NOVA IMS Information Management School

MGI

Master Degree Program in

Information Management

An investigation on how blockchain technology can transform the Know-Your-Customer (KYC) process.

Liam Lamey Botha

Dissertation

presented as partial requirement for obtaining the Master Degree Program in Information Management

NOVA Information Management School
Instituto Superior de Estatística e Gestão de Informação
Universidade Nova de Lisboa

NOVA Information Management School
Instituto Superior de Estatística e Gestão de Informação
Universidade Nova de Lisboa

AN INVESTIGATION ON HOW BLOCKCHAIN TECHNOLOGY CAN TRANSFORM THE KNOW-YOUR-CUSTOMER (KYC) PROCESS.

By

Liam Lamey Botha

Master Thesis presented as partial requirement for obtaining the Master's degree in Information Management, with a specialization in Information Systems and Technologies Management

Supervisor: Vitor Duarte dos Santos

November 2023

STATEMENT OF INTEGRITY

I hereby declare having conducted this academic work with integrity. I confirm that I have not used plagiarism or any form of undue use of information or falsification of results along the process leading to its elaboration. I further declare that I have fully acknowledge the Rules of Conduct and Code of Honor from the NOVA Information Management School.

Knysna South Africa – 20/11/2023

ACKNOWLEDGEMENTS

First and foremost, I would like to express my deepest gratitude to my parents, Anthon and Suyenne Botha for their continuous emotional support and guidance throughout my whole academic journey. Their overwhelming encouragement has not only been instrumental in my academic success but has also allowed me the invaluable opportunity to pursue my master's degree abroad in Portugal, creating an unforgettable and enriching experience. Secondly, I would like to thank my brother Sven Botha, whose dedication and hard work have been a constant inspiration. He has been a shining example that hard work truly pays off.

Lastly, I extend my gratitude to my supervisor and professor Vitor dos Santos, for providing invaluable knowledge and guidance throughout my academic journey at NOVA IMS. His mentorship has played a crucial role in shaping my educational experience, and I am truly appreciative of the insights and support he has shared.

ABSTRACT

The Know-Your-Customer (KYC) process plays a crucial role in combating financial fraud and money laundering. The KYC process involves validating a customer's identity through the inspection and analysis of various forms of documentation. This mandatory process must be completed before a financial institution and a customer can establish a business relationship. However, the current procedures are outdated, as they prove to be extremely costly and time-consuming, which hinders the overall efficiency of the process. The adoption of blockchain technology has the potential to transform this process by eliminating redundant tasks and establishing a platform where KYC information can be seamlessly shared across various financial institutions. In this article, we undertake a systematic literature review employing the Systematic Mapping Process to identify prior research conducted within the scope of the KYC and blockchain. Throughout the systematic literature review, we present the findings of previous researchers and emphasise the similarities and differences of their findings. Lastly, we present a conceptual model for a subscription-based KYC system utilising blockchain technology. The model aims to enhance and expand upon previous research conducted within this scope. This model incorporates tokens as a means of payment between financial institutions and central authorities, who are responsible for overseeing the KYC process. This model utilises a permissioned blockchain along with an InterPlanetary File System (IPFS) network for documentation storage. It encourages collaboration among financial institutions, as it enables the distribution of the customer's KYC verification status among entities operating on the platform.

KEYWORDS

Blockchain; Know-Your-Customer; KYC; Distributed Ledger Technology; Identity Verification.

Sustainable Development Goals (SGD): Decent Work and Economic Growth

INDEX

LIST OF FIGURES

LIST OF TABLES

LIST OF ABBREVIATIONS AND ACRONYMS

AES	Advanced Encryption Standard
AML	Anti-money laundering
CID	Content Identifier
CFT	Countering the Financing of Terrorism
DDoS	Distributed Denial of Service
FATF	Financial Action Task Force
FI	Financial Institution
GDPR	General Data Protection Regulation
ICO	Initial Coin Offering
IPFS	InterPlanetary File System
KYC	Know Your Customer
SCM	Supply Chain Management
SLR	Systematic Literature Review

1 INTRODUCTION

1.1 BACKGROUND & PROBLEM IDENTIFICATION

KYC, also known as “Know Your Customer” or “Know Your Client”, is a mandatory process that financial institutions are required to perform to identify and verify a customer's identity when establishing a financial relationship. The aim of this process is to prevent financial institutions from being used for illicit criminal activities, such as money laundering, terrorist financing, and corruption. This process helps financial institutions understand the nature of the customer's activities and identify the potential risks involved in engaging with a particular customer.

The current KYC process places a significant burden on financial institutions, as this process is described as “costly, inefficient, and inconvenient for customers” (Schlatt et al., 2022). According to a survey conducted by Thomson Reuters, the estimated average yearly costs for financial institutions to meet KYC obligations are around $60 million, with some companies even spending upwards of $500 million (Harrop & Mairs, 2016). However, these costs can significantly escalate due to fines issued to financial institutions for breaching anti-money laundering (AML) and KYC regulations (Parra Moyano & Ross, 2017).

The current process is not only a significant financial burden but also time-consuming for both the customer and the financial institution involved. On average, it takes 26 working days to onboard a corporate customer, with some corporate customers experiencing an onboarding time in excess of 4 months (Harrop & Mairs, 2016). This process tends to increase in duration based on the size of the entity being dealt with. No business may be conducted between the two entities until this process is completed, resulting in an opportunity cost for both entities involved (Parra Moyano & Ross, 2017). According to the survey conducted by Thomson Reuters, 89% of customers indicated that they had a negative KYC experience (Harrop & Mairs, 2016).

The current KYC process in place is inefficient, as this process is repeated each time a customer wishes to engage in a new relationship with a financial institution. Due to the current inefficiencies of the KYC process, alternative solutions have been proposed and studied. Some of these alternative methods include using big data analytics for risk reduction, as well as employing cluster analysis to identify illicit criminal activities and money laundering (Parra Moyano & Ross, 2017). Another commonly discussed solution is the use of blockchain technology within the KYC environment. There has been a substantial increase in the amount of research performed that explores developing a model for implementing the KYC process using distributed ledger technology. By using blockchain technology, KYC information can be stored in a distributed ledger, allowing customers to share their KYC status with all the financial institutions with which they intend to engage (Parra Moyano & Ross, 2017).

By conducting this research, we aim to answer the following research question.

RQ1: *“How can the application of blockchain technology be used to improve the current KYC process and are there any limitations associated?”*

In order to accurately answer the research question, various sources of research in this field need to be identified and analysed. This will enable us to identify any similarities and differences based on previous research already conducted.

1.2 OBJECTIVES

The purpose of this research is to provide a comprehensive study on how blockchain technology can improve the KYC process. Existing research will be analysed to compare different frameworks and models proposed from previous research. The previous research conducted in this field will be used as a guideline when formulating our conceptual model.

To achieve the main goal of this research paper, we have defined the following intermediate objectives:

- Identify existing frameworks or conceptual models proposed based on previous research.
- Identify the benefits and limitations of a blockchain-based KYC process - highlight any potential improvements or limitations based on previous research conducted in this field.
- Examine the ethical issues with storing sensitive customer information on a distributed ledger.
- Provide a set of guidelines on how blockchain technology can improve the KYC process.
- Outline areas of potential future research within this area.

1.3 IMPORTANCE & RELEVANCE

The concept of adopting blockchain technology to transform the KYC process is an emerging area of research, thus previous research conducted has mostly focused on conceptual studies (Parra-Moyano et al., 2018). This study aims to uncover the potential benefits and obstacles hindering financial institutions from adopting blockchain for the KYC process. Additionally, we will examine the ethical considerations related to data storage and handling of confidential customer data.

The purpose of this research aims to accelerate the use of blockchain for KYC by promoting a conceptual model that offers an improvement over previous research conducted. The adoption of blockchain technology is expected to lower the cost of conducting the KYC process for both financial institutions and customers. In doing so, customers only need to verify their identity once and are capable of sharing their KYC status with multiple financial institutions. The goal is to improve the efficiency and convenience of the current KYC process for all parties involved.

The current research exploring the application of blockchain in KYC is extremely limited. This study aims to fill research gaps and encourage financial institutions to adopt blockchain technology. By reducing costs, financial institutions can distribute resources to improve customer satisfaction. This research has the potential to have a positive impact on the field.

Many companies are adopting blockchain technology to improve operations and reap its benefits. However, the current KYC process is outdated and in need of revision. This study aims to address this issue and to find solutions using blockchain technology.

2 LITERATURE REVIEW

2.1 KNOW-YOUR-CUSTOMER (KYC)

2.1.1 Context & Concept

The KYC process falls within the greater scope of anti-money laundering (AML) and countering the financing of terrorism (CFT) compliance measures which financial institutions employ to protect themselves and customers against licit criminal activities.

The concept of KYC was first introduced in 1970 by the United States government, as an effort to combat money laundering and tracking down illicit funds (Mulligan, 1999). The 'Bank Secrecy Act (BSA)' which was enacted in 1970, "required banks to maintain certain records and reports, thus creating a paper trail useful to law enforcement agencies investigating criminal, regulatory, and tax evasion schemes" (Mulligan, 1999). These regulations have been continuously updated and have since increased in complexity. However, the term "KYC" only became popular in the late 1990s.

Traditional KYC processes involve manual collection and verification of customer data through various means such as identity documents, utility bills, and other official records. This approach has been widely used by financial institutions for many years and is still in use today. However, it has been criticised for being time-consuming, slow, and prone to errors.

Over the last 30 years, the KYC process has transformed with the rise of digitalisation within the financial sector. What once was a tedious manual, paper-based process, has evolved into a more digitalise and automated one. These advances have improved the accuracy, efficiency, and cost effectiveness of the KYC process. In an attempt to diminish the risk of identity fraud, advanced digital solutions such as biometrics and artificial intelligence (AI) have been utilised to enhance the precision of customer data. However, there is still considerable room for further improvement within the current process.

Below, Figure 2.1 illustrates the current KYC process adopted by majority of financial institutions. This figure illustrates that a customer must complete the KYC processes multiple times for each financial institution they wish to engage with. Each financial institution with which the customer engages incurs a cost for performing the KYC validation process. If a customer wishes to only engage with a single financial institution, then no inefficiencies are caused. However, large companies often engage with multiple financial institutions and experience extensive delays waiting for KYC approval.

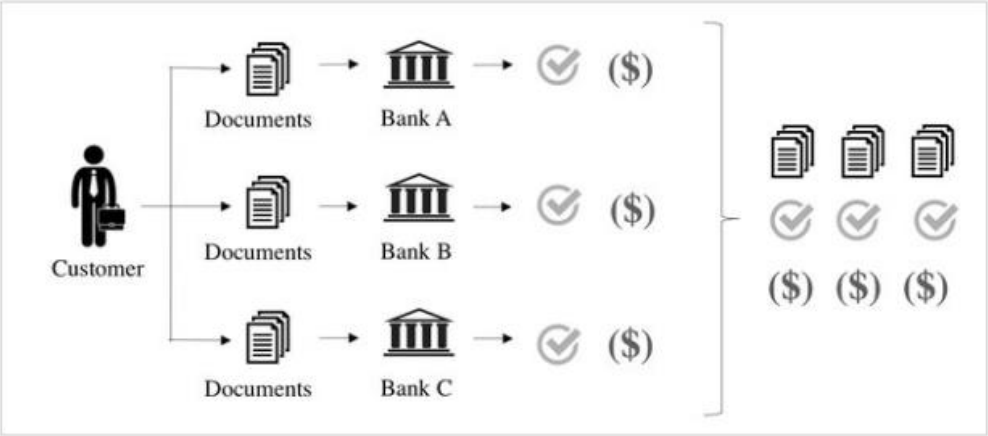

Figure 2-1 – Current KYC Process (Parra Moyano & Ross, 2017)

2.1.2 Processes & Approaches

Currently, the Financial Action Task Force (FATF) is responsible for setting the international standard for KYC. Typically, the KYC process includes the collection and verification of a customer's personal and financial information. This information can be gathered in the form of a government-issued ID, proof of address, and the source of funds. The current KYC process typically consists of several components. These components include:

1. Customer Identification Programs (CIP) – Firms need to collect a client's name, date of birth, address, and identification number using reliable sources of documents or data. This data is then verified, and customers are screened to ensure they do not appear on any government sanction lists (KYC3, 2018).

2. Customer Due Diligence (CDD) – During this process, a risk assessment is performed based on the customer's available data to detect any suspicious behaviour or identify the nature of the relationship between the customer and the firm. Continuous monitoring of financial transactions is carried out during this process to identify any suspicious activity (KYC3, 2018).

3. Enhanced Due Diligence (EDD) – In cases where customers are deemed to be a higher risk, a more in-depth monitoring and investigative research approach is employed (KYC3, 2018). EDD is utilised for customers deemed high-risk, such as those from high-risk jurisdictions, engaged in high-risk business sectors, or with a history of financial crime.

4. Ongoing Monitoring – During this process, a customer's information and risk profile are continuously monitored and updated throughout the relationship with the customer.

This enables the financial institution to detect any changes in the customer's behaviour or activities which may indicate an increase in risk. This process is vital as it allows financial institutions to stay updated on the risk associated with a particular client (KYC3, 2018).

The above-mentioned components are crucial for financial institutions as it helps them to comply with AML and CTF regulations. Failure to comply with these regulations may result in hefty fines being issued for lack of compliance. It is essential that these components are thoroughly conducted as it allows financial institutions to maintain their reputation.

Before a new financial relationship between the customer and the financial institution can be established, this process needs to be completed, and the customer's documentation has to be either validated or rejected (Parra Moyano & Ross, 2017). Currently, this process must be repeated each time a customer wishes to engage with a new financial institution. This leads to reoccurring costs in both money and time from performing a duplicate process. By using blockchain technology, KYC documentation can be stored in a distributed ledger which will allow customers to share their KYC status with all the financial institutions which they intend to work with. This improved system allows significant cost and time reductions. This paper aims to highlight the potential benefits of using a blockchain-based KYC approach, as well as provide an in-depth comparison of the previous research conducted within this field.

2.1.3 Challenges & Opportunities

Although the KYC process has somewhat transformed from a paper-based to a digitalised approach, there are still many issues with the current system in place. Below, we will highlight some of the challenges faced with the current KYC system.

1. Time-Consuming – Due to the complexity of the KYC process, the time taken to onboard a client can take up to an excess of 4 months (Harrop & Mairs, 2016). This results in delays for both the financial institution and the customer, as no business transactions can take place until the KYC process has concluded. Due to the high risks associated with some customers, additional measures and monitoring may be required which increases the overall duration of the process (Malhotra et al., 2022).

2. High Costs – Currently, the KYC process is performed separately by each financial institution which a customer wishes to engage with. This results in large costs being incurred by financial institutions to conform with the regulations of the process. On average, financial institutions spend upwards of "$60 million" per year to perform the KYC process (Harrop & Mairs, 2016). The current process is very resource-intensive and necessitates significant investments in technology and skilled personnel to complete the process. These costs faced by financial institutions can be further amplified if fines are imposed for not conforming to the correct regulations (Malhotra et al., 2022).

3. Complexity – The complexity of the KYC process can vary based on the regulations and requirements imposed by each country and industry. Companies operating in multiple jurisdictions may encounter numerous additional challenges when conducting the KYC process.

4. Human Error – During the onboarding process, there may be human errors involved during manual data entry which may influence the KYC process outcome for trustworthy users. Because of these errors, customers might have to redo the KYC process, which leads to increased costs for the financial institution conducting the process. The main cause for this error is the lack of an automated system (Malhotra et al., 2022).

5. Data Privacy and Security – The KYC process involves the collection and storage of copious amounts of sensitive personal data and documents. It is vital that companies handle and store this information in a secure manner. In the event of a data breach, customers may lose trust in the financial institution, which could ruin the reputation of the company. Financial institutions need to ensure that they are using adequate measures, such as encryption when it comes to securing sensitive data.

6. Lack of Standardisation – Various countries and industries have their own requirements and regulations when performing the KYC process. This often makes it very challenging for financial institutions to conform to these regulations, especially when there are transactions between customers from different nations (Malhotra et al., 2022). In the article by (Harrop & Mairs, 2016), it is mentioned that 87% of banks and 75% of investment managers believe that "regulatory and legislative change is the most influential factor for their KYC process". Financial institutions are required to stay up to date with the latest laws and regulations; however, this can prove to be difficult as regulations are constantly changing and evolving.

To conclude, the current KYC process has numerous limitations and inefficiencies, providing an opportunity to research and suggest new methods and models to improve it. One such possibility we will be investigating is the utilisation of blockchain technology in the KYC process.

2.2 BLOCKCHAIN

2.2.1 Concepts & History

The concept of blockchain technology was first introduced by Satoshi Nakamoto in 2008 (Nakamoto & System, 2008). In the paper, Nakamoto introduces the concept of Bitcoin, which is described as a "decentralized digital currency" which enables direct transactions without any intermediaries (Nakamoto & System, 2008). Nakamoto mentions a decentralized ledger which records transactions in a secure and transparent way, which is today known as "blockchain".

Blockchain stores information in what is known as a "block". These blocks are linked together to form a chain of immutable records. Each block contains a cryptographic hash of the previous block in the chain. The hash value is generated using a complex algorithm which takes all the data within the block into consideration when generating the hash. Once a block has been added to the chain it is considered verified and it cannot be altered. Transactions on the blockchain are transparent, allowing any individual to view them (Mohanta et al., 2018). The first block in the chain is always referred to as the "Genesis Block" (Nakamoto & System, 2008). Blockchain users can identify each other using public keys and securely exchange messages and conduct transactions through cryptographic signatures utilizing their private keys (Glaser, 2017).

Blockchain technology operates on a decentralised basis, eliminating the need for a central authority. The network is made up of numerous nodes, each keeping a complete copy of the blockchain, creating a distributed system where every node holds a full version of the blockchain and can verify transactions (Hayes, 2023). A new transaction is broadcasted to the network and validated by multiple nodes. After enough nodes have confirmed the transaction, it is added to a block and appended to the blockchain. The newly created block is then broadcasted to all nodes in the network, which update their copies of the blockchain with the new block added (Hayes, 2023).

One of the major key components of blockchain is the consensus mechanism, which is responsible for adding new blocks to the chain and ensuring that the network of nodes reaches an agreement regarding the blockchain's state. Various consensus mechanisms have been employed in blockchain networks, with the most popular ones including Proof of Work, Proof of Stake, Delegated Proof of Stake, and Byzantine Fault Tolerance (Hayes, 2023). A consensus mechanism enables various untrusted/unknown peers within a distributed environment to reach a common agreement about the current state of the blockchain network. In doing so, it establishes trust between unknown peers and ensures that each block added to the chain represents the agreed-upon truth.

2.2.2 Benefits & Limitations

The following section outlines the key advantages and limitations of blockchain technology to consider before implementing a blockchain-based solution. Understanding the potential benefits and restrictions of blockchain is crucial for making informed implementation decisions. These identified benefits and limitations of blockchain technology will play a vital role in designing a framework for a blockchain-based KYC application.

Benefits of blockchain technology:

1. Security - Blockchain employs cryptographic methods to secure transactions, effectively preventing tampering attempts and strengthening system security against cyber threats (Kshetri, 2017).

2. Immutable - Once a block has been verified and added to the blockchain, it cannot be altered or deleted. This feature ensures a secure and tamper-proof record of transactions, making blockchain ideal for applications that involve sensitive information meant to remain unaltered.

3. Transparency - The transparency and traceability offered by blockchain technology can aid institutions in detecting and preventing money laundering and other financial crimes. The unalterable nature of blockchain ensures that all transactions are recorded and can be traced to their origin, enabling the tracking of a transaction's complete life cycle.

4. Interoperability – Blockchain networks can be made interoperable, enabling them to communicate and exchange information with other blockchain networks. This enables the sharing of customer information across multiple organizations, streamlining the Know Your Customer (KYC) process.

Limitations of blockchain technology:

1. Complexity – Despite its potential, blockchain is still in its early stages of development, and widespread adoption is scarce. Perceived complexity, security concerns, and the absence of clear regulations lead many businesses and individuals to approach blockchain adoption cautiously.

2. Scalability – Many existing blockchain systems face limitations in scalability, causing slow transaction processing speeds and high gas fees (Malhotra et al., 2022). For example, Bitcoin is only able to process 7 transactions per second. This can pose difficulties in handling high-volume transactions promptly, making it unsuitable for widespread usage.

3. Data Privacy – While blockchain technology offers robust security for customer data, it has limited privacy. Transactions are recorded on a public ledger, making customers' personal information accessible to all participants within the network.

4. Interoperability – While Interoperability is one of the advantages of blockchain technology, it can also be a disadvantage. The use of diverse protocols and standards among blockchain systems makes it difficult for them to interconnect. This can hamper their ability to collaborate and may limit their growth prospects (Crosby et al., 2016).

2.2.3 Applications

Although the concept of blockchain technology was initially created for cryptocurrencies such as Bitcoin, it has since been adapted and applied in various areas of informatics as a means to enhance systems (Parra-Moyano et al., 2018). The following section discusses the diverse sectors in which blockchain technology has been applied to enhance operations and promote overall efficiency. The application of blockchain technology extends far beyond cryptocurrency and the Information Technology sector.

1. Supply Chain Management – Blockchain technology has made a significant impact on the supply chain management industry. The use of blockchain technology allows the supply chain sector to be more trustful and reliable by enhancing transparency between the supplier and consumer (Mohanta et al., 2018). In a blockchain network, the absence of a central authority ensures that every member of the supply chain can access equal information, minimizing the chance of deceit and making all dealings transparent and secure. Blockchain technology improves transparency and traceability along the supply chain, allowing goods to be traced as they move through the supply chain. This improves overall quality assurance, as goods can be traced back to their origin, preventing counterfeit goods.

2. Financial Systems – Blockchain technology has facilitated the creation of various digital cryptocurrencies such as Bitcoin, Ethereum, Litecoin and many others. The application of blockchain technology in financial systems has simplified cross-border payments by reducing transaction fees and increasing the overall speed of financial transactions.

3. Healthcare – Blockchain technology plays a vital role in preserving the privacy of patients by securely storing their data in a digital ledger format (Mohanta et al., 2018). Blockchain has the potential to enhance healthcare quality through secure and

streamlined sharing of medical records between healthcare providers. It can also mitigate fraud in the industry through secure and transparent transactions.

4. Real Estate – The traditional real estate process is burdened with risks and time-consuming procedures, involving multiple legal stages and extensive paper documentation. Blockchain and smart contracts can address these issues by providing a centralised system for buying and selling properties without the need for intermediaries. The documents undergo digital verification and validation and are securely stored in a distributed ledger that is visible to all participants (Mohanta et al., 2018).

As previously noted, blockchain technology has numerous potential use cases. In this paper, we will examine the benefits it can bring to the KYC process. While proper implementation of blockchain can lead to meaningful results, designing a blockchain-based system also involves many complexities. Despite these limitations, we believe that blockchain's integration into the KYC process will have a positive impact overall.

3 METHODOLOGY

To conduct extensive research that adds meaning and value in the area of KYC and blockchain development, it is essential to thoroughly analyse the existing research conducted and discover any earlier frameworks that have been developed and proposed. This process involves highlighting the similarities and differences between various research studies conducted within the scope.

To conduct this study, a Systematic Literature Review (SLR) will be carried out, encompassing a comprehensive analysis and evaluation of all relevant research on KYC, blockchain and distributed ledger technology. Data will be gathered from multiple sources; however, finding these sources may be challenging due to the limited research conducted within this field. Therefore, a thorough search and collection process is required. To ensure that the research is meaningful and adds value to this field, well-defined goals and objectives need to be established first. After conducting the SLR, we will propose a conceptual model that builds upon earlier research and enhances it by introducing improvements.

To conduct a thorough and meaningful SLR we will employ the "Systematic Mapping Process" designed by (Petersen et al., 2007) as our chosen research methodology. This methodology is widely used to aid research within the software engineering field. As illustrated in Figure 3-1, the Systematic Mapping Process consists of 5 steps, with each step resulting in its own outcome. The final output of the process is to produce a systematic map.

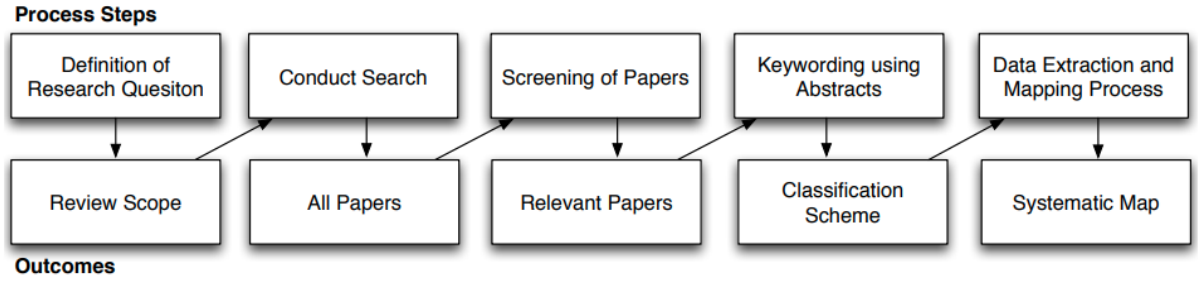

Figure 3-1 – Systematic Mapping Process (Petersen et al., 2007)

1. Definition of Research of Scope:

In this step, we outline the fundamental areas of our research and define the questions we aim to answer through our investigation. The following research question has been formulated, which aligns with the objectives of our study.

RQ1: "How can the application of blockchain technology be used to improve the current KYC process and are there any limitations associated?".

2. Conduct Search for Primary Studies

Before conducting an extensive search of all scientific articles relevant to our research area, we need to select various research databases to aid with the search process. In this step, we identified four different research databases that we deemed to be the most appropriate for our study. The research databases identified are as follows:

- Scopus
- ScienceDirect
- IEEE Xplore
- Google Scholar

These 4 research databases will serve as our main source of data for collecting and analysing relevant research articles. In the next phase, we will create various search terms that will be used when collecting research articles. The following key search terms were employed when searching for research articles that are relevant to our study:

- “Blockchain and KYC”
- “Blockchain and Know-Your-Customer”
- “Distributed Ledger Technology and KYC”
- “Blockchain and Identity verification”

The following search query was created to acquire various research articles:

("Blockchain" AND "KYC") OR ("Blockchain" AND "Know Your Customer") OR ("Distributed Ledger Technology" AND "KYC") OR ("Blockchain" AND "Identity Verification")

The above search query was applied across all four research databases. This query identified any research article containing any of the key phrases within the title or anywhere within the text of the article. The outcome of this process resulted in 2391 research articles identified across the 4 research databases. Table 3-1 illustrates the number of research articles extracted from each research database.

Table 3-1 - Number of research articles extracted from initial search

Research Database	Number of Research Articles
Scopus	692
ScienceDirect	461
IEEE Xplore	78
Google Scholar	1160
Total:	2391

3. Screening of Papers (Inclusion and Exclusion Rules)

The outcome from the initial search resulted in a large set of research articles, however, not all articles identified are directly relevant to our study. For example, some articles identified merely mention our specific search query terms without exploring the core components thereof. Therefore, it is essential to eliminate irrelevant articles. During this phase, research articles were filtered based on their relevance to our research question and objectives. Research articles that did not align with our objectives were removed in order to produce a more accurate SLR.

The following articles were excluded based on these exclusion rules:

- Duplicate articles appearing in more than 1 research database.
- Articles with restricted access.
- Articles that merely mention search query terms and do not cover the core components.

Table 3-2 – Number of research articles after exclusion rules applied

Research Database	Number of Research Articles
Scopus	168
ScienceDirect	11
IEEE Xplore	11
Google Scholar	131
Total:	**321**

4. Keywording of Abstracts

To enhance the overall data quality, research articles were filtered based on their abstract, title and keywords using our search query. This resulted in a more refined and accurate set of research articles. The result of this process further narrowed down our result to 28 research articles, as indicated by Table 3-3.

Table 3-3 – Number of research articles after keywording of abstracts

Research Database	Number of Research Articles
Scopus	11
ScienceDirect	4
IEEE Xplore	3
Google Scholar	10
Total:	**28**

5. Data Extraction and Mapping of Studies

In this step the relevant research articles are organised into categories, facilitating easier comparison and analysis of comparable research articles. By categorising the research articles based on their type of research, we can identify key similarities and differences among them. For our research purposes, articles were categorised into the following categories.

- Models and Frameworks.
- Literature Reviews and Case Studies.

It is crucial to follow specific procedures and methods to make sure that only relevant research articles are considered to maintain high-quality data in an SLR. This procedure is essential as it enables the location and evaluation of all prior significant research. By doing so, aim to conduct a literature review of high value, which will hopefully add significant value to our area of research.

Table 3-4 – Number of research articles per research category

Research Category	**Number of Research Articles**
Models and Frameworks	17
Literature Reviews and Case Studies.	11
Total:	**28**

4 RESULTS & DISCUSSION

The following section offers an in-depth analysis and discussion of the research articles gathered surrounding the topic of KYC and blockchain technology. In the analysis, research articles were categorised and compared based on their core content. These research articles were classified as follows:

1. Models and Frameworks.
2. Literature Reviews and Case Studies.

The identified research articles are categorised together to conduct a more precise and accurate comparison of the existing literature within the scope of KYC and blockchain technology. In this section, we discuss and highlight the key similarities and differences discovered from our analysis of the existing literature surrounding KYC and blockchain.

4.1 MODELS & FRAMEWORKS

The analysis of existing models and frameworks revealed that there are various use cases for user identification and KYC verification that stretch beyond the financial sector. While the majority of the research articles analysed focus on user identification within the financial sector, several articles incorporated user identification for various use cases.

For instance, authors (Feulner et al., 2022) proposed a proof of concept that uses self-sovereign identity for event ticketing systems. The authors (Feulner et al., 2022) designed their solution to combat ticket fraud and scalping. In their proof-of-concept, users store their verifiable credentials in a digital wallet on their smartphones. Users are required to provide these verifiable credentials when buying tickets and entering venues. In order for a user to receive their verifiable credentials, they are required to provide the correct documentation to their KYC provider. Only upon successful verification of documents, will the user receive their verifiable credentials. When purchasing a ticket, a proof request is sent to the user from the use of smart contracts. This request automatically searches for any verifiable credentials that satisfy the proof request. If the verifiable credentials satisfy the proof request, the ticket purchase is completed.

The authors (Sai et al., 2023) designed a “microfinance” application that utilises blockchain technology to connect lenders and borrowers in a decentralised manner. The authors (Sai et al., 2023) highlighted the challenges that many individuals around the world encounter when attempting to secure loans due to factors such as “lack of income and collateral”. These individuals often rely on microloans for financial aid which have high interest rates and are often controlled by loan sharks. In their design, the authors proposed a solution where a central government body is responsible for KYC verification and maintains a database where all citizen data is stored.

In the article by (Sun et al., 2022), the authors investigate how virtual asset services providers (VASPs) are currently being exploited for money laundering and illegal foreign exchange. The authors (Sun et al., 2022) identified that currently, most VASPs lack some sort of user identity management. Therefore, the authors proposed an identity solution for Ethereum-based wallet accounts by incorporating smart contracts and Merkle trees. The solution involves a user submitting a KYC

request to the central KYC provider. The KYC provider then proceeds to validate the user's documentation, once validated a KYCNFT is minted using a smart contract. The authors mention that existing solutions lack user privacy as identity providers can associate users with their wallets. This results in a lack of personal privacy as balances and transaction records are exposed to the identity provider. The authors (Sun et al., 2022) solve this issue by allowing the user to link their identity with their wallet, rather than the KYC provider doing so.

Throughout the analysis, many different blockchain platforms were used to implement the various models and frameworks identified. Table 4-1 presents a list of articles analysed along with the proposed or implemented blockchain network. As seen in this table, 12 out of 17 research articles analysed opted to use the Ethereum blockchain network. The authors (Sai et al., 2023) initially implemented their proposed solution on a private Ethereum network. However, due to experiencing high gas fees when calling certain smart contract functions, the authors opted to implement their solution using the Polygon blockchain instead. In doing so, the authors managed to significantly reduce the gas fees when performing functions such as adding KYC information to the blockchain and requesting KYC information. In a separate article, authors (Kapsoulis et al., 2020) opted to use the Quorum network due to its unique "security and permissions" features. Quorum allows for the creation of smart contracts which are only accessible to specified users. The authors (Ostern & Riedel, 2021) developed a blockchain-based KYC system for Initial Coin Offerings (ICOs). In their proposed design they used the EOS blockchain platform. The authors stated that their motivation for choosing EOS over Ethereum was due to significant cost reductions. When comparing the identity verification costs of EOS vs Ethereum, EOS costs $0.09 per investor, whereas Ethereum costs $0.75.

Furthermore, authors (Ullah et al., 2021) proposed a framework that utilises the Hyperledger Fabric network. This network acts as a private blockchain network where only authorised users can interact with the system. Hyperledger is a private and permissioned network, which means that only authorised users can access the network. Their motivation for choosing this network is that Ethereum-based KYC solutions are less secure and more expensive to operate. The solution proposed consists of a permission blockchain, a distributed storage database and a customer-centred user experience.

Based on the analysis of previous research literature, it is crucial to identify the key features and limitations before choosing a blockchain network. Features such as privacy, security, flexibility, scalability, performance and costs are essential factors to consider when implementing a framework on a specific blockchain network.

Table 4-1 – Comparison of Blockchain Network proposed/implemented

Author(s)	Ethereum	Polygon	Quorum	EOS	Hyperledger Fabric
(Sai et al., 2023)	✓	✓			
(Patil & Sangeetha, 2022)	✓				
(Geetha et al., 2022)	✓				
(Parra Moyano & Ross, 2017)	✓				
(Kapsoulis et al., 2020)			✓		
(Ostern & Riedel, 2021)				✓	
(Feulner et al., 2022)					
(Sun et al., 2022)	✓				
(Hongmei, 2021)	✓				
(Páez et al., 2020)					
(Gao et al., 2021)					
(Hwang et al., 2021)	✓				
(George et al., 2019)	✓				
(Biradar & Dakshayini, 2020)					✓
(Ullah et al., 2021)					✓
(Sundareswaran et al., 2020)	✓				
(Yadav & Chandak, 2019)	✓				

Throughout the literature analysis, several authors proposed various techniques and approaches as to what they deemed to be the best approach for implementing a blockchain-based KYC solution. The authors (Patil & Sangeetha, 2022) proposed a unique solution which incorporates a "voting system". In this approach, customers submit a KYC verification request to the bank, along with the required documentation. The bank stores the documentation off-chain in a secure storage and generates a hash link of the documents, which is added to the blockchain. Banks, which have been granted permission by the administrator, can upvote or downvote the KYC data as a means to express their consent. If a customer receives more upvotes than downvotes, the KYC status is approved. If the total number of downvotes is equal to one-third of the total number of votes, the KYC status is rejected. Banks operating within the network are also able to upvote and downvote other banks. This functionality allows the identification of any corrupt or

malicious actors During the analysis, the article by (Patil & Sangeetha, 2022) was the only framework proposed that made use of a voting system for verification.

Authors (Parra Moyano & Ross, 2017) proposed a KYC framework where the costs of conducting the KYC verification are proportionally shared across each financial institution the customer interacts with. The proposed framework uses a central regulator that is responsible for approving which financial institutions can interact with the system. The KYC process starts when a customer wishes to engage with a new financial institution. A new account is created for the customer and the customer receives a private and public key. The customer then shares their KYC documentation along with their public key. These documents are stored locally to preserve customer privacy.

Once the KYC verification has been conducted, the bank creates a "document package" which includes a hash of the documents stored, a certificate of KYC approval and a list of all financial institutions which have access the customer's data. This "document package" is stored on a private blockchain using a smart contract. The cost of performing the KYC verification process is predetermined based on several factors. When a customer wishes to engage with an additional financial institution, the financial institution is required to pay a proportional part of the total cost of conducting the KYC verification process. This fee is calculated as "m/k". Where "m" is the total cost of conducting the KYC verification, which is predetermined. And "k" is the number of financial institutions which have already interacted with the specific customer. This fee is divided equally between all financial institutions which have already interacted with the customer. This proposed framework ensures that the KYC verification process is only performed once, and all costs of performing the KYC verification process are distributed equally among the financial institutions that require the KYC status of a customer.

The analysis revealed that there are various methods of choosing a KYC provider. A KYC provider is described as the entity that is responsible for conducting the KYC verification process. Based on the analysis, there are two common types of approaches. The first type involves the financial institution being responsible for conducting the KYC verification process. Each financial institution operating within the system would have to carry out its own KYC verification process. The second type involves the KYC verification process being conducted by a central authority or a third-party regulator. In this scenario, the central authority would conduct all of KYC verification requests. The authors (Hwang et al., 2021) highlighted the negative impacts of a central authority infrastructure. They argued that if attackers were to breach the central authority, they would have total control of the verification process and could issue fake KYC verification statuses. Furthermore, central authorities are susceptible to DDoS attacks which can bring the entire KYC verification process to a standstill. However, the authors (Parra Moyano & Ross, 2017) considered the possibility of a centralised KYC solution. They argued that by incorporating a central authority, banks would significantly benefit from the reduction in operating costs, and therefore it could encourage new financial institutions to form as the barrier to entry is lower as a result of the reduction in operating costs. More financial institutions lead to an increase in competition; therefore, customers are likely to experience lower bank fees. However, authors (Parra Moyano & Ross, 2017) stated that this scenario is unlikely as regulators would incur additional costs. Table 4-2 illustrates the type of KYC provider used in each of the research articles analysed.

Table 4-2 – Comparison of KYC provider used

Author(s)	Central Authority	Financial Institution
(Sai et al., 2023)	✓	
(Patil & Sangeetha, 2022)		✓
(Geetha et al., 2022)		✓
(Parra Moyano & Ross, 2017)		✓
(Kapsoulis et al., 2020)	✓	
(Ostern & Riedel, 2021)	✓	
(Feulner et al., 2022)		
(Sun et al., 2022)	✓	
(Hongmei, 2021)		
(Páez et al., 2020)	✓	
(Gao et al., 2021)	✓	
(Hwang et al., 2021)	✓	
(George et al., 2019)		✓
(Biradar & Dakshayini, 2020)		✓
(Ullah et al., 2021)		✓
(Sundareswaran et al., 2020)		
(Yadav & Chandak, 2019)	✓	

There was much discussion among the various authors on the best method of storing private KYC customer data. The first option was to store data off-chain in a local database. The next option was to store KYC data directly onto the blockchain. Due to the high costs of storing large files on a blockchain network, some authors proposed a framework where KYC data is stored in a local database. A hash of the data stored is generated and uploaded onto the blockchain. By generating a hash value of the data stored, any data that is changed or tampered with can be identified, as the hash value of the data will change.

Authors (Kapsoulis et al., 2020) stated that due to blockchains transparency and irreversibility, it is not suitable for storing private and sensitive information, such as KYC data, directly onto the blockchain. They also mentioned that data encrypted before being stored on the blockchain has the possibility of being decrypted and exposed if the decryption key were ever to be made public. Furthermore, authors (Hwang et al., 2021) discuss the regulatory issues involved with storing KYC data directly on a blockchain.

They state that the General Data Protection Regulation (GDPR) recommends the pseudonymisation of personal data as well as mandates that "the data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay". Due to blockchain's immutable property, any data stored on the blockchain cannot be altered or erased.

The authors (Kapsoulis et al., 2020) proposed a KYC framework using the Quorum blockchain and an InterPlanetary File System (IPFS) for data storage. IPFS is a protocol that is used for storing and retrieving data in a decentralised peer-to-peer network. When files are stored on an IPFS network, they are fragmented, and a hash value of the files is created. This hash value is known as the content identifier or CID. The CID is used to route back to the files for retrieval. In this framework, the CIDs are stored in a private smart contract which only authorised administrators have access to. By making use of IPFS technology, the authors were able to enhance user privacy and security compared to other permissioned blockchain solutions.

The authors (Sundareswaran et al., 2020) proposed a solution that directly stores data in the Ethereum blockchain network. Their solution aimed to solve the lack of privacy and high costs faced when storing KYC data onto a blockchain network. To reduce costs, the authors compressed the KYC data by using the LZ compression algorithm. The data was also encrypted using AES symmetric key encryption. Their proposed solution resulted in slight cost savings due to the compression of the data. However, they experienced slower data retrieval time due to the decompression required when retrieving the data.

The authors (Ostern & Riedel, 2021) stressed the importance of thoroughly analysing General Data Protection Regulations (GDPR) and AML regulations before designing and proposing a blockchain-based KYC solution. They highlighted the difficulties when designing a global system, as regulations may vary based on each jurisdiction. Furthermore, they identified the need for flexible smart contracts as the system would have to adapt to legal changes. The authors (Ostern & Riedel, 2021) proposed an off-chain storage solution but refrained from using hash values to allow for later data correction.

Figure 4-1 provides a comparison between the various articles of literature analysed and the technologies each framework utilised. The comparison reveals that smart contracts are crucial when designing and implementing a blockchain-based KYC framework. The concept of smart contracts was first introduced in the early 1990s by computer scientist Nicholas Szabo. Szabo defined a smart contract as a "computerised transaction protocol that executes the terms of a contract" (Szabo, 1994). Smart contracts were designed to reduce the need for trusted intermediaries by minimising accidental and malicious exceptions (Szabo, 1994). The main utility of smart contracts was to allow the contractual terms of an agreement to be embedded within certain hardware and software (Szabo, 1997). In doing so, it allows for specific contractual clauses to be automatically enforced once a specific condition is met. Smart contracts are composed of various conditions statements which are designed to replicate real-world contracts. Once a particular condition is met, a response statement is automatically executed. For example, if a rental smart contract was created between a lessee and a lessor, and the lessee was late with the monthly payment of rent. The smart contract would automatically trigger once the specified date has passed and would enforce a late penalty fee. This penalty fee could automatically be deducted from the deposit. Smart contracts play a key role in

developing a blockchain-based KYC system, as the smart contract acts as a form of communication between the user and the blockchain.

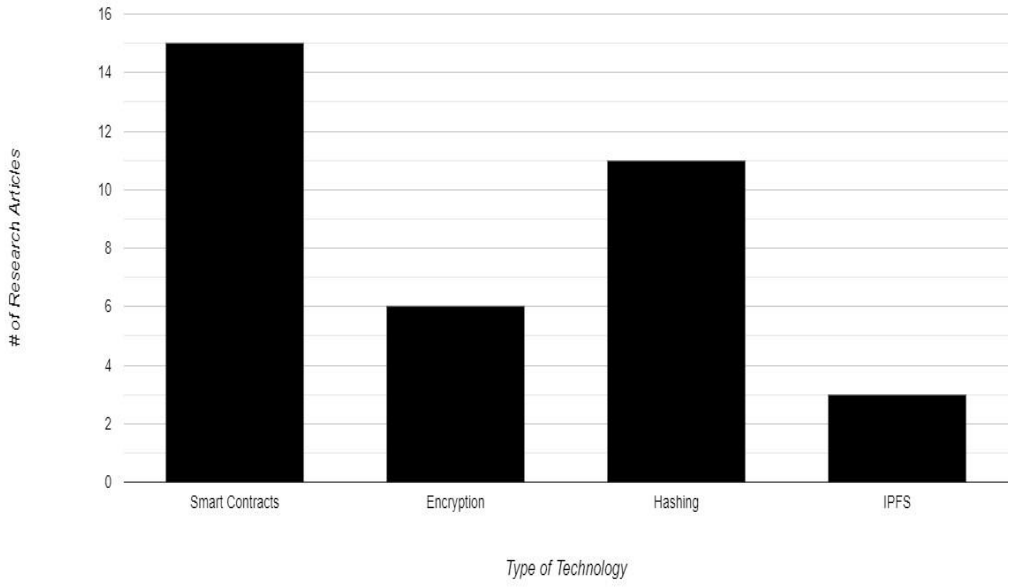

Figure 4-1 - Comparison of Various Technologies Used

4.2 LITERATURE REVIEWS & CASE STUDIES

The authors (Thiraviya Suyambu et al., 2020) reviewed various applications of blockchain technology across multiple organisations. In their research, they studied a case where auditing firm KPMG tested a blockchain-based KYC solution involving multiple financial institutions. The results of the tests showed that a blockchain-based KYC solution eliminated KYC duplication costs, prevented KYC tampering, and allowed for more effective monitoring by regulators.

The paper by (Thommandru & Chakka, 2023) discusses the issues surrounding compliance and AML policies in the banking sector with regard to new emerging technologies. They discuss two blockchain-based KYC solutions, namely OnRamp and Quadrata. The OnRamp platform includes “ID verification and sanction and politically exposed person screening”. Quadrata is an Ethereum-based passport platform. This passport is stored as a non-transferable NFT and contains the necessary KYC and AML compliance information of a customer. The authors mention that the most optimal KYC solution is a single entity that is adopted worldwide, as the cost reductions of the process will be maximised. However, this case is highly unlikely due to politics and differences in regulations across jurisdictions.

Furthermore, the authors (Shbair et al., 2018) discussed the importance of testing large-scale applications before being deployed onto a blockchain. In this paper, they discuss the core benefits of a testbed environment called Grid'5000. This testbed simulates a real blockchain environment and is a highly controllable and reconfigurable environment that allows for experiments to be performed. Testbeds are used to test aspects such as privacy, security, scalability, and flexibility before a blockchain application is deployed. Using Grid'5000, the authors implemented an Ethereum-based KYC solution that uses an IPFS to store KYC documents. The authors use the testbed to evaluate the performance of the smart contract by performing certain tasks such as client registration events. This paper highlights the significance and importance of thoroughly testing blockchain-based applications before they are deployed onto a blockchain network.

In the paper by (Limba, 2019), the author discusses the current impact of cryptocurrencies on national security. They mention that cryptocurrencies have become a major tool for conducting criminal activities. The paper highlights that cryptocurrencies are being exploited due to their lack of AML and KYC policies, making them vulnerable to money laundering, illegal goods transactions, tax evasion, and money theft. The author concludes that cryptocurrencies are difficult to be regulated for 3 main reasons: 1) Cryptocurrencies are a global market product, meaning that it is difficult to determine who will regulate the market. 2) Cryptocurrencies have an IT-based financial operating model that requires new ways to implement appropriate KYC and AML regulations. 3) Cryptocurrency transactions are automatic and are impossible to stop.

The authors (Kulkarni & Singh, 2019) conducted a literature review based on the current KYC challenges that banks face and questioned whether a blockchain-based KYC approach was the right solution. Based on their research they concluded that a private blockchain is the most suitable approach for developing a blockchain-based KYC solution. A private blockchain provides better security and authentication policies, as well as is more in line with GDPR requirements.

4.3 Proposal of Conceptual Model

Based on the analysis of previous research conducted, we have identified the key aspects to consider when developing a blockchain-based KYC model. In this section, we utilise the knowledge gained from our analysis to propose an enhanced blockchain-based KYC model. These key aspects identified will serve as a guideline when proposing our model. The key aspects identified are as follows:

3. Blockchain network (storage limitations, gas fees and scalability).
4. Documentation storage method (off-chain vs on-chain storage).
5. KYC verification approach (central authority vs financial institution).
6. Security and privacy measures (preserving customer confidentiality).
7. KYC, AML and GDPR regulations.

The following section proposes a blockchain-based KYC conceptual model that aims to improve upon previous conceptual models and frameworks developed. This section proposes a token subscription-based framework built on the Hyperledger Fabric network and utilises an IPFS for secure off-chain document storage. In this model, an external central authority or regulator will be responsible for

conducting the KYC verification and is responsible for access control to the KYC platform. Although the KYC verification process is outsourced to an external entity, financial institutions will still bear the costs of conducting the KYC verification process through annual subscriptions and tokens. Financial institutions are required to pay an annual subscription fee to access the KYC verification platform. This annual subscription fee will be calculated based on various factors and can be altered as needed by the central authority. Upon successful registration and payment of the annual subscription, the financial institution will receive an allocated number of tokens. These tokens will serve as a payment method from the financial institution to the central authority for conducting the KYC verification process. The cost of conducting the KYC verification process will depend on various factors, such as the risk profile of the entity and the type/complexity of the entity. An IPFS network was selected to handle the storage of various sensitive and private documentation. Due to the fact that we are working with a substantial amount of sensitive data, the decision was made to store data off-chain to enhance customers' confidentiality and security of data. As previous studies revealed storing data on-chain poses a security risk as well as impacts the overall performance of the blockchain.

In the proposed model, sensitive KYC documentation will be securely stored in an IPFS network maintained by the central authority. Once data is stored onto the IPFS network, a hash value is generated which is used to locate and retrieve data. This hash value is stored in the blockchain along with either customer or financial institution data. An IPFS network can combat malicious activities such as data manipulation and tampering. Any alteration to the data stored in the IPFS can be identified, as the hash value stored on the blockchain will no longer match the hash value of the modified data stored on the IPFS network.

The proposed model promotes collaboration across various financial institutions as the cost of conducting the KYC process is shared equally among each financial institution that accesses a particular customer's KYC information. The financial institution first selected by the customer when applying for KYC verification will bear the full cost of conducting the KYC verification process. Every subsequent financial institution that requires access to the customer's KYC status will equally share costs through distributing tokens.

By opting to use a central authority, financial institutions no longer need to employ resources to conduct the KYC process. Financial institutions will no longer need to train employees to conduct this process, nor will they be required to keep up with the ever-changing rules and regulations surrounding KYC and AML. This provides financial institutions the opportunity to enhance operations in other areas and increase overall customer satisfaction. The central authority will have the capability to establish separate departments tailored to cater for the various types of entities applying for KYC verification. An annual subscription model was proposed as this provides the central authority with upfront revenue and increases their cash flow. The influx in cash flow can be strategically reinvested within the central authority to enhance the services provided to the various financial institutions. For example, the central authority can utilise the upfront revenue to employ additional resources, which could ultimately reduce the turnaround time of conducting the KYC process. In the proposed model, the KYC verification process only needs to be conducted once. Once completed, the customer can seamlessly share their KYC status with every financial institution operating on the platform, eliminating additional time delays or costs. Customers engaging with multiple financial institutions will significantly benefit from this approach, as it enables them to

establish business relationships with multiple financial institutions after completing the KYC process just once.

For the proposed model to be an effective tool in combating the current challenges experienced in the KYC process, its success relies on a multitude of financial institutions participating on the platform. The proposed model yields the highest return for customers, financial institutions, and the central authority when there are a large number of financial institutions operating on the platform. For the proposed model to function, the first essential step is the onboarding of financial institutions. Figure 4-1 illustrates the registration/onboarding process for financial institutions. A detailed outline of each step is as follows:

4.3.1 Financial Institution Onboarding Process

1. A FI submits a registration request using the online platform along with the required documentation.
2. The central authority receives the request from the FI and analyses the documentation to ensure that the FI meets all current regulatory requirements. This process ensures that all FIs operating within the system meet the legal requirements and are not used in illicit operations. The central authority notifies the FI of the outcome of the registration process. If their application is successful, the central authority sends a payment request to the FI for their annual subscription to access the KYC platform.
3. The FI accepts the payment request and sends the requested amount to the central authority using the online platform.
4. Once the payment has been received by the central authority, they will store the documentation of the FI on the IPFS network.
5. The central authority retrieves the hash value of the storage location of the documentation stored on the IPFS network.
6. The central authority then invokes a smart contract with the following information: details of the financial institution, hash value of documents, subscription start and end date and transaction ID.
7. The smart contract will create a new entry on the blockchain storing this information. This blockchain provides a list of authorised FIs from which customers can select when sharing their KYC status.
8. Once the details are stored onto the blockchain, the smart contract triggers an automatic response to the FI informing them that their account is active and allocates a fixed number of tokens to their account.

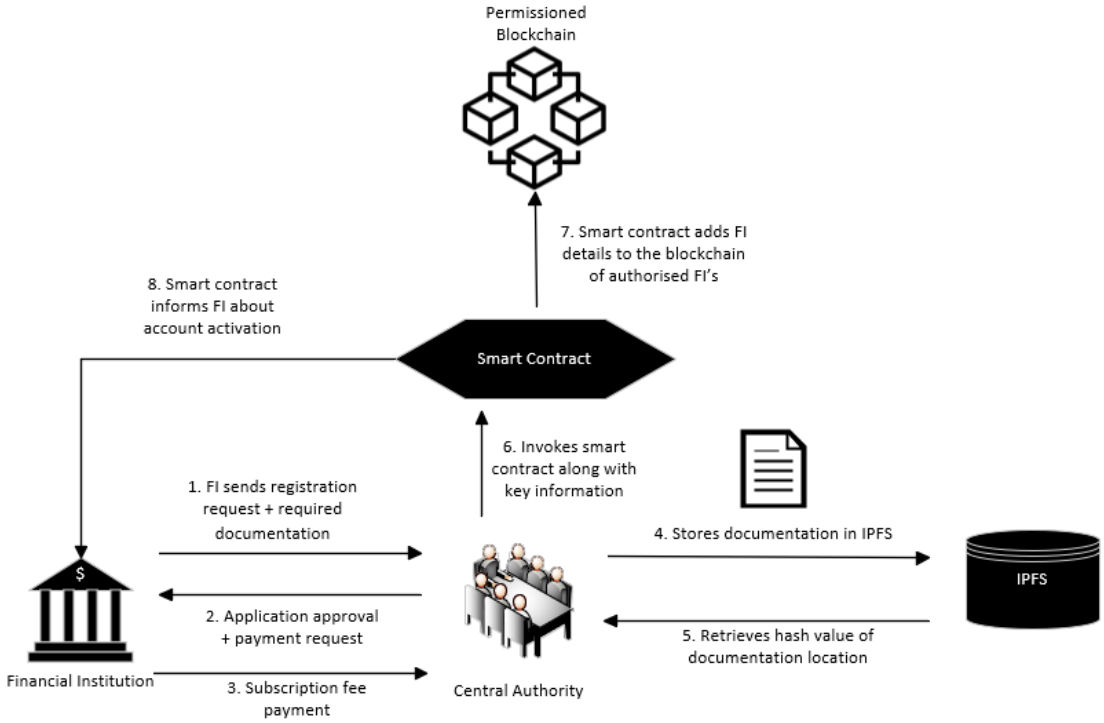

Figure 4-2 – Financial Institution Registration/Onboarding Process

Once financial institutions have successfully been registered and onboarded onto the platform, customers can commence with their registration and apply for KYC verification. Figure 4-2 illustrates the customer registration/onboarding process. A detailed outline of the process is as follows:

4.3.2 Customer Onboarding Process

9. A customer creates a new account on the online KYC platform. During this step, the customer selects a FI from a list of authorised Fis with which they would like to share their KYC status with. The customer is required to upload the necessary KYC documentation with their registration.
10. When the customer submits their application, their documentation is automatically stored in the IPFS.
11. The FI selected then receives a KYC request, which they must either accept or reject. The request will include the customer's details, along with a token fee for conducting the KYC verification process. This fee is calculated by an algorithm that assesses the complexity of conducting the KYC verification request based on the type of customer applying for KYC verification. For the FI to accept the request, they must have a sufficient token balance. Additional tokens can be purchased by the FI directly on the online platform. The price of the tokens will be determined by the central authority. If the FI accepts the customer's KYC request and has a sufficient token balance, the request is forwarded to the central authority.

12. To conduct the KYC verification process, the central authority must use the hash value to retrieve the customer's KYC documentation stored on the IPFS. After the documentation has been retrieved, the central authority will examine the KYC documentation to ensure that it meets the current KYC and AML regulations. After careful examination, the central authority will either approve or deny the KYC verification request.
13. Once the verification process has concluded, the central authority will invoke a smart contract containing the following information: customer ID, KYC status, hash value of documents, expiry date of KYC status (if KYC status was approved), cost of conducting the KYC process in tokens, and an array data structure containing the ID of the FI which the customer has selected. The array data structure will act as a control mechanism in determining which FIs have access to a particular customer's KYC status.
14. The smart contract will create a new entry on the permissioned blockchain, storing the information provided in the smart contract. This blockchain will keep a record of all customer KYC requests, as well as which FIs have access to each customer's KYC status.
15. Once the information is stored on the blockchain, a smart contract will trigger notifying the FI about the outcome of the customer's KYC verification process. The same smart contract will notify the customer of the outcome of the KYC verification process.

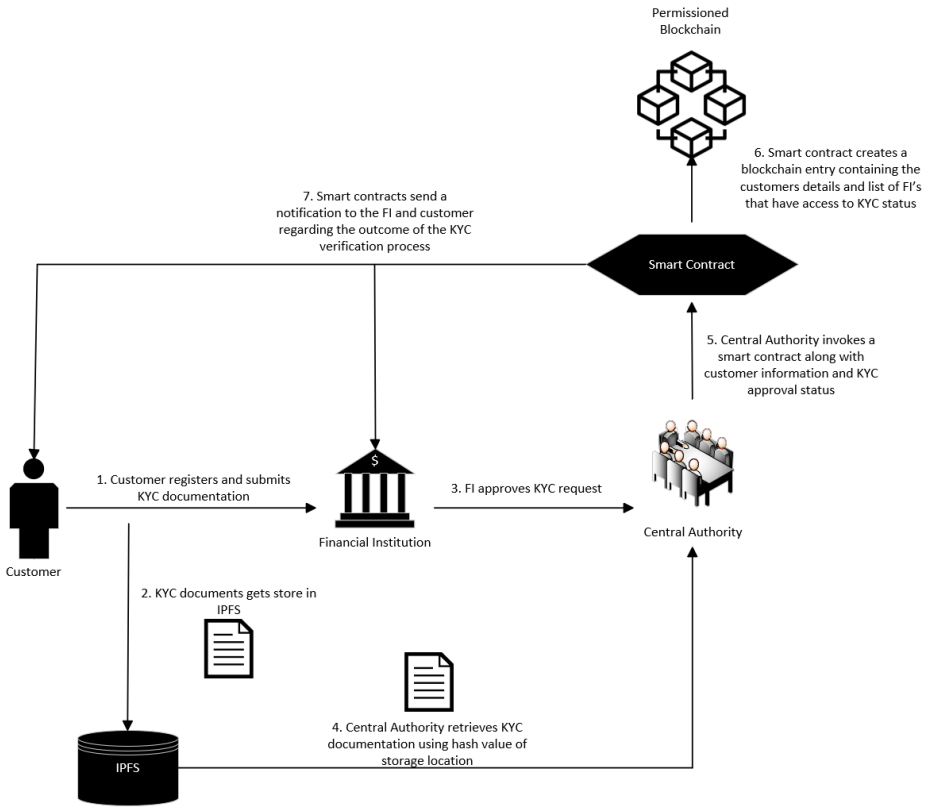

Figure 4-3 – Customer Registration/Onboarding Process

4.3.3 Sharing KYC Status Process

Up until this point, the described processes may not yield significant improvements compared to traditional KYC approaches in terms of reducing redundant tasks, costs, and time. The true enhancements become apparent when a customer shares their KYC status with more than one financial institution. The proposed conceptual model enables customers to interact with multiple financial institutions by sharing their KYC status with multiple financial institutions. Figure 4-3 illustrates the process of a customer sharing their KYC status with multiple financial institutions. This figure highlights the efficiency of subsequent KYC information sharing, as it eliminates the need to conduct the KYC process more than once. The ability to share KYC information across multiple financial institutions results in significant reductions in costs and time. A detailed outline of the KYC status-sharing process is as follows:

16. A customer accesses their account on the online platform and chooses to share their valid KYC status with an additional FI. The customer selects the specific FI which they wish to share their KYC status with from a list of authorised FIs and submits their request.
17. The FI then receives the customer's request to share their KYC status with them. The FI will review the customer's request and will either accept or reject the request. The request will include the customer's details along with a token fee to gain access to the customer's KYC status. This fee will be calculated using the following formula $\frac{x}{y+1}$, where x is the number of tokens that it costs to conduct the initial KYC verification process, and y is the number of FIs that currently have access to the customer's KYC status. To be able to accept the request, the FI must have a sufficient token balance.
18. Upon successful approval of the request, a smart contract is automatically triggered. The smart contract retrieves the array data structure of FIs that currently have access to the customer's KYC status from the blockchain. Once this list has been retrieved, the smart contract automatically updates the token balance of each FI within the array by equally distributing the number of tokens paid in the previous step. Subsequently, the smart contract updates the array containing the list of FIs with access to the customer's KYC status by inserting the ID of the new FI.
19. After the information on the blockchain has been successfully updated, the smart contract triggers a notification to the customer and the FI, informing them that the KYC status has been shared successfully.

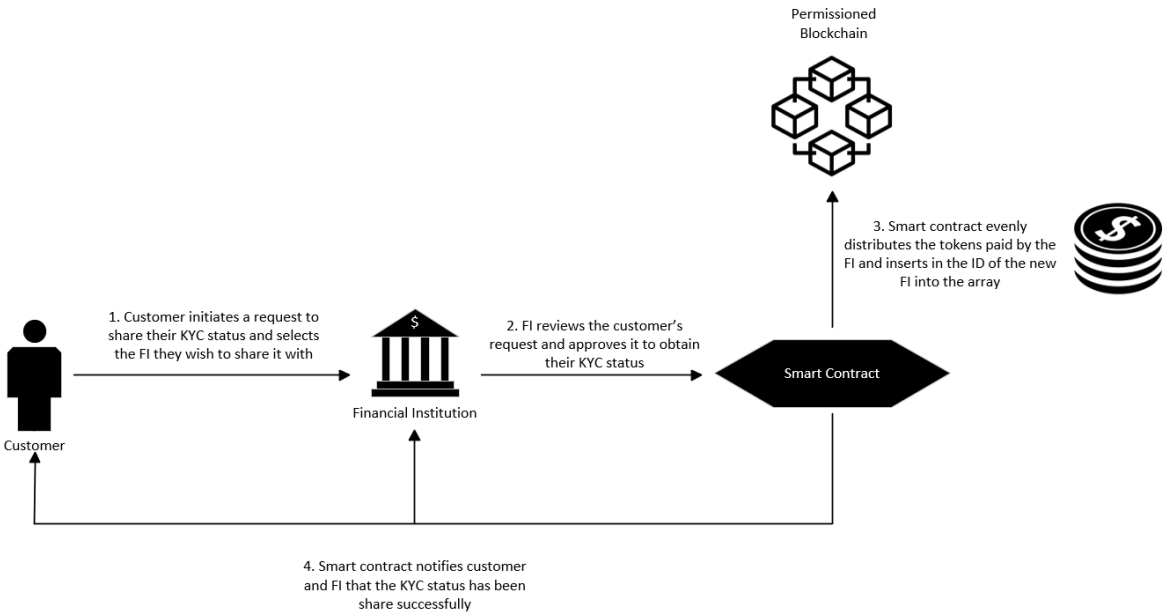

Figure 4-4 – Sharing KYC Status Process

4.3.4 Limitations of Proposed Conceptual Model

Based on the proposed conceptual model, the following limitations have been identified, as presented below.

- Due to the KYC verification process being conducted by a central authority, financial institutions will be unable to prioritise or fast-track certain customer KYC applications. The financial institution will have to wait for the response of the central authority and are excluded from having any involvement. A potential solution to this is that financial institutions can opt to pay an increased amount of tokens to prioritise their requests. However, this may pose additional challenges as other financial institutions may find this unfair and will be deterred from using the platform.
- The model was only proposed on a conceptual level; therefore, we are unable to carry out tests to analyse the performance of the model. Additionally, testing the security and scalability of the model is not possible. The model will first have to be developed and implemented before these areas can be analysed.
- Financial institutions might be resistant to joining the platform for fear of vendor lock-in. Financial institutions will be forced to continue paying an annual subscription to access KYC information, failure to do so will result in loss of all KYC information. This fear might incline financial institutions to prefer conducting the KYC process themselves.

- There is a risk that the central authority may exploit its power by setting unfair costs for conducting the KYC verification. As the central authority controls the pricing of tokens, there is a potential that these prices are manipulated to yield a greater profit.
- The system is controlled by a central authority, any data breaches or cyber-attacks on the central authority can lead to total system failure. This will impact every single financial institution operating on the platform and could bring the KYC process to a standstill.

5 CONCLUSIONS & FUTURE WORKS

The KYC process is a vital procedure that is essential for financial institutions to perform to comprehend the nature of their customer's activities. The process is employed to prevent illicit criminal activities, such as money laundering, terrorist financing, and corruption. However, the existing KYC process is inefficient and outdated, leading to large financial burdens and significant time loss. In this study, we investigate the possibility of transforming the KYC process with the implementation of blockchain technology. By incorporating blockchain technology into the KYC process, it enables the sharing of KYC information across multiple financial institutions in a secure manner.

In this study, we conducted a Systematic Literature Review to comprehensively understand and explore the existing research conducted on blockchain technology and the KYC process. This review revealed that multiple frameworks were proposed and developed, each presenting a unique approach to tackling the problem at hand. Various similarities and differences between the research articles analysed were identified and discussed.

Using the knowledge gained through the analysis of existing research, we have proposed a conceptual model for a blockchain-based KYC approach. While our model is only proposed on a conceptual level, it aims to improve existing frameworks by tackling the problems and limitations faced in previous studies. The conceptual model features a subscription-based approach along with tokens serving as a form of payment for conducting the KYC verification process. The model utilises a permissioned blockchain and an IPFS network for documentation storage. The use of blockchain technology allows a customer's KYC status to be shared with multiple financial institutions without incurring any additional costs or time delays. The model promotes collaboration between financial institutions, as the cost of conducting the KYC process is distributed proportionately through the use of tokens.

Although various blockchain-based KYC models have been proposed and developed, we are yet to see wide-scale adoption of this technology. Financial institutions may be hesitant to adopt this technology due to its complexities and their lack of experience in dealing with it. The goal of our research was aimed at investigating how blockchain technology can be used to transform and enhance the existing KYC process. As a result, we have successfully developed a conceptual model that we believe will improve the current KYC procedures. We believe that the findings of our research positively contribute to the area of blockchain technology and regulatory compliance and can be used to guide future research. However, a limitation within our research arises due to the non-implementation of the conceptual model. Implementation of the conceptual model was not possible due to time constraints faced in conducting this master thesis investigation. Future research will prioritise implementing the conceptual model to evaluate its performance, security, and scalability within a real-world environment.

BIBLIOGRAPHICAL REFERENCES

Biradar, R. R., & Dakshayini, M. (2020). Blockchain enabled KYC solutions using hyperledge fabric. *2020 International Conference on Mainstreaming Block Chain Implementation, ICOMBI 2020*, 12–14. https://doi.org/10.23919/ICOMBI48604.2020.9203407

Crosby, M., Pattanayak, P., Verma, S., & Kalyanaraman, V. (2016). BlockChain Technology: Beyond Bitcoin. *Applied Innovation Review*, *2*.

Feulner, S., Sedlmeir, J., Schlatt, V., & Urbach, N. (2022). Exploring the use of self-sovereign identity for event ticketing systems. *Electronic Markets*, *32*(3), 1759–1777. https://doi.org/10.1007/s12525-022-00573-9

Gao, S., Su, Q., Zhang, R., Zhu, J., Sui, Z., & Wang, J. (2021). A Privacy-Preserving Identity Authentication Scheme Based on the Blockchain. *Security and Communication Networks*, *2021*. https://doi.org/10.1155/2021/9992353

Geetha, R., Padmavathy, T., & Umarani Srikanth, G. (2022). A Scalable Block Chain Framework for User Identity Management in a Decentralized Network. *Wireless Personal Communications*, *123*(4), 3719–3736. https://doi.org/10.1007/s11277-021-09310-5

George, D., Wani, A., & Bhatia, A. (2019). A Blockchain based Solution to Know Your Customer (KYC) Dilemma. *International Symposium on Advanced Networks and Telecommunication Systems, ANTS*, *2019-Decem*, 1–6. https://doi.org/10.1109/ANTS47819.2019.9118042

Glaser, F. (2017). *Pervasive Decentralisation of Digital Infrastructures: A Framework for Blockchain enabled System and Use Case Analysis*. https://doi.org/10.24251/HICSS.2017.186

Harrop, M. D., & Mairs, B. (2016). *Thomson Reuters 2016 Know Your Customer Surveys Reveal Escalating Costs and Complexity*. Thomson Reuters. https://www.thomsonreuters.com/en/press-releases/2016/may/thomson-reuters-2016-know-your-customer-surveys.html

Hayes, A. (2023). *Blockchain Facts: What Is It, How It Works, and How It Can Be Used*. Investopedia. https://www.investopedia.com/terms/b/blockchain.asp

Hongmei, Z. (2021). A Cross-Border E-Commerce Approach Based on Blockchain Technology. *Mobile Information Systems*, *2021*. https://doi.org/10.1155/2021/2006082

Hwang, G. H., Chang, T. K., & Chiang, H. W. (2021). A Semidecentralized PKI System Based on Public Blockchains with Automatic Indemnification Mechanism. *Security and Communication Networks*, *2021*. https://doi.org/10.1155/2021/7400466

Kapsoulis, N., Psychas, A., Palaiokrassas, G., Marinakis, A., Litke, A., & Varvarigou, T. (2020). Know your customer (KYC) implementation with smart contracts on a privacy-oriented decentralized architecture. *Future Internet*, *12*(2). https://doi.org/10.3390/fi12020041

Kshetri, N. (2017). Blockchain's roles in strengthening cybersecurity and protecting privacy. *Telecommunications Policy*, *41*(10), 1027–1038. https://doi.org/10.1016/J.TELPOL.2017.09.003

Kulkarni, V. V., & Singh, A. P. (2019). *Sustainable KYC through Blockchain Technology in Global Banks Sustainable KYC through Blockchain Technology in Global Banks*. *January 2020*. https://doi.org/10.35219/eai1584040929

KYC3. (2018). *Your Guide To KYC And AML Compliance*. https://www.kyc3.com/quick-guide-to-kyc-and-aml-compliance/

Limba, T. (2019). *TOWARDS SUSTAINABLE CRYPTOCURRENCY: RISK MITIGATIONS FROM A PERSPECTIVE OF NATIONAL SECURITY*. *9*(2). https://doi.org/http://doi.org/10.9770/jssi.2020.10.2(14)

Malhotra, D., Saini, P., & Singh, A. K. (2022). How Blockchain Can Automate KYC: Systematic Review. In *Wireless Personal Communications* (Vol. 122, Issue 2). Springer US. https://doi.org/10.1007/s11277-021-08977-0

Mohanta, B. K., Panda, S. S., & Jena, D. (2018). An Overview of Smart Contract and Use Cases in Blockchain Technology. *2018 9th International Conference on Computing, Communication and Networking Technologies, ICCCNT 2018*, *November*, 1–4. https://doi.org/10.1109/ICCCNT.2018.8494045

Mulligan, D. (1999). Know Your Customer Regulations and the International Banking System: Towards a General Self-Regulatory Regime. *Fordham International Law Journal*, *22*(5), 2324–2372.

Nakamoto, S., & System, A. P. E. C. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System比特币：一种点对点的电子现金系统*. https://git.dhimmel.com/bitcoin-whitepaper/

Ostern, N. K., & Riedel, J. (2021). Know-Your-Customer (KYC) Requirements for Initial Coin Offerings: Toward Designing a Compliant-by-Design KYC-System Based on Blockchain Technology. *Business and Information Systems Engineering*, *63*(5), 551–567. https://doi.org/10.1007/s12599-020-00677-6

Páez, R., Pérez, M., Ramírez, G., Montes, J., & Bouvarel, L. (2020). An architecture for biometric electronic identification document system based on blockchain. *Future Internet*, *12*(1), 1–19. https://doi.org/10.3390/fi12010010

Parra-Moyano, J., Thoroddsen, T., & Ross, O. (2018). Optimized and Dynamic KYC System Based on Blockchain Technology. *SSRN Electronic Journal*, *September 2019*. https://doi.org/10.2139/ssrn.3248913

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

Patil, P., & Sangeetha, M. (2022). Blockchain-based Decentralized KYC Verification Framework for Banks. *Procedia Computer Science*, *215*, 529–536. https://doi.org/10.1016/j.procs.2022.12.055

Petersen, K., Feldt, R., Mujtaba, S., & Mattsson, M. (2007). *Systematic Mapping Studies in Software Engineering*. 1–10.

Sai, B. D. S., Nikhil, R., Prasad, S., & Naik, N. S. (2023). A decentralised KYC based approach for microfinance using blockchain technology. *Cyber Security and Applications*, *1*(August 2022), 100009. https://doi.org/10.1016/j.csa.2022.100009

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

Shbair, W. M., Steichen, M., Francois, J., & State, R. (2018). Blockchain orchestration and experimentation framework: A case study of KYC. *IEEE/IFIP Network Operations and Management Symposium: Cognitive Management in a Cyber World, NOMS 2018*, 1–6. https://doi.org/10.1109/NOMS.2018.8406327

Sun, N., Zhang, Y., & Liu, Y. (2022). A Privacy-Preserving KYC-Compliant Identity Scheme for Accounts on All Public Blockchains. *Sustainability (Switzerland)*, *14*(21), 1–18. https://doi.org/10.3390/su142114584

Sundareswaran, N., Sasirekha, S., Louis Paul, I. J., Balakrishnan, S., & Swaminathan, G. (2020). Optimised KYC Blockchain System. *2020 International Conference on Innovative Trends in Information Technology (ICITIIT)*, 1–6. https://doi.org/10.1109/ICITIIT49094.2020.9071533

Szabo, N. (1994). *Smart Contracts*. https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/smart.contracts.html

Szabo, N. (1997). *The Idea of Smart Contracts*. https://www.fon.hum.uva.nl/rob/Courses/InformationInSpeech/CDROM/Literature/LOTwinterschool2006/szabo.best.vwh.net/idea.html

Thiraviya Suyambu, G., Anand, M., & Janakirani, M. (2020). Blockchain - A most disruptive technology on the spotlight of world engineering education paradigm. *Procedia Computer Science*, *172*(2019), 152–158. https://doi.org/10.1016/j.procs.2020.05.023

Thommandru, A., & Chakka, D. B. (2023). Recalibrating the Banking Sector with Blockchain Technology for Effective Anti-Money Laundering Compliances by Banks. *Sustainable Futures*, *5*(February). https://doi.org/10.1016/j.sftr.2023.100107

Ullah, N., Al-Dhlan, K. A., & Al-Rahmi, W. M. (2021). KYC optimization by blockchain based hyperledger fabric network. *Proceedings - 2021 4th International Conference on Advanced Electronic Materials, Computers and Software Engineering, AEMCSE 2021*, 1294–1299. https://doi.org/10.1109/AEMCSE51986.2021.00264

Yadav, P., & Chandak, R. (2019). Transforming the Know Your Customer (KYC) Process using Blockchain. *2019 6th IEEE International Conference on Advances in Computing, Communication and Control, ICAC3 2019*, 1–5. https://doi.org/10.1109/ICAC347590.2019.9036811