) believed that blockchain would have an effect on the existence of businesses, not only in terms of how they are financed and run, but also in terms of how they generate value and execute their basic organizational functions. According to Ito et al. (2017), blockchain adoption would necessitate a difficult structural reform of large sections of the economic structure, which will necessitate study and experimentation. They also say that those who embrace blockchain technology would prosper in the new economy. Despite the fact that banks and financial institutions are committed to adopting blockchain technology, Beck and Müller-Bloch (2017) agreed that it was still uncertain how they would behave to implement the new disruptive technology. Taherdoost (2018) stretched the significance for policymakers to consider the reasons for a new technology's acceptance or rejection in order to predict and plan in an effective way for consumer adoption.

2.3.3 Interoperability in Adoption of Blockchain

Interoperability is a property that allows blockchain-based platforms to interact and exchange data (Courcelas & Timsit, 2019). Although there are a variety of ways to achieve interoperability between blockchains, there are two main models, according to Courcelas and Timsit (2019). Using trusted third-party authorities (Trusted Bridging) to verify transactions or data falls under one class of interoperability approaches. Two or more blockchains, for example, may accept to allow an off-chain entity to exchange information between them or log the state of their respective blockchains so that each could trust what has happened on the other. Multiple blockchains may also rely on a third-party data source for trusted reference data, such as certificates that confirm a person's or asset's identity. The other model of interoperability approach (Trustless Bridging) includes explicitly sharing information across blockchains without the use of a third-party authority. While incorporating a newly developed blockchain-based process with the current process remains a challenge, new ideas might acquire momentum.

2.3.4 Blockchain Adoption Models for Theoretical Framework

Taherdoost (2018) opined the value of emerging technology explanations for policy makers to better predict and brace themselves for the introduction of a new technology. Instead of being guided by the acceptance of banks' clients, blockchain adoption in a highly regulated sector like the banking industry should be influenced by new legislation and best guidelines from regulators and practitioners (Kawasmi et al., 2020). Models for technology acceptance have been thoroughly studied over the past couple of decades and have given many models, such as the TAM, the Extension of Technological Acceptation Model (ETAM), and Rogers DOI (Taherdoost 2018). One of the most widely embraced and used technology adoption models is TAM, according to Gangwar et al. (2014) and Taherdoost (2018). They explained that the incentive to adopt TAM is attributable to three factors: perceived usefulness (PU), perceived ease-of-use (PEOU), and attitude towards (A). Wang et al. (2016) suggested a blockchain maturity model (BCMM), as it was considered that a business should be able to assess its maturity level in order to implement a technology newly introduced.

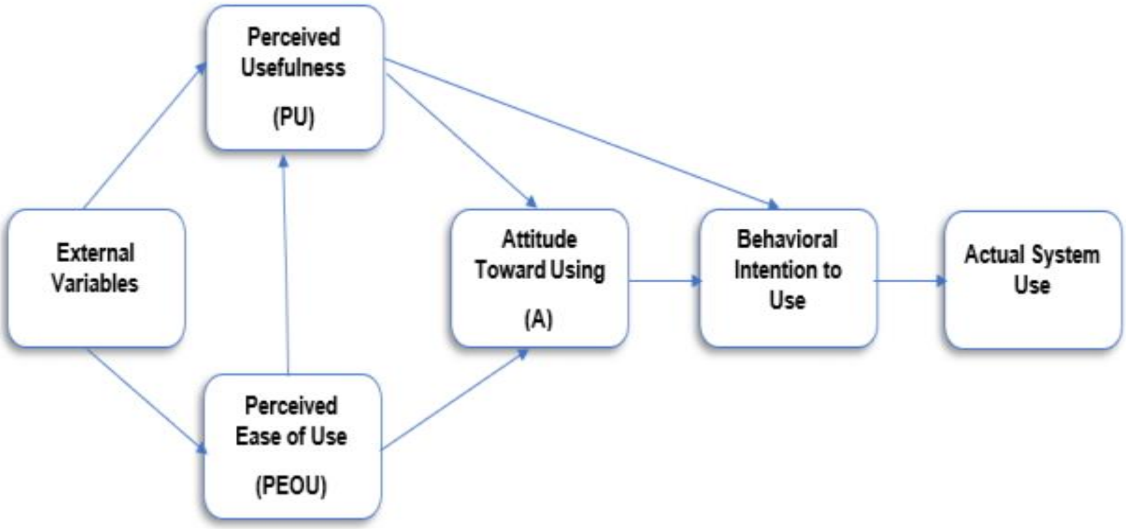
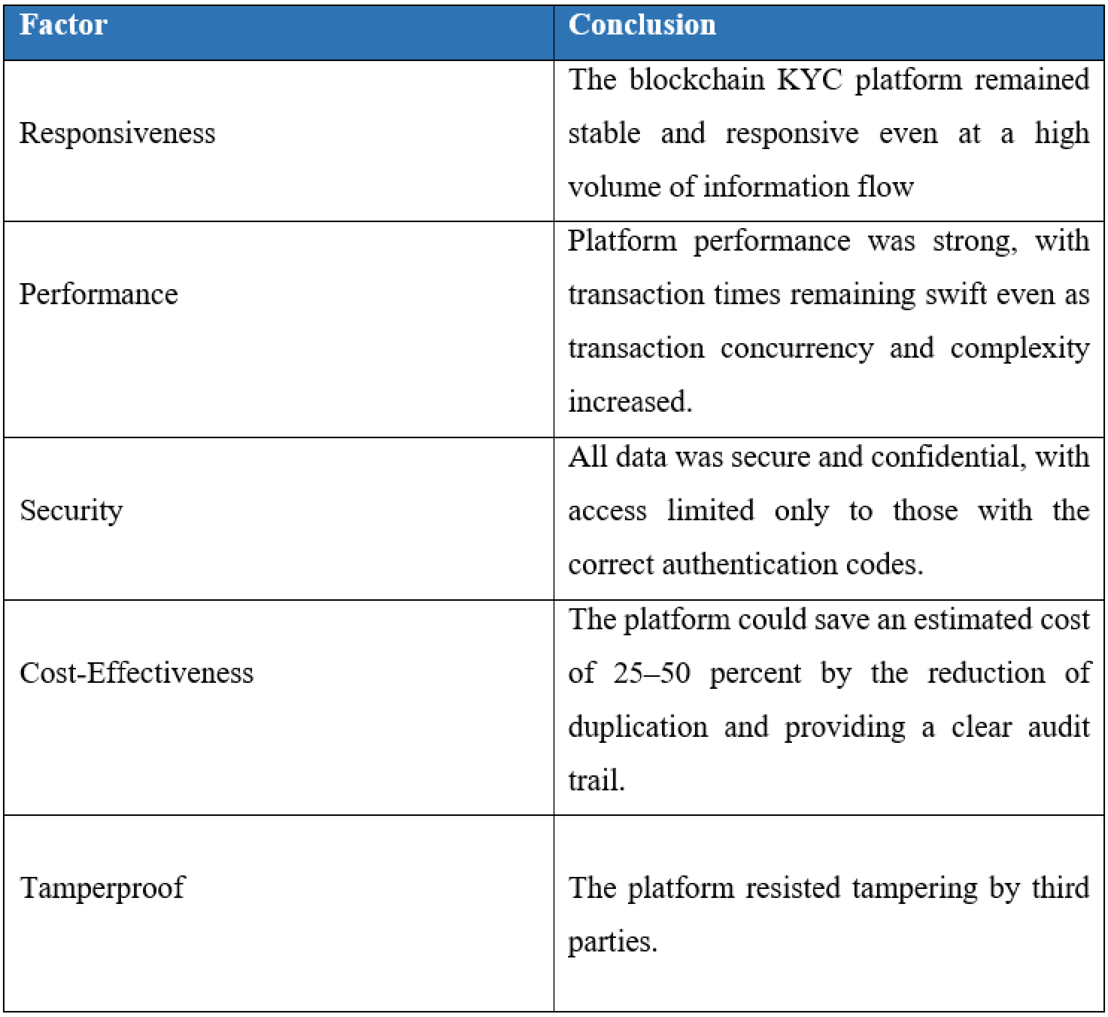

Perceived Usefulness (PU)
External Variables
Attitude Toward Using (A)
Behavioral Intention to Use
Actual System Use
Perceived Ease of Use (PEOU)

Figure 6: Technology Acceptance Model (Davis, 1989)

2.3.5 Blockchain-Based KYC Cases

Although the technology got the obvious potential, the feasibility of a KYC utility must be evaluated in order to determine its true applicability (Eamonn & Chia, 2018). KPMG in Singapore and Bluzelle Networks collaborated on a proof-of-concept KYC utility with a blockchain network in 2017, with three Singaporean banks — HSBC, OCBC, and Mitsubishi UFJ Financial Group (MUFG) — and the Singaporean regulator Info-communications Media Development Authority (IMDA). All new KYC specifications were first inquired on the single network, and current user data were exchanged with user's authorization after the distributed KYC system was created. Customer data was then authorized by relevant third-party sources, with the results reported in the KYC shared ledger, bolstering the platform's depth of data. All customer behavior, approvals, and new data given to each of the three banks were monitored and registered. KPMG in 2017 created this proof-of-concept prototype to evaluate the technicalities of a blockchain network, such as usability, fun security, and scalability (Eamonn & Chia, 2018). The test results ascertained the conclusions as presented below:

Table 3: Test Result of Blockchain-based KYC Prototype by KPMG (Source: Author)



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:

Société Générale, Natixis, Commerzbank, Euler Hermes, Tikehau Capital, and R3, all of them are members of Clipeum, a European association of banks, insurers, and asset managers. Through the development of an open-source financial ecosystem for collaboration in the processing and pooling of KYC-related documents, they are attempting to address a number of market inefficiencies and other hindrances space ("KYC [DLT] - The Hottest KYC Projects in Trade Finance", 2020). The platform offers a multi-Financial-Institution based, information-sharing network to help speed up the end-to-end KYC onboarding, but it is primarily based on document processing. Banks will have to perform their own autonomous KYC verifications, but by providing APIs, Clipeum can make it easier for them to do so. This ensures that if a FI seeks access to a particular collection of records, the treasurer may issue whatever access the bank requires. A treasurer who wishes to end a business arrangement with a specific FI may withdraw access to that institution's information at any time, effectively shutting down the flow of data from that bank's data (Patel & Ganne, 2020).

KYC-Chain

KYC-Chain is a distributed ledger technology-based process system for streamlining the KYC onboarding process and controlling the entire customer journey. Sanction's screening, identity verifying, OCR extraction software, API integrations, and more are part of the solution system, which was born out of dissatisfaction with the current KYC method. Users can build turn-key solutions that comply with different legal requirements of various regulatory environments using their completely customizable toolkit (*Bringing Digitalization to the Business World*, 2020) . Over 500 000 active onboardings have been completed by the organization in 240 countries and territories until today.

Shyft

In January 2018, IBM collaborated with Deutsche Bank and HSBC to create *"Proof-of-Concept Blockchain-based Shared KYC"* (Curry M., 2019). Shyft is a blockchain-based public network that allows the user companies to share internal information and request the consent from their clients to share their personal documents while staying compliant with the regulation and privacy standards as GDPR. It also includes a creditability function that assigns a score to users based on previous transaction activity and compliance (*Shyft Network Inc.*, 2021). Shyft is basically a public network that would allow other companies in the data ecosystem to share encrypted data stored in an external database. All the sensitive data stored externally would have their own encrypted attestations that would be stored on-chain as encrypted metadata (*Shyft Network Inc.*, 2021). This network would never participate in any transaction or involve in any custody of data, instead, it allows the users to share data to the participants in the network of their own choice.

2.4 Summary

The earlier studies and the theoretical context for this analysis are the key sections of this chapter. Previous years' studies have been thoroughly looked into for the identity verification, the evolution of the verification processes, including their impacts and drawbacks, traditional and non-traditional way of KYC verification, and the scopes and barriers of blockchain based KYC verification process. The elements, processes, forms, and features of blockchain technology have also been studied from the previous research papers and applications. The suitability of blockchain for KYC verification has been studied as well as its capacity of improvements in the banking industry with its best performance. The factors and conditions concerning the adoption of blockchain technology and their impact on the system for verification have been investigated in the theoretical framework section, and the potential of blockchain technology for improving the interoperability among different financial institutions has been observed as well. Customers' responsiveness towards new technology and acceptance towards advanced KYC verification process has been studied from earlier studies considering different models as an aid to the issue. Finally, information from early adopters or testers of blockchain technology in this KYC verification has been collected to observe the competence of the technology in the banking industry.

3 . Research Methodology

3.1 Introduction

It was asserted at the study's inception that the current systems of KYC verification are inefficient, unreliable, and inconvenient, and this analysis seeks to investigate, recognize, and suggest the implementation of blockchain technology in the systems. After examining prior documents on this topic and identifying the existing information gap, we aim to close it through this study. As such, this chapter is intended to outline the research methods used in this research.

3.2 Research Questions

The primary objective of this study was to begin with an examination of existing systems and the suggestion of a blockchain technology model to improve the verification process for banks and fintechs in KYC. The analysis so far indicates that the development of the processes is really essential in the world of KYC verification. Furthermore, it highlights the various application areas for which blockchain technology has been applied, demonstrating how useful it is for handling these purposes. The aim of this analysis is to explain and describe the relationship between the major objective of the research questions, that are,

Main research question:
How can the use of DLT (Blockchain) improve the KYC process of Financial Institutions?

SRQ1: How to establish the implication of blockchain technology on the KYC management of Financial Institutions?
SRQ2: How to determine the benchmark to measure the performance of the blockchain-based KYC verification process?
SRQ3: How would the implementation of the blockchain-based KYC face operational and legal challenges?

Each one of these sub-questions would be further expanded into specific questions in order to obtain more direct information on the topic.

SRQ1 expands to these questions,

1. What is the present condition of the KYC verification process before the application of blockchain technology?
2. What aspects of the current KYC verification process could be improved?
3. What would be considered an improved KYC verification system?

Abovementioned set of sub-questions provides a comprehensive understanding of the current process. The current process aspect and the features indicating an improved system are to be enhanced. By this exploration, it is understood that blockchain technology needs to fill the void in the existing framework.

SRQ2 expands into these questions,

1. What are the major indicators of effectiveness in the KYC verification process?
2. What are the major indicators of efficiency in the KYC verification process?
3. What could be considered as a convenient KYC verification process?

The abovementioned set of sub-questions would explore how to assess the improvements that blockchain technology would introduce to KYC verification process.

SRQ3 expands into these questions,

1. What are the key challenges related to the legal and compliance framework?
2. What are the key challenges related to operational process and interoperability?
3. What are the key ways to overcome the challenges?

The abovementioned set of sub-questions would aim to illustrate the challenges of the implementation of blockchain technology.

3.3 Case Study Design

Runeson et al. (2012) asserted that the case study design is the most suitable for achieving exploratory analysis goals. They also examined case studies concepts, concluding that a case study examines recent phenomena in their context. This highlight demonstrates how well this design fits the set of data from a current event. Furthermore, the form of research issue has a significant impact on the design selection. Additionally, the form of research issue influences the design selection process. For a contemporary topic like KYC verification process, this study uses exploratory research questions defined by "how" and "what" thus making the case study research method the appropriate one to use.

A case study refers to an empirical investigation examining an existing topic critically without distinguishing it from its real-world context, according to Yin (2009). When the phenomenon cannot be isolated from its context comprehensively, this study is acceptable. He went on to say that a case study is conducted with the aim of gaining in-depth knowledge of a current problem. This distinguishes the case study from all other types of design. Yin (2009) mentioned two kinds of case study: multiple and single case studies, with Gustafsson (2017) explaining the distinctions between them. A multi-case study should be considered when the aim of the analysis is to understand the differences between cases, according to Gustafsson, and a multi-case study analyzes data both within and across cases. On the other hand, when the aim is to examine a particular item or group, a single case study is sufficient. A single case provides a broader explanation. Additionally, a single case provides a researcher with more time for observation than a multi-case study, allowing for the creation of a new and improved theory, claimed by Siggelkow, cited in Gustafsson (2017).

The research's goal is to examine the adoption of blockchain technology in KYC verification process, with a particular emphasis on European banks and fintechs. This research will use the single case study design, taking into account the previous discussion of when to use the case study design and the concept of the different forms of case study.

3.4 Data Collection

Kabir (2016) mentioned that data collection is indeed a critical and time-consuming process of study. It is universal in all fields of study, regardless of the methodology used. The aim of any data collection is to elicit sufficient evidence that eventually results in data analysis and, ultimately, the solution of the study's problem. He additionally stressed the importance of reliability in data collection and stated that it should be pursued throughout the course of data collection.

Kabir (2016) also stated that the first step in the research process is data collection, which allows a researcher to answer questions, experiment with ideas, and analyze data. It placed more emphasis on knowledge that could address research questions than on it. In order to get answers, an efficient data collection process must yield information that is useful to researchers.

Verne et al. cited in Runeson (2012) discussed three standards for data collection, “the use of multiple sources of data, creation of a case study database, and validation and maintenance of chain of evidence.” These concepts relate in part to triangulation, which means using several data points, different data types, and several data sources to control the perception of one source of information (Runeson et al., 2012). Reliability and validity are ensured by the triangulation of data.

For making sure to cover enough databases, previous records and interviews with major stakeholders have been used. Additionally, the subject areas involved the various viewpoints that were identified using interviews. It is outlined in greater detail in the following section.

3.4.1 Document Review

A document review is a comprehensive examination of established literature on a topic. A researcher becomes aware of the information gap on a subject by reviewing records, which then informs or justifies the need for a new investigation. In order to write a solid paper, a researcher may need to review a substantial collection of documents, as previous research will provide the foundation for such writing. Another tool of evidence used in paper reviewing often tells readers that a writer has a considerable amount of experience of debate, making the conclusions more credible and legitimate (Denney & Tewksbury, 2013).

Before starting the actual review, one should take a broad perspective of the subject and identify the different aspects of it. Quality research is critical in this area (Denney and Tewksbury, 2013). Hence, in this study, which focuses on how blockchain technology can boost KYC verification, the various process and components of the verification process were investigated. Then the theory behind using blockchain for the verification process, discussing topics like cryptocurrencies and their learnings were discussed.

Scholarly articles and books, essays, trade journal articles, and accounts, as well as national and foreign newspapers and magazines, were used to compile the documents. When it comes to document sources, finding appropriate pieces of literature to detail the

European situation concerning KYC verifications was especially difficult as it is a new technology. Hence, documents on that subject were scarce. In cases where an academic journal that addressed the topic could not be identified, grey literature was consulted. The document inclusion documents' target dates ranged from 2010 to 2020. Where later documents were unavailable, earlier documents were used instead.

3.4.2 Interviews

In this research, interviews were also used as a data collection tool. Interviewing is focused on making contact, collecting information, and getting feedback from target participants. The interview may be structured, semi-structured, or unstructured, depending on the situation. The semi-structured interview will include interview questions and a reference such as a list of things to discuss. Many queries leave room for flexibility (Kabir, 2016).

The semi-structured interview method was used to elicit responses from participants in this study. The interview questions were mainly open-ended, with a few closed questions interspersed, allowing for the detailed expression of responses and any additional inputs. Measures were taken to ensure that responses were accurate.

Responses were collected from a total of 10 respondents from one European Bank and a Fintech. Due to the pandemic, all the interviews were conducted over the phone or MS Teams. As the interviews might have some confidential information, the identities of the respondents were hidden. The audio was transcribed with an android application named Otter, and thematic analysis was done using Nvivo.

3.5 Analysis Procedures

According to Runeson et al. (2012), it is understood precisely what happened in the case thanks to data analysis. The researcher will draw trends and conclusions from the data if they have a good understanding of the situation. The researcher should have enough detail on every stage of the investigation and the procedure, and it is more of an iteration process than a linear line (Runeson et al. 2012).

Clarke’s and Raun’s six 6 phases analysis procedures were adopted (Terry et al., 2017), these are,

1. Familiarization with the data: This phase involved transcribing the audio recording, highlighted in the preceding section, into text files and then repeatedly reviewing the texts for familiarity.

2. Generation of codes: Using the NVIVO software program, the author named essential sections of the text files. Certain segments of data required multiple codes.

3. Construction of themes: To ensure that the theming was right, the author checked the possible themes against the codes and the data set once more.

4. Reviewing potential themes: To ensure that the theming was right, the author checked the possible themes against the codes and the data set once more.

5. Defining and naming themes: The study of the themes resulted in the definition and naming of the thematic plots.

6. Producing the report: The author chose the most appropriate excerpts for the study writing about the research issue and literature, from which the conclusions are drawn.

3.6 Validity Procedures

The reliability of the results is referred to as validity and the degree to which they are not skewed by the researcher's subjective viewpoints, and it is important to keep this criterion in mind throughout the study process (Runeson et al., 2012). According to Shenton (2004), transferability, confirmability, credibility, and dependability (reliability) can all be used to evaluate a study's validity.

3.6.1 Credibility

Shenton provided guidance on how to gain credibility. These are some criteria he shared,

- The analysis must accomplish what it was created for. It must do so by adhering to well-established procedures such as data collection and analysis.

- Triangulation entails a variety of data collection techniques and sources. Shenton also indicated that the researcher could request responses from service providers as well as service recipients.

- Another approach is to use iterative questioning during the interview to evoke a comprehensive response from participants.

- To ensure the consistency of the data, member tests were recommended during the interview and after transcription.

This research took the requisite steps to achieve the conditions mentioned, and as a result, it is reliable.

3.6.2 Transferability

This applies to how easily the study's results can be extended to other contexts. These study findings can be transferred to all parts of the world managing sanction policy by the US government. A sufficient description of the case has been provided to ensure a smooth transfer of knowledge.

3.6.3 Reliability

The researcher must maintain a chain of evidence in order to be reliable. The records and procedures used in the analysis are referred to as the 'the chain of evidence.' Replicating the original findings is a worthwhile exercise for a different investigator to engage in for those findings to be relevant. Additional research is now possible because of the large depth of information available.

3.6.4 Confirmability

Confirmability implies that results must represent participants' ideas and experiences rather than the researcher's prejudices. It is found that the confirmability requirements were met during the research process. Triangulation, as discussed earlier, is one of these requirements. The requirements for confirmability are met in this study.

3.7 Summary

This chapter focused on the methodology used in this study. It discussed the case study as an appropriate design, detailing how the research questions were created. It went on to clarify how the study data was obtained and how the data was analyzed using Larke and Raun's six-phase procedures. Secondly, it was discussed how the research's validity is determined.

4 Result

4.1 Introduction

The case and subject chosen, as well as the data collected, are all detailed in this chapter of the research. It explains in detail how Nvivo software was used to analyze interviews. Additionally, it provides a thorough summary of the findings of the interviews.

4.2 Case and Subject Description

Since there is no universally accepted standard for know your customer (KYC) legislation, various banks will have different documentation standards for their corporate clients. There is a difference in the amount of interaction expected between corporations and their financial institutions during the Know Your Customer (KYC) phase. FIs reported contacting corporate clients an average of four times during the KYC compliance process. In 2017, financial institutions with annual revenues of more than $10 billion invested $150 million, up from $142 million in 2016. Over the next 12 months, they expect CDD/KYC spending to increase another 13%. (*KYC Compliance: The Rising Challenge for Financial Institutions*, 2017), while corporates reported contacting them an average of eight times.

Another problem is security issues, partly because the documentation needed for KYC includes personal documents (such as passports, national IDs, proof of address) of company directors, which is very confidential information and subject to strict legal binding according to GDPR. The World Bank and the CCAF (Cambridge Centre for Alternative Finance) conducted a regulatory survey, which found that a recent regulatory survey conducted by the World Bank and the CCAF, nearly half of regulators have taken steps to promote digitalization in financial services, prompting a greater regulatory emphasis on KYC (*Regulating Alternative Finance: Results from A Global Regulator Survey*, 2019). Facilitating or enabling electronic KYC (eKYC), or simplifying KYC processes and procedures, allowing the use of digital identities, digital/electronic signatures, streamlined and/or digital customer due diligence (CDD) tests (such as through the use of facial recognition), and allowing providers to digitally onboard customers are some of the measures that have been proposed.

Although several regulators have taken a soft approach to enact the above steps by issuing and offering structured guidelines, others have chosen to enact fully formulated regulations. For example, in the United Kingdom, the Financial Conduct Authority (FCA) issued guidelines on how retail financial institutions can use digital authentication to accept scanned documents and selfie match images to verify identities. The Central Bank of Malaysia (BNM), on the other hand, released a structured eKYC policy document to help and promote the use of eKYC technologies and virtual onboarding in Malaysia.

All of these legislative changes present a new challenge for businesses, which must not only keep up with the latest developments, but also devote precious time and money to complying with any new regulations. Although digitalization improves sustainability and business continuity, it also increases the risk of financial crime, such as market manipulation and fraud. As a result, risk management and KYC controls are becoming increasingly important, especially for those working in highly regulated industries like finance and banking. Digitalization is presenting a range of implementation challenges, such as delayed or failed business processes and transactions, as change is never quick. Though the study is mainly based on the European financial arena, it could relate to most of the part of the world. The analysis was done with the data gathered from one European bank and one fintech.

KYC process, including document gather, verifying documents, filing the KYC report, are all done by the KYC specialist. They take help from Relationship Managers regarding the communication with the customers. KYC team is generally part of the group business support division. Group business support division handles all the back-office operations done for the front office operations. KYC cell is segmented into 4-5 teams depending on the company. ODD, CDD, EDD, document research team, data analyst team, offboarding team are part of the whole KYC process. This research aimed to fully comprehend the existing verification system's problems, discover how the implementation of blockchain technology may enhance existing processes, investigate the factors that may obstruct the technology's effective implementation, and, finally, create a structure to direct the technology's adoption for KYC verification. The interviews were with those who cope with the current process on a daily basis including several KYC analysts and specialists who are experts in blockchain with a degree in IT. Due to confidentiality, the real names have been omitted from the transcription.

4.3 Presentation of Findings

This segment dives deep into the results of the data collected and analyzed from the interviews and offers interpretations. The interview discussed the topic of the previous chapter, but it is worthwhile to mention that most of the questions were open-ended in nature and split into six sections.

The first section was designed to learn about the respondents' backgrounds to evaluate the credibility of their answers, and the following sections were designed to elicit responses that were compatible with the research questions. The interviews' audio recordings were transcribed into texts compliant with Nvivo software. Following the transcription, the text files were imported into Nvivo software, and codes were applied to them. Inductive and deductive procedures are combined in the encoding scheme. To put it another way, the codes were created based on the research questions as well as the problems that arose from the data collection. Following that, the codes were classified into thematic areas as shown below :

- 01_Understanding current system
- 02_Aspects to improve
- 03_An improved KYC process
- 04_Factors of evaluation
- 05_Challenges of implementation
- 06_Ways to overcome the challenges

4.3.1 General Description of the Respondents

This segment provides a quick overview of the respondents who were chosen to take part in the interviews. The respondents for this study included people who have direct experiences with processes in their daily activities, as stated in section 4.2. The aim of the first segment of the interviews was to learn about the positions they held and the roles they played. The subsequent discussions revealed that the respondents have years of experience in roles that enable them to have a high level of involvement in KYC verification process. Most of them have experience of 1-3 years, judging that it is quite a new field for the banks and fintechs. As a result, it is reasonable to assume that the respondents are well and could contribute meaningfully to the analysis.

4.3.2 Establishing the Implication of Blockchain Technology

As the methodology of the study, this study was designed based on the case studies to further understand the process of KYC verification in the current system of banking and find out the enhanced and improved way of KYC verification based on blockchain technology. To narrow down the study on the implication of blockchain technology on the KYC verification among financial institutions, several sub-research questions were developed to get the best answers to the problem. Among all the SRQs, '**SRQ1**: How to establish the implication of blockchain technology on the KYC management of Financial Institutions?' was focussed on the most to get to the core objective of the study. The other SRQs being '**SRQ2:** How to determine the benchmark to measure the performance of the blockchain-based KYC verification process?' and '**SRQ3:** How would the implementation of the blockchain-based KYC face operational and legal challenges?', the interview questions were based on these sub-research questions to garner the best results out of the respondents for the research objective and then code the results and group them into several themes to develop the findings for the study. Considering the themes as the results of the interview as presented in section 4.3, they are described and defined in details in the following sections.

4.3.3 Understanding of the Current System of KYC

The implementation of any improvements requires a thorough understanding of the existing process. As a result, it is important to answer the question, "What are the current conditions in KYC verification process prior to the implementation of blockchain technology?" The literature on modalities in current verification process was reviewed in the earlier stages of this project. Through the findings of the interviews, this segment examines the applicability of the same to the case of a European bank. To address the questions 'What is the manual KYC process?' and 'What aspects of implementation would be considered as an improvement of KYC system?', it is obligatory for this work to go through the details of the current system and understand the differences in the area of implementations between the current manual system and an improved KYC process.

Communication: Most of the respondents said they communicate via RMs; if RMs approve the line of communication, the specialists communicate via email. But in a special case, they communicate via phone call. No one from the KYC team visits the customer or has an F2F meeting with the customer. One respondent described the process like this, "*In my team we were told that we are not allowed to directly contact our customer. First, we need to get permission from Relationship Managers (RM); if RM allows then we can contact. We contact them by email, if needed, sometime we can make we can call them as well. But upon RM approvals, it differs from customer to customer; sometimes customers are too busy. So it's better that RM contacts them directly. Because we are working from the back office, we don't have physical contact with the customers. But RMs know the customers.*"

Source of Information: For the source of information, the respondents use public sources and some approved private sources. Public source means national business registry, the national portal for the residents, for example, virk.com (Denmark), retriever.se (Sweden). The private sources are the sources like Orbis, Dow Jones. Also, the information that can not be found online or ID documents are retrieved from the customer. One respondent said, "*I collect the information from various public or non-public sources, and of course, we ask many questions to customers, and we receive most of the information from the customer*."

Validity of the document: According to the compliance rule, there are some legal obligations about the validity of the documents. For example, personal address proof can not be older than 3 months, and for business accounts, ownership documents can not be older than 3 months. Sometimes an ODD case takes more than three months to complete; thus, the bank asks for the same documents again from the customer. One respondent said, *"I need to ask the customer for the same document after three months if I can not finish. It is very frustrating for me and also for the customer."*

Compliance: KYC is used for assessing customer risk level and a legal obligation for adhering to AML regulations. Every bank does the KYC process just to follow the compliance. Banks also have their own compliance team who ensures that the KYC process is being done maintaining the government rules. Respondents mentioned that work instructions and processes are written by the compliance team. Every country has a different legal system so, the compliance rules for them are different from each other.

GDPR: GDPR ("General Data Protection Regulation") is a very important factor in the KYC verification process. The European banking industry must follow the rules of GDPR as it was implemented by the European parliament (Radley-Gardner et al., 2016). GDPR ensures the data privacy of any personal information. Without the consent of the customer, no bank or FI can use the information of a person which not publicly available. One respondent said, *"Data privacy, that's a tricky one because we have GDPR laws. So, handling data, ensuring privacy and security is the most difficult part of our process; of course, nobody wants to give out sensitive information; also, we can not search on Google by using a personal name. Later, they might come and ask us about the reason for searching, which might end up in suing the bank!"*

Time Consuming: The current process is very time-consuming, according to all the respondents. It can take up to 6 months just to finish one single ODD or high-risk ODD case because of all the constraints of the process. One respondent said, *"The way we do our verification in our organization at the moment takes quite a long time. Sometimes it takes more than three months. And on that time, we have to upload all of the new documents again."*

Customer Dissatisfaction: Among the respondents, contradictory opinions were found about customer dissatisfaction. Some said their customers are satisfied with the current process according to the customer feedback. Some said the customers are dissatisfied, but they are just getting on with it because they do not have any alternative.

4.3.4 Aspects of Current System to be Improved

Regulation: From the accumulated studies and the conducted interviews, the regulation has been considered as a tough aspect to improve the overall KYC process as the current law is almost resistant to the adaptation of any new technological disruption. And even if the regulation gets adapted with the disruption, the procedure will take too long for the adjustments that usually no financial institutions can afford as millions of transactions and customer onboarding occur simultaneously. And the current regulations in the manual procedure are too tedious as the verified documents take too much time to get feedback for the authorization leading to customer dissatisfaction. And in the fast-paced world, the regulations are continuously evolving for newer purposes and requirements that the financial institutions might find hard to adjust with while constantly updating all the existing documents. Referring to this aspect, one of the respondents highlighted the concern as: *"I will say the toughest part of these is the ever-changing movement in regulation. In this world, the requirements are always evolving. So what we were working* *on today obviously might not be correct tomorrow. So due to the changes in regulation, we need to update all the existing documents that we have in order to comply to the actual or the current law."*

Automation: Most of the respondents could not stretch enough on the aspect of automation for the KYC process as this will lessen a lot of hurdles for both the financial institutions and the customers as well. As per the manual procedure, collecting, storing, verifying the data, and complying with the regulation while doing the verification takes up a lot of time and increases the complexity of the procedure. To spot the importance of implementing automation in the current system, one of the respondents said, *"Automation and a central database would be great. When I say automation, I mean will click a button in my system, will interact with another system to get the information without any human intervention, like nobody will see the sensitive information of that particular person, it will be all between the systems, and so we won't have any problems with privacy or security of data."*

While highlighting the importance of automation, the respondents emphasized on the concern of human intervention and so on the security concern of data privacy. Following these concerns, the concern of technological error comes accordingly as the slightest of an error might discard the whole process and cause overall system loss. Hence, one of the respondents overshadowed on the aspect like: *"But, sometimes, I don't trust fully automation process, because this is a very sensitive issue, even the slightest mistake could lead to a huge amount of fine from the auditors. I think even with automation, there should be a human supervisor."*

Data Security: In the manual structure, after collecting the necessary documents from the customer, creating an internal database with the verified documents is necessary to keep the process smooth. Yet, it might be worrisome for the customers sometimes if they do not feel safe enough with the document sharing process with the financial institutions considering the risk related to the third-party platform. Highlighting on this sector of improvement, one respondent shared his concern as below: *"We need to provide a platform that is secure. And so, even if it's a platform that is internal for us. We can not deal with it if it's a third party company; we need to make sure that the customer is comfortable uploading their private information on these system."*

Time Effective: Time effectiveness has come out to be a very important factor from the interviews and the earlier studies as well for the KYC procedure in every segment of the banking industry as customer identity verification is very time-sensitive for the organizations. The hurdle of repeating a single verification procedure every single time a customer wants to join a new program makes it very time-consuming and tedious as the organization has to go through all the documents complying with the regulation over and over again. And contacting the customers for the documents every time becomes another time-consuming challenge as per one of the respondents: *"…..this takes a quite long time. And if we need to contact the customer, sometimes it takes more than two months, three months, and you cannot poke them every second because they are very valuable to our organization."*

Customer Convenience: User experience is one of those aspects that require close attention from any organization. And when it comes to financial institutions, every journey of a customer to onboard on a new program is crucial for the organization to retain the customer's satisfaction. Keeping the customer's convenience in mind for document sharing, communication with any relationship manager, and avoidance of repetitiveness of the same procedure is highlighted in one of the respondents comment as follows: *"Customer convenience needs to be improved, there is no point of asking the same customer same question every year, it hurts the bank's approach to improve user experience."*

Data Sharing: Data sharing is crucial for a bank or any financial institution. But on top of that, having access to the data is more critical in the current system of KYC verification. To get access to a certain information, one might have to go through several protocols and still not have the certainty of having access to the database. And to improve this aspect of the current manual system, a centralized database should be utilized among or within the financial institutions as per one of the respondents: *"I would do it more centralized inside the bank because you probably already know here that maybe there is the information somewhere in the bank, but it's in some other department, and you don't have access to the databases, or you just don't know that they could have this information."*

Moreover, while focusing on the interoperability of the current system in terms of data sharing globally, or just among several financial institutions, one respondent shared his point of view for the European banks as: *"To think more globally. I think that at least* *some European banks could share the information among them in spite of having GDPR."*

Communication: Communication being the key to the sensitiveness of the current process of KYC, most respondents shared their views by emphasizing the importance of timely communication among the stakeholders even if it requires heavy usage of technology to make the process faster and training of the employees. Raising the concern towards this aspect, one interviewee responded that, *"I think our communication needs to be faster and direct, RMs are busy people, customers are busy people, so it takes a long time for them to reply with information; thus, the process lengthens."*

4.3.5 Improved KYC Verification Process

Although the things that could be improved have already been discussed, the answers will be used to figure out what an ideal DLT based KYC verification method entails and what void blockchain can fill.

Customer Convenience: In the improved KYC process that is based on blockchain technology, customer convenience would be the first thing to keep in mind through making the entire labor-intensive process very smooth by reducing the hassle of data sharing to just one time. The DLT based system would allow the customer to share the document only once with the first financial institution, and the rest of the document verification and sharing would be managed by that organization through installing the verified documents into the public ledger.

Automated: As most of the respondents in the interviews have shown their interests towards having an automated system of KYC verification to have a less labor-intensive and hassle-free process, one of the respondents who specializes in the area of blockchain have elucidated the aspects of a blockchain-based improved KYC process that would automate the system for all the stakeholders to a major extent, if not completely.

Tamper Proof: The DLT based system of KYC verification would require an overall tamper-proof process to earn the credibility to the customers. The documents shared by the customers are very delicate and sensitive for the financial institutions to protect their clients' data privacy. Hence, a tamper-proof process is crucial. And the improved KYC system, according to one respondent, would ensure the security of the data of a customer even while sharing the documents for the first time with any financial institution as the documents would not be stored or shared in the ledger while sharing until they are hashed and verified. Another aspect of the system being tamper-proof is the concern of the regulator party. In the enhanced KYC process based on blockchain technology, the system would be decentralized while having a regulatory authority for each institution to routinely check the verified documents of the customers and prevent any kind of anti-money laundering acts. But this might raise the concern of data breach for some legislatives or countries. Therefore, a centralized system might also be improved for risk management where only one entity or authority would be specialized to regulate all the documents centrally and undergo all the KYC responsibilities, and no third-party regulator would have unlimited availability to the database. Any financial institution looking for access to any customer's KYC verification record would have to be permitted by the central authority. This Trusted-Third-Party (TTP) regulatory body might enhance the system to be more tamper-proof, but this would not allow the FIs to actually know their customers. But some literature considers the risk of a corrupt regulator much less considerable compared to the benefit of having higher financial stability of an institution achieved through the constant supervision of a regulator in a decentralized system. However, the reverse engineering of the smart contracts and the bugs in the smart contracts might result in an unintentional exposure of the customer's information.

Accurate: Accuracy of any system is a must-have for providing error-free, continuous services to the customers. Though any technology-based system would have bugs that might corrupt the system, the blockchain-based KYC verification process ensures the installment of large-sized documents with higher accuracy than that of the manual system, which is more time inducive and might create manmade errors for the massive sets of documents and data sharing. But the unintentional errors caused by the bugs in the smart contracts should be considered as exceptions.

Easier Document Retrieval: Though it is almost impossible to alter the data in a network like Ethereum than in a private network because of the existing large mining community, data sharing and retrieval would be made very easy for the customers and the banks in a permissioned ledger as it would only require a key to decrypt the hash code values of the documents for any institution that would be provided by the customer. According to one of our interviewees, having a copy of the document package of each customer locally stored by the financial institutions in their databases, enhances the data retrieval process to be more efficient and faster.

Cost-Effective: According to most of the respondents, for both processes in a DLT based KYC verification, cost-effectiveness would be ensured for both the customers and the financial institutions. In a decentralized system, the cost would be proportionally distributed among the financial institutions using the core KYC verification data recorded by the first financial institution. Once the customer approves, the FI then pays up its fraction of payment to the customer’s smart contract, and its account's public key from which the payment was made would be added to the list of onboarded financial institutions in the smart contract. The transaction would occur in cryptocurrency which then is compensated by the smart contract equally to the participating institutions. Thus, the cost would eventually be lessened by the system for all the stakeholders as the documents would be copied and stored in the local databases for the financial institutions for future usages as well. Even in the centralized KYC verification process, though the specialized entity would require additional charges for the core KYC verification, the cost of conducting the KYC would be removed from the banks, and so the fees would be lowered for the customers as well.

Time-Effective: The customer would be required to go through the KYC verification every time he or she wanted to build a new relationship with any financial institution in the manual procedure of KYC. Whereas the improved KYC process would require the customer to share the document only once with the first financial institution, and the verified documents would later be shared through the blessing of the distributed ledger technology with other organizations with the consent of the customer. This would reduce the hassle of lengthy communication and stuck verification process to a greater extent.

Less Workload: If the centralized system of blockchain-based KYC allows only one central authority or regulator-operated KYC office to approve or reject a customer’s document, this would reduce an overall set of the workload from the financial institutions of creating an entire financial entity for conducting the core KYC verification of the customer’s documents. All an FI would need to do is get permission from the central authority for accessing the document packages of the clients. On the other hand, the decentralized method would allow the financial institutions to copy and store the accessed verified documents in their local databases that would cut down a massive workload from the FIs of repetitively collecting and verifying the documents for the customers and continuously communicating with the clients asking for the necessary documents.

4.3.6 Factors of Evaluation

Via interviews, respondents were asked for their opinions on how to assess the verification process's reliability, effectiveness, and convenience. Some respondents said they didn't have well-established standards for assessment in their units when asked how they would assess the systems. Every individual, on the other hand, had an opinion on how the verification method should be judged.

Effectiveness

- **Accuracy:** Most of the respondents noted that accuracy of information is a very important measure for proper evaluation. The condition of being a good process includes being accurate. According to the answers, one of the most significant explanations for accuracy is that any wrongly done verification procedure could jeopardize the institution's reputation in the eyes of external auditors. One respondent said, *"Also, we check the accuracy of the cases done because when FSA (Financial Supervisory Authority) comes, they will check the accuracy of our work."*
- **Reliability:** According to the answers, reliability is closely linked to accuracy and refers to a verification outcome's ability to reflect the truth in a KYC scenario. Although inaccuracy is the result of unintended mistakes, unreliability is the result of deliberate attempts to distort the reality. As a result, reliability can be used to assess the efficacy of evaluations.
- **Cheaper:** An effective solution or process is always budget-friendly. A respondent said, *"If we talk about efficiency, every team has an allocation of human resources, so every team has a budget. If the budget exceeds the performance, then cost-cutting happens."*

Efficiency

- **Quality Assurance:** All the ODD, CDD, EDD cases pass through an internal quality check. With the QC pass, the process can not progress to finalization. Quality check is done by the senior experts who are subject matter experts and have a lot of experience in the field of compliance. Quality assurance result can be delivered in three ways, 1. Pass , 2. Fail , 3. Pass with comment.

- **Number of Cases:** The number of case done per week or month is the most used scale of performance evaluation. Several respondents have talked about this. Every team has a KPI of its own. KYC team also has a target to match. One respondent said, *" How do I measure it well? we can measure by the amount of cases done, we can measure the amount of cases prepared for weeks, or we can measure it in amounts of cases, or amount of requests that were received from the customer."* According to another respondent, the number of high-risk cases with different characteristics could be used to measure. She said, *" I think that we can measure the efficiency for instance by the number of cases filed with sanction exposure. So, by the number of something suspicious that can be measured, and that was found in relation to the clients."*

- **Lead Time:** The time between the beginning of a process and its completion is referred to as lead time. So, the total time from starting a case to finishing a case is considered as the lead time. Lead time could be different for different risk level cases.

Convenience

- **Customer Contact:** For the KYC process, contacting the customer is an essential issue, but most of the time, banks contact the customer several times that might create a negative impact on customer convenience. One respondent said, *"For example, a measure could be. As for how many times in a year, they have to give the same information to different counterparties. Getting this data could show that wasting our time on the same act."*

- **Feedback:** The knowledge, insights, problems, and input shared by the community about their interactions with the business, product, or services are known as customer feedback. Even (and especially) when it's negative, this feedback can help enhance the customer experience and empower positive change in every industry. Customer feedback is also used as a criterion for evaluation. One respondent said, *"We do have customer surveys, first of all, and we can get* *the feedback directly from the customer, and then we see if our statistics improve after they use the system."*

4.3.7 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 are 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."*

Different Legal Requirement: All the respondents agreed to this challenge that in the absence of a common KYC standard, different countries have non-identical ID verification compliance rules. The customer might not understand the inconsistent requirements in different countries and would send legally invalid documents. In order to rectify the mistakes, banks would have to contact the customer one more time. One respondent spot a light on this matter, saying,*"Let's say for Denmark. We don't need a certified passport, and it was for Sweden we need a legally certified passport. So the main challenge is that they're different. It's in we have to comply with all the requirements if the customer has products in different countries."*

Redundancy of Jobs: The majority of the respondents shared this concern about being jobless or unemployed if blockchain or any kind of automated process is implemented.
One respondent shared his concern like this, *"If we use blockchain, then there will be less need for people like me because most of the process will be automated. And it will take less time. So one specialist can finish 10 cases, whereas they're finishing three cases right now, per week. So efficiency will be increased. Thus, it will create redundancy in the job market."*
Though, another respondent said that we would still need some human intervention as well, so it's not that everybody would lose their jobs. She also stated that the people who can keep up with the new procedures or processes would find another role eventually.

Consumption of Energy: One respondent expressed his concern over the power needed to create and run the blockchain. Any overuse of electricity is considered harmful to the environment. He said, *"I know it takes an enormous amount of energy to create a block; they are created by big data centers. Using too much energy is certainly good for the environment."*

Operational Challenge: One respondent who is a software developer illustrated his concern over the way of updating information on the blockchain. Data can not be modified or altered on the blockchain network, so it will be a hassle to update the information. For example, if a customer wants to change his name, he/she would need to create a new block containing that information. The respondent said, *"Blockchain would be a blessing only if they were able to compensate for the negative effects of obsolete records. At the moment, we've been introduced to a secure banking process in which banks gather all customer data and store it in a large database. And they're the ones in charge of updating every document on a yearly basis, and we were worried those documents wouldn't be updated on time on blockchain. The customer has to create a new block with the transaction."*

4.3.8 Ways to Overcome the Challenges

Authorization System: One IT specialist opined that the issue with the GDPR could be resolved with a customized authorization system. An authorization system would obstruct an unwanted person or group of persons from acquiring KYC information. He said, "*If we could provide access or some kind of authorization system where some specific system or a specific person will be able to access that specific customer information, the legal risk can be avoided*."

Customer Push: Interview analysis showed that a push from the customer side would boost the possibility of implementing the new process. Participants from the interview said that if banks from Europe start to use blockchain, the customers in North America might demand the same improved process. Then the banks would be under pressure from the customer to implement blockchain or any kind of improved process.

Skill Based Training: Several answers during the interview emphasized the crucial importance of professional development in preparation for the implementation. Additionally, a critical review of the results in this area indicates that improving staff skills for more active positions would alleviate the fear of redundancy.

Common KYC Standard: Several interviewees conveyed that having a different KYC regulation is a problem. There is no common standard of law; without a common law, there is no point in having a solution that is accepted worldwide.

Acceptance from Authority: An interviewee who is a team lead of a KYC team revealed a bigger picture of how the blockchain implementation could be accelerated. He informed how the legal system works in banks. Apparently, the compliance rules are part of a long line of chain. In order to bring change, a decision has to come from the top. He said, *"There are several organizational authorities that deal with these issues at the general level; then it cascades down to the legal systems of every country. So, it's unless this blockchain system is accepted at the operational level from an international body like the EU or the US or anything, it is difficult to implement it."*

Awareness: The interview process showed that blockchain is quite new for most of the respondents, and they do not know much about it. Though they said, it is being known right now because of the rise of cryptocurrencies, especially bitcoin. A KYC expert tagged blockchain as a maze and expressed that, "*Though blockchain is quite a maze to most of the people, well, it is a maze to be honest, if we can make it easier to understand to the stakeholder and make them aware of using it, the implementation will be much easier."*

4.4 Summary

The chapter began by explaining the case and the topic under investigation. Following that, it included a brief summary of the interviewees in order to explain the relevance of their contributions, and finally, it presented the interview results. The following tables summarize the results for each of the sub-research questions. The SRQs were broken down even further into simpler questions. The questionnaire items were derived from the simplified questions.

Table 4: Summary of the Findings

Research Questions	Findings from the Interviews
SRQ1: How to establish the implication of blockchain technology on the KYC management of Financial Institutions?	
What is the current state of the KYC process prior to the implementation of blockchain technology?	• The process is very time-consuming. • Validity of the documents are time-sensitive. • Compliance rules vary from country to country. • Sources of information are both public and private. • The communication process has too many layers. • GDPR is followed while handling data • Customer dissatisfaction level relies on the frequency of contact for KYC purposes.
What aspects of the current KYC verification process could be improved?	• Time Effectiveness • Regulation • Automation • Customer Convenient • Data Sharing • Data Security
What would be considered an improved KYC verification process?	• Faster Process • Tamper Proof • Automation • Customer Convenient • Less Workload • Easier Document Retrieval • Accurate • Cost-Effective

Table 4 continued here.

Research Questions	Findings from the Interviews
SRQ2: How to determine the benchmark to measure the performance of the blockchain-based KYC verification process?	
What are the major indicators of effectiveness in the KYC verification process?	• Accuracy • Reliability • Cheaper
What are the major indicators of efficiency in the KYC verification process?	• Lead Time • Number of Case • Quality Assurance
What could be considered as a convenient KYC verification process?	• Customer Contact • Customer Feedback
SRQ3: How the implementation of the blockchain-based KYC would face operational and legal challenges?	
What are the key challenges related to the legal and compliance framework?	• Legal Risk • Different Legal Requirement
What are the key challenges related to operational process and interoperability?	• Resistance to Change • Educating Customers • Training of the Employees • Redundancy of Jobs • Interoperability • Trust Issue • Consumption of Energy
What are the key ways to overcome the challenges?	• Common KYC Standard • Skill Based Training • Customer Push • Awareness • Acceptance from the Authority • Authorization System

5 Conclusion and Future Work

5.1 Introduction

The findings of the study are discussed in this chapter. The results will be consolidated and recommendations after gathering broad information from reviewing relevant documents and conducting interviews with participants on the research questions. The chapter also discusses the implications of the findings, the study's shortcomings, and potential areas for future studies.

5.2 Recommendations

The decentralization and immutability of Blockchain technology make it an effective and secure method for verifying transactions stored there. However, practical steps should be implemented in order for it to be enforced effectively. As a result, the following recommendations for the implementation of blockchain technology for KYC verification process in European financial institutions and non-bank financial institutions (NBFIs) could be practiced.

5.2.1 Automation

In the improved KYC system, as per the respondents and the earlier studies, there should be one home bank that would initiate the core KYC verification process for a customer for the first time, and the customer would share the necessary documents with the bank from a customer portal network, through the system’s surface. The verified documents would then be stored in the permissioned ledger with an e-Signature, in a document package that would contain all the previously hashed documents, including the certificate of approval consisting the verification result (accepted/rejected). After the core KYC verification, the customer would be provided with a new account consisting of a public and a private key and a smart contract of the account containing a list of the public keys of all the onboarded financial institutions' wallets.

The process would be automated for different financial institutions as they would be able to share data through the smart contracts with each other. If another FI wants to get access to that customer’s verified documents stored in the ledger by the home bank, it would need to have the consent of the customer. If the customer approves, the other FI would get access to the keys of the customer and get the smart contract’s address formed by the home bank. After reading the smart contract, FI/NBFI would get the e-signed digital certificate with the core KYC verification result of the customer, including the list of the previously onboarded FIs with the number of their public keys. Further access is given to the FI into the document package created by the home bank. This way, all the onboarded institutions would be able to store their customers’ data locally with complete anonymity of the stakeholders, and the system would therefore be partially automated by reducing the time-intensive communication hassle and laborious verification process for both parties.

5.2.2 Feasibility Study

Feasibility studies are critical in determining whether a planned project is feasible (Mintzberg et al., 1976). FIs and NBFIs need to run at least three types of feasibility studies for the concept of a new blockchain-based KYC process. Primarily, the feasibility assessment would start with the technical feasibility to determine whether the whole concept is technically possible or not. Our findings from the interview regarding technical feasibility showed that Even if the public ledger only contains the hash values of the documents and the keys to the document package, no bank would be comfortable storing their customers' information on public ledger as it might appear very apparent to the insider frauds or financial terrorists to decrypt the document packages from the historical patterns of the transactions using the hash codes and the keys. Having a copy of the document package of each customer locally stored by the financial institutions in their databases enhances the data retrieval process to be more efficient and faster. Therefore, it is recommended for each financial institution to have a unique account for each customer in a permissioned ledger to have better data protection and easier document retrieval for the banks.

The profit comes from the customers for every business; therefore, they are the most valuable stakeholder or any process. Banks ought to run a survey among the customers (personal banking and business banking) to converge the customer expectation and potential criticism about the new process. Reluctance from the customers would certainly be obstructive to the implementation of the blockchain-based KYC verification process. Another type of study is the legal feasibility study. As it was mentioned several times that legal standard among the countries are non-identical and not concrete, it is very crucial to run an analysis on the basis of legal requirements to determine if the project would be compliant with major authoritarian figures (EU, US).

5.2.3 Common Standard of KYC

From the result analysis, it was evident that the lack of a common standard of KYC laws is making the whole process cumbersome and extensive. Though for the core KYC law, most of the countries follow the Patriot Act 2001 of the United States of America, the identification and verification process are different in the majority of the countries. The distinction includes legality of ID copies, time-sensitivity of the document, additional information needed for the beneficial owners of the business, and so on. Also, there are a considerable amount of differences in data privacy laws between Europe and the US that are the result of having GDPR in Europe. In Asia and Africa, the KYC laws are not considered strict and not properly followed. It is highly unlikely that the countries would decide to have a common standard for the whole world, but it could be expected that the major financial hubs in the world would follow a common standard. This practice would ease up the KYC verification process regardless of having a manual one or a blockchain-based one.

5.2.4 Pilot Project

Although the technology got obvious potential, the feasibility of a KYC utility must be evaluated in order to determine its true applicability (Eamonn & Chia, 2018). In terms of risk-minimizing and cost management, creating a pilot project for any financial institution before incorporating the technology entirely in the system would be wise. This would reduce most of the risks of failure to the actual system and allow the organization to have amendment plans for future implications. This futuristic technology of blockchain might be very new to the banking industry, and having run a pilot project before any implementation would allow the firm to instantly disrupt the project and amend with technological disruption. As of 2017, KPMG International created a proof-of-concept prototype in collaboration with three financial groups: HSBC, OCBC, and Mitsubishi to put the blockchain platform's technical aspects to the test and understand the suitability of the DLT based KYC verification process. Like this tested prototype, a pilot project for any FI must consider the results of the system’s functionality, scalability, and data security. Relationship anonymity among the stakeholders should be a factor, while the stability and responsiveness of the platform should also be checked during voluminous information flow. The pilot project must align with the desired transaction or data-sharing time for the organizations, whereas the data must remain confidential while providing access to only the limited parties with actual authorization codes. The percentage of cost savings of the DLT based system compared against the current system must also be measured to get a better understanding from the pilot project and forecast possible implementing solutions for the bank.

5.2.5 Collaboration

Collaboration enables participants to accomplish more together than they might separately, benefit greater groups of individuals, and develop both personally and professionally (Green & Johnson, 2015). For the successful implementation of such a crucial and complex project, collaboration among the banks is an indispensable step. Major banks in the world have the monetary power to run such a project, but with collaboration, the journey would be more progressive and cheaper. Think tanks and specialists from different institutions would create an insightful and innovative result. Several collaborations around the are already in progress. For example, collaboration among HSBC, OCBC, and Mitsubishi in 2017 provided significant knowledge about the process. In Europe. BNP Paribas Fortis, Belgian Banks Belfius, ING Belgium, and KBC, four vital Belgian FIs, have teamed up for the collaboration to use a blockchain application named KUBE for sharing information about the business clients. It would make it easier for companies and banks to verify and maintain corporate identities. As a result, KUBE will be able to provide services to companies faster while also stepping up its battle against money laundering and fraud. Due to KUBE, the Belgian financial sector would be the first to use blockchain for company identification on a large scale. (*Four Major Banks and Isabel Group Join Forces to Streamline Business Services with KUBE*, 2020).

5.2.6 Educating Customers and Employees

According to the previously mentioned challenges of implementing blockchain-based KYC utility, redundancy in the jobs would increase the rate of resistance to the change in terms of technological adaptation among the customers as well as the employees of the FIs. Hence, it would be recommended for the FIs to create an efficient and effective strategy of educating the existing employees by getting them acquainted with the new technology through various mentorship programmes according to the level of difficulty required for each employee. Even for the customers, creating the awareness about the new technology would be very crucial. Otherwise, earning their trust for a financial institution to share their documents in a completely new system might get difficult. Therefore, any program specialized for the customers should consist of various workshops or monthly seminars including newsletters emailed to the customers on a monthly or quarterly basis. Instead of cutting down on the number of existing, unskilled employees, educating and upskilling them would allow the new technology to avoid critical situations like unemployment or employee displacement.

5.2.7 Research & Development

Research and development (R&D) is a broad term that refers to businesses' practices for developing and launching new solutions or products. It's usually the first step in the process (Kenton, 2021). In both the public and private sectors, R&D is often correlated with creativity. Research & development enables a business entity to stay one step ahead of its competitors. An innovative and progressive process like the use of blockchain in KYC verification would certainly require extensive research and development to make it suitable for daily practices. Spending money on R&D is an investment for the company in the long run. Profit from R&D might come from different sources, like cost minimization of own process, improving quality of the services, income/licensing fees from the legal patent, and so on. A groundbreaking improvement in the use of blockchain in KYC verification from research & development would assuredly put an institution top of the race.

5.3 Impact of the Study

The purpose of this study was to thoroughly review the current KYC verification process in European FIs and NBFIs in order to identify the issues. Following that, we investigated the use of blockchain technology to solve the problems and established guidelines for its adoption in the case of KYC verification. The study also defined the characteristics of effective verification and identified specific areas in which technology-assisted enhancement is needed. This research discusses a new method for achieving effectiveness, performance, and convenience in KYC verification in the context of European FIs and NBFIs.

Although the cost and complexity of KYC verification around the world continue to rise, this research aims to make the most significant changes to the existing structure.

5.4 Limitation

This study was not excluded from the flaws associated with this research design, despite its commitment to following the suggested rigorous methodological course. The method of analyzing qualitative data is often questioned because it is focused on the researcher's judgment and interpretation, as opposed to the collection of rules and formulas used in quantitative data analysis (Patton, 1999). During the study, there is the possibility of skewed interpretations of the results, which may have an impact on the conclusions.

When it comes to the transferability of qualitative research results and conclusions, there are many points of view. The failure to extend the findings of qualitative studies to a larger population is a challenge for positivists. However, the probability of a transfer ought not to be completely disregarded (Shenton. 2004). Another group of researchers argues that the reader should determine if the analysis is transferable and that an author should provide adequate contextual information. As a result, although this research has given sufficient background, it is impossible to conclude that the results can be applied.

Due to the COVID-19 situation, the physical interview was not possible. All the interviews were done over MS Teams or phone calls. Due to the confidentiality and sensitivity of the information shared during the interviews, the author had to convince the respondents about complete anonymity; thus, the actual identification has been removed from the transcription. However, the recording of the interviews contains respondents' name, workplace, and some off-the-record conversations that would be against the code of conduct of their workplace. For this reason, the audio files and transcription have not been added to the thesis. However, in need of authenticity, the audio and transcription could be shared upon request with permission from the interviewee.

5.5 Future Research

To improve the implementation process and understand the consequences of implementing blockchain, more research is needed. FIs and NBFIs must understand how blockchain adoption can affect their confidentiality, data protection, and other sensitive details. This expertise would be needed to determine which rules and policies should be followed in order to avoid privacy violations.

Since the research was conducted in Europe, the results might not be applicable elsewhere. It's possible that similar studies in other countries on other continents would produce different results due to their legal systems being different. Further research in more cases is essential and recommended for transferability. This research may also be replicated using the evidence presented to verify its credibility.

The aim of this study was to provide a framework for the adoption of blockchain technology for KYC verification process, but it did not go into detail on how to implement it. A new research design is proposed to make the solution development and deployment easier. Although adoption addresses how FIs and NBFIs should embrace and incorporate technology into their processes to provide more reliable, accurate, and seamless services, actual implementation research would address how to configure and manage the technology as well as train employees on the operations to enhance productivity.

References

Alammary, A., Alhazmi, S., Almasri, M., & Gillani, S. (2019). Blockchain-Based Applications in Education: *A Systematic Review. Applied Sciences*, 9(2400), 18.

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

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

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

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/

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*, 55–81. 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

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.pdf

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

Crosby, M., Pradan, P., Sanjeev, V., & Vignesh, K. (2016). *BlockChain Technology: Beyond Bitcoin*. *2*, 16.

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

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

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

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

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

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

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/

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

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.

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

Garnaut, R. (2015). Introduction to the Forum on the Murray Financial System Inquiry. Australian Economic Review, 48(2), 177-179. doi: 10.1111/1467-8462.12108

Geldenhuys, D. J. S., & Hoffman, A. J. (2012). A digital signature issuing and verification system for auto identification tokens. *2012 International Conference on Wireless Communications, Networking and Mobile Computing, WiCOM 2012*, 1–7. https://doi.org/10.1109/WiCOM.2012.6478280

Grech, A., & Camilleri, A. (2017). Blockchain in Education. *Joint Research Centre (JRC)*. https://doi.org/10.2760/60649

Green, B. N., & Johnson, C. D. (2015). Interprofessional collaboration in research, education, and clinical practice: Working together for a better future. *The Journal of Chiropractic Education*, *29*(1), 1–10. https://doi.org/10.7899/JCE-14-36

Gustafsson, J. (2017). Single case studies vs. multiple case studies: A comparative study

Hanbar, H., Shukla, V., Modi, C., & Vyjayanthi, C. (2020). Optimizing e-KYC Process Using Distributed Ledger Technology and Smart Contracts. In A. Saha, N. Kar, & S. Deb (Eds.), *Advances in Computational Intelligence, Security and Internet of Things* (pp. 132–145). Springer. https://doi.org/10.1007/978-981-15-3666-3_12

Holbl, M., Kamisalic, A., Turkanovic, M., Kompara, M., Podgorelec, B., & Hericko, M. (2018). EduCTX: An Ecosystem for Managing Digital Micro-Credentials. 2018 28th EAEEIE Annual Conference, EAEEIE 2018, 1–9. https://doi.org/10.1109/EAEEIE.2018.8534284

Indian business prepares to tap into Aadhaar, a state-owned fingerprint-identification system. (2016). Retrieved 13 April 2021, from https://www.economist.com/business/2016/12/24/indian-business-prepares-to-tap-into-aadhaar-a-state-owned-fingerprint-identification-system

Ismail, L., Hameed, H., Aishamsi, M., Aihammadi, M., & Aidhanhani, N. (2019). Towards a blockchain deployment at UAE University: Performance evaluation and blockchain taxonomy. *ACM International Conference Proceeding Series,* Part F148153, 30–38. https://doi.org/10.1145/3320154.3320156

Kabir, S. M. S. (2016). Methods of data collection. In Basic Guidelines for Research: An Introductory Approach for All Disciplines (First, Vol. 14, Issue 2, pp. 201–276). https://doi.org/10.5005/jp/books/13075_10

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

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

Kenton, W. (2021). *Why Research and Development (R&D) Matters*. Investopedia. https://www.investopedia.com/terms/r/randd.asp

KYC [DLT]—The hottest KYC projects in trade finance. (2020, November 2). *Trade Finance Global*. https://www.tradefinanceglobal.com/posts/kyc-dlt-the-hottest-kyc-projects-in-trade-finance-yes-they-use-blockchain/

KYC compliance: The rising challenge for financial institutions. (2017). Thomson Reuters. https://d3kex6ty6anzzh.cloudfront.net/uploads/39/3973a2f5f7888855106b5d244df6192d0750c803.pdf

Legget, K. (2012, February 4). Poor Data Quality: An Often Overlooked Cause Of Poor Customer Satisfaction Scores. *Forrester*. https://go.forrester.com/blogs/12-02-04-poor_data_quality_an_often_overlooked_cause_of_poor_customer_satisfaction_scores/

*l*Underwood, S., 2016. Blockchain beyond bitcoin. Commun. ACM 59 (1), 15–17. https://doi.org/10.1145/2994581.Werbach, K., 2018.

Manav Gupta. (2017). Blockchain for Dummies, IBM Limited Edition. In For Dummies

Mintzberg, H., Raisinghani, D., & Theoret, A. (1976). *The Structure of "Unstructured" Decision Processes*. https://doi.org/10.2307/2392045

Moyano, J., & Ross, O. (2017). KYC Optimization Using Distributed Ledger Technology. *Business & Information Systems Engineering*, *59*(6), 411–423.

Murphy, S. (2016). Unlocking the blockchain: a global legal and regulatory guide. In *Norton Rose Fulbright*. http://www.nortonrosefulbright.com/files/unlocking-the-blockchainchapter-1-141574.pdf

Nakamoto, S. (2008). Bitcoin: A Peer-to-Peer Electronic Cash System. www.bitcoin.org

Parra Moyano, J., & Ross, O. (2017). KYC Optimization Using Distributed Ledger Technology. *Business & Information Systems Engineering*, *59*(6), 411-423. doi: 10.1007/s12599-017-0504-2

Parra-Moyano, J., Ross, O., & Thoroddsen, T. (2019). Optimized and Dynamic KYC System Based on Blockchain Technology. *International Journal of Blockchains and Cryptocurrencies*, *1*, 1. https://doi.org/10.1504/IJBC.2019.10021398

Patel, D., & Ganne, E. (2020). *BLOCKCHAIN & DLT IN TRADE: WHERE DO WE STAND?* World Trade Organization (WTO). https://www.wto.org/english/res_e/booksp_e/blockchainanddlt_e.pdf

Patton, M. Q. (1999). Enhancing the Quality and Credibility of Qualitative Analysis.

Peihani, M. (2016). Basel Committee on Banking Supervision. Brill Research Perspectives in International Banking and Securities Law, 1(1), 1-87. doi: 10.1163/24056936-12340001

Radley-Gardner, O., Beale, H., & Zimmermann, R. (Eds.). (2016). *Fundamental Texts On European Private Law*. Hart Publishing. https://doi.org/10.5040/9781782258674

REGULATING ALTERNATIVE FINANCE: RESULTS FROM A GLOBAL REGULATOR SURVEY. (2019). The World Bank Group. http://documents1.worldbank.org/curated/pt/266801571428246032/pdf/Regulating-Alternative-Finance-Results-from-a-Global-Regulatory-Survey.pdf

Runeson, P., Host, M., Rainer, A., & Regnell, B. (2012). Case Study Research in Software Engineering. John Wiley and Sons Ltd. http://www.worldcat.org/title/case-study-research%20in-software-engineering-guidelines-and-examples/oclc/828789615&referer=brief_resu

Shenton, A. K. (2004). Strategies for ensuring trustworthiness in qualitative research projects. Education for Information, 22(2), 63–75. https://doi.org/10.3233/EFI-2004-22201

Shyft Network Inc. (2021). https://www.shyft.network/

Sultan, K., Ruhi, U., & Lakhani, R. (2018). Conceptualizing blockchains: Characteristics & applications. Proceedings of the 11th IADIS International Conference Information Systems 2018, IS 2018.

Swan, M., 2015. Blockchain: Blueprint for a new economy. O'Reilly Media, Inc. ISBN:978-1-4919-2049-7.

Tapscott, A., Tapscott, D., 2017. How Blockchain is changing finance. Harvard Business Review, March 1st, 2017. [Online] Available from:https://hbr.org/2017/03/how-Blockchain-is-changing-finance(Accessed: April 5th, 2020).

Tara, L. (2013, September 13). JPMorgan to spend $4 billion on compliance and risk controls: WSJ. *Reuters*. https://www.reuters.com/article/us-usa-jpmorgan-risk-idUSBRE98C00720130913

The use of DLT in post-trade processes: Advisory Groups on Market Infrastructures for Securities and Collateral and for Payments (p. 40). (2021). European Central Bank.

The use of DLT in post-trade processes: Advisory Groups on Market Infrastructures for Securities and Collateral and for Payments (p. 40). (2021). European Central Bank.

Thomson Reuters 2016 Know Your Customer Surveys Reveal Escalating Costs and Complexity. (2016). Retrieved 16 April 2021, from https://www.thomsonreuters.com/en/press-releases/2016/may/thomson-reuters-2016-know-your-customer-surveys.html

Thomson Reuters 2017 Global KYC Surveys Attest to Even Greater Compliance Pain Points. (2017). Thomson Reuters. https://www.thomsonreuters.com/en/press-releases/2017/october/thomson-reuters-2017-global-kyc-surveys-attest-to-even-greater-compliance-pain-points.htm

Xu, M., Chen, X., & Kou, G. (2019). A systematic review of blockchain. *Financial Innovation*, *5*(1), 27. https://doi.org/10.1186/s40854-019-0147-z

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2018). Blockchain Technology Overview. https://doi.org/10.6028/NIST.IR.8202

Yang, W., Garg, S., Raza, A., Herbert, D., & Kang, B. (2018). Blockchain: Trends and Future. In K.

Yin, R. K. (2009). Case Study Research Design and Methods. In Applied Social Research Methods Seiries (Vol. 5). http://cemusstudent.se/wpcontent/uploads/2012/02/YIN_K_ROBERT-1.pdf%5CnISBN 978-1-412296099-1

Yoshida & M. Lee (Eds.), Knowledge Management and Acquisition for Intelligent Systems (pp. 201–210). Springer Nature Switzerland AG. https://doi.org/10.1227/01.NEU.0000320425.55569.21

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017a). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017.

Appendices

Appendix 1: Interview Questions

Section 1: Introductory discussion

1. Please introduce yourself briefly.
2. What is your role in this unit?
3. How long have you been in this position?

Section 2: Questions about procedures in the current system of KYC process?

1. How do you gather or receive the information needed for CDD/ODD?
2. How do you contact the customer?
3. Can you finish ODD/CDD if you are unable to verify the document? If no, why?
4. How do you access other data sources? Are they approved and reliable?

Section 3: Questions about automation in workflow

1. How would you describe your computer skill? Basic, Average, Highly Skilled.
2. What type of automation process are you currently using?
3. What do you know about centralized data sharing?
4. Do you think centralized data sharing for KYC would be a positive step to improve the process?

Section 4: Questions about challenges in the current system

1. What do you perceive as challenges of the current system of verification and data sharing?
2. How are you dealing with those obstacles you face in the current system?
3. What aspect of the current system do you think needs to be improved for more effectiveness?
4. Do you think the current system is effective and efficient? How do you measure that?
5. Would you say that your customers are usually pleased with the current process? A. If Yes, how can you tell when they are satisfied? B. If no, what are the reasons for dissatisfaction?

Section 5: Understanding the respondents' knowledge about the blockchain

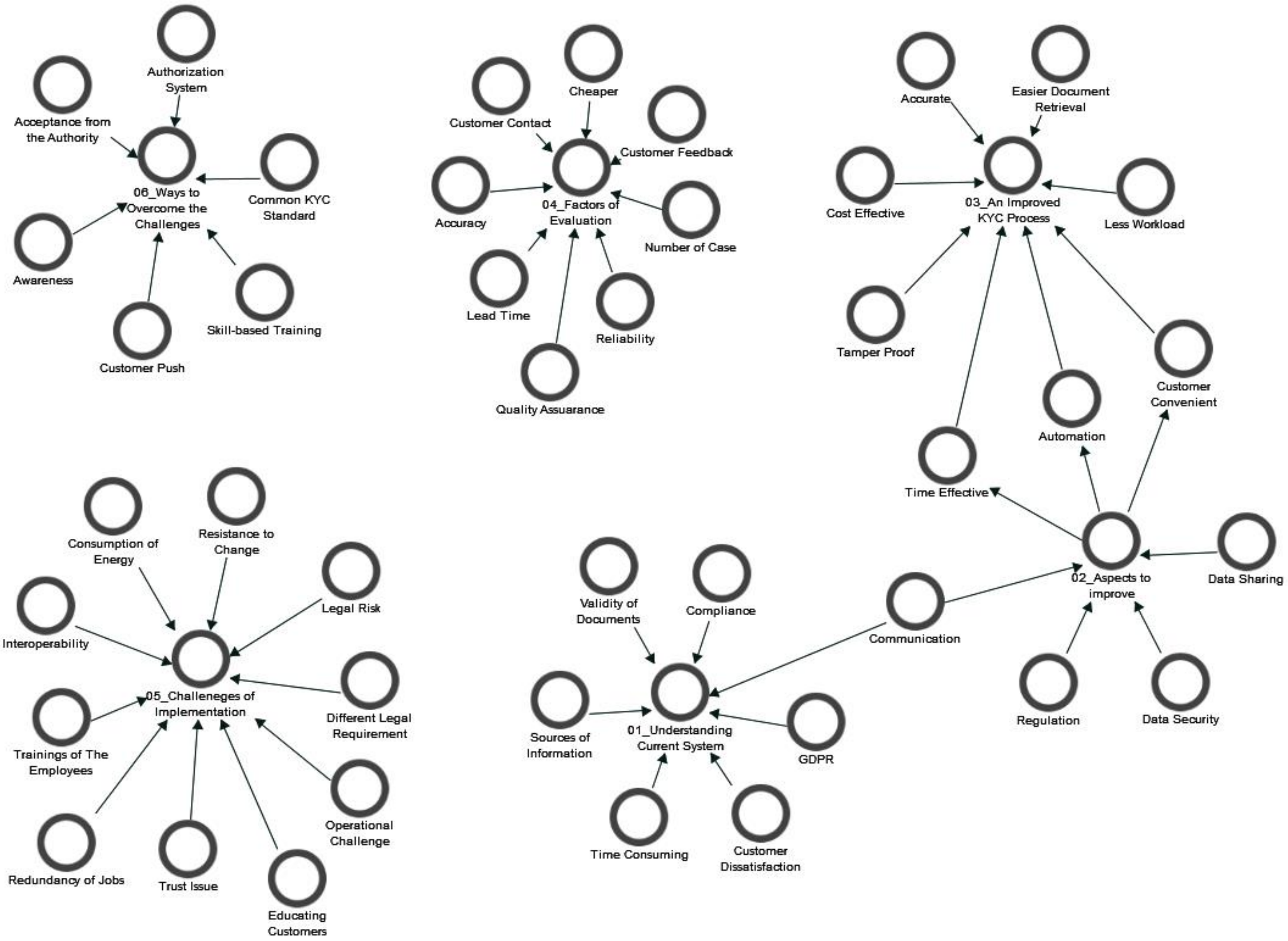
1. What do you know about blockchain technology? Do you trust blockchain technology? (I would explain briefly if the interviewee does not know about blockchain, based on explanation, we would have further discussion)
2. Do you think it will benefit the document and identity verification process in your unit if blockchain is implemented?
3. Do you think there might be major operational and legal risk issues with the application of blockchain to the current system?
4. How do you think the problems could be tackled?

Section 6: Questions about challenges of implementation

1. What do you think of challenges about the different legal requirements for different countries?

2. Do you think Internal QA and Government Audit will be less vigilant about the authenticity of the information?
3. Do you think banks will share the data among them? If yes, will there be any interoperability issue? If no, explain, please.
4. Would you feel comfortable with the new process?
5. Do you think that your role in the current verification system will be enhanced/affected by integration to blockchain?

Appendix 2: Thematic Plotting of Code Categories



Appendix 3 – Non-exclusive licence for reproduction and publication of a graduation thesis[1]

I Hafizul Islam

1. Grant Tallinn University of Technology free licence (non-exclusive licence) for my thesis "ADOPTION OF BLOCKCHAIN ON KNOW YOUR CUSTOMER (KYC) VERIFICATION PROCESS: A THEMATIC ANALYSIS ON EUROPEAN BANKING INDUSTRY", supervised by Alexander Horst Norta.
   1.1. to be reproduced for the purposes of preservation and electronic publication of the graduation thesis, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright;
   1.2. to be published via the web of Tallinn University of Technology, incl. to be entered in the digital collection of the library of Tallinn University of Technology until expiry of the term of copyright.
2. I am aware that the author also retains the rights specified in clause 1 of the non-exclusive licence.
3. I confirm that granting the non-exclusive licence does not infringe other persons' intellectual property rights, the rights arising from the Personal Data Protection Act or rights arising from other legislation.

10.05.2021

[1] The non-exclusive licence is not valid during the validity of access restriction indicated in the student's application for restriction on access to the graduation thesis that has been signed by the school's dean, except in case of the university's right to reproduce the thesis for preservation purposes only. If a graduation thesis is based on the joint creative activity of two or more persons and the co-author(s) has/have not granted, by the set deadline, the student defending his/her graduation thesis consent to reproduce and publish the graduation thesis in compliance with clauses 1.1 and 1.2 of the non-exclusive licence, the non-exclusive license shall not be valid for the period.