A FRAMEWORK FOR THE ADOPTION OF BLOCKCHAIN TECHNOLOGY IN ACADEMIC CERTIFICATE-VERIFICATION SYSTEMS: A CASE STUDY OF NIGERIA

Thesis · June 2020

CITATIONS
0

READS
1,776

1 author:

Mercy Effiong
Tallinn University of Technology
1 PUBLICATION **0** CITATIONS

SEE PROFILE

TALLINN UNIVERSITY OF TECHNOLOGY

School of Information Technologies

Mercy Ebiot Effiong

184572 IVGM

A FRAMEWORK FOR THE ADOPTION OF BLOCKCHAIN TECHNOLOGY IN ACADEMIC CERTIFICATE-VERIFICATION SYSTEMS: A CASE STUDY OF NIGERIA

Master's Thesis

Supervisor: Alexander Norta

PhD

Associate Professor

TALLINNA TEHNIKAÜLIKOOL

Infotehnoloogia teaduskond

Mercy Ebiot Effiong

187542IVGM

RAAMISTIK PLOKIAHELA TEHNOLOOGIA KASUTUSELE VÕTUKS AKADEEMILISTES SERTIFIKAADIGA-VERIFITSEERITAVATES SÜSTEEMIDES: UURING NIGEERIA NÄITEL

Magistritöö

Juhendaja: Alexander H. 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: Mercy Ebiot Effiong

07.05.2020

Abstract

An academic certificate is an all-important document that can potentially open an individual up to new opportunities. In many cases, it represents an excellent first step to candidate selection during recruitment. While the benefits of certificate ownership are covetable, not everyone is willing or able to obtain the same through legitimate means. All over the world, the incidences of false academic credentials have become prolific. Many strategies to combat this menace have proven abortive and have not measured up with modern techniques deployed in academic fraud. The certificate verification approach in Nigeria and many countries rely heavily on paper-based database and documentation, which makes the process extremely cumbersome, unreliable, and time-consuming with a high administrative cost. It is in the light of these problems that this study seeks to explore and understand the underlying issues in certificate verification systems in Nigeria and then develop a framework for its optimization through the adoption of blockchain technology. The case study design was deemed appropriate for the research. The author obtained data from the review of documents and interviews with relevant persons. The findings revealed that the problems in the system stem first from the manual processes in the current systems, which causes cumbersomeness, delayed responses, high administrative costs, high verification fee, and client dissatisfaction. The findings also showed that the adoption of blockchain could be hindered by inadequate electric supply, poor ICT infrastructures, Poor funding, Lack of digital skills, ignorance of Blockchain and Resistance to change caused by fear of displacement, technophobia, seeking control, and corruption. From the insights gained from the early adopters, the author developed a framework for the adoption of blockchain technology for certificate verification systems.
Keywords: Academic Certificate, Academic Records, Blockchain, Nigeria, Verification.

This thesis is written in English Language and is sixty-five (65) pages long, including five (5) chapters, four (4) figures, and five (5) tables.

List of abbreviations and terms

BPMN	Business Process Model And Notation
BUID	British University In Dubai
CATS	Credit Accumulation And Transfer Systems
DLT	Distributed Ledger Technology
GOVTECH	Government Technology Agency
ISPs	Internet Service Providers
ITS	Institute For Tourism Studies
MCAST	Malta College For Arts, Science, and Technology
MEDE	Ministry For Education And Employment
MOE	Ministry of Education
NCC	Nigeria Communication Commussion
NCFHE	National Commission for Further and Higher Education
NP	Ngee Ann Polytechnic
NUC	National University Commission
NUCDB	Nigerian Universities Commission Database
NYSC	National Youth Service Corps
SSG	SkillsFuture Singapore
URL	Uniform Resource Locator

Table of Content

List of figures

List of tables

1 Introduction

An academic certificate is an all-important document. A degree can potentially open an individual up to new opportunities for a better life, empowering one mentally and socially for a meaningful and fulfilled life. In many cases, it is a distinguishing factor among a group of persons, placing people in certain social strata and economic status. Even though it is not finite, however, it represents an excellent first step for candidate selection for companies during recruitment (NationalStudentClearingHouse, 2016). While the benefits of certificate ownership are covetable, not everyone is willing or able to obtain same through legitimate means.

The world over, with no exception to Nigeria, the incidences of false academic credentials have become prolific. Every sphere of endeavor is affected by the fake degree phenomenon. In 2017, for example, not less than 40,000 people within a city were reported to have entered into the Indian labor force with fake credentials (Trines, 2017). Also, in Nigeria, among graduates who were mobilized to serve in the National Youth Service Corps (NYSC) in one of the 2019 batches, sixty of them were found to possess fake credentials. On another occasion, the NYSC was compelled to contact the National Universities Commission (NUC) over supposed graduates who were seriously lacking the abilities and intelligence commensurate to a real graduate (This Day, 2019).

Individuals who desire to attain an overall betterment while boycotting the cost, time, and hard work a genuine certificate demands indulge in certificate forgery. Also, the means and opportunity to claim a fake degree is unprecedently easy nowadays (Attewell & Domina, 2011). However, Douglas cited in (Eckstein, 2003) believes that the major reason academic fraud in the form of fake documents is continually increasing is due to the failure of institutions and organizations to examine degrees and credentials.

Eckstein (2003) points out that moves to improve the educational sector would prove futile except that such issues as fraudulent qualifications were adequately addressed. Many strategies to combat this menace have proven abortive and have not measured up with modern techniques deployed in academic fraud.

The blockchain technology has emerged as a vital mechanism for tamper-proof digital records and is fast becoming applicable in different industries. Poorni et al. (2020), described that blockchain is a decentralized communication and data management solution that is just budding and needs no trusted third party. Without recourse to a central authority, various parties can provably transact on the technology even though they do not trust themselves. Srivastava et al. (2019) also emphasized that blockchain addresses the problems related to certificate verification by offering verifiable digitally time-stamped records that are resistant to modification. The blockchain, initially associated with virtual currency, has quickly gained prominence in different other areas of life. Without the need for a controlling entity, transactions can be initiated and validated on the blockchain. This features its unique selling point. To this end, studies have identified blockchain technology as possessing the potentials to address the problem of authenticating certificates adequately.

This study will be contributing to this emerging area of research by developing a guide for the adoption of blockchain technology for certificate verification systems in Nigeria and other developing countries. This chapter provides preliminary information on the study by defining the problems in Section 1.1, stating the objectives that it aims to achieve in Section 1.2 and setting the frame of reference for the rest of the paper in Section 1.3.

1.1 Problem Statement

According to the National Student Clearing House (2016), when verification becomes increasingly popular among institutions and employers, people will most probably cease from falsifying credentials. Certificate verification policies and processes are changing to combat the menace. The electronic verification of certificates is gradually gaining popularity and deployed in some institutions. The automated system facilitates a seamless and instant verification of certificates by simply querying an institution's database. An employer may not need to contact an institution directly to verify a certificate (Bond & Blousson, 2015).

Contrarily, the certificate forgery phenomena in Nigeria continues to deepen and will likely persist without a reliable system to verify certificate claims. The approach to certificate verification in Nigeria relies heavily on paper-based database and

documentation, which makes the process extremely cumbersome and time consuming with a high administrative cost. Fake credential scandals among public figures who allegedly pass their credentials through security agents for checks during screening and yet were not detected, prove that this method is ineffective and cannot be trusted.

While this problem persists, the damage it causes is repercussive. The effect is far-reaching from employers to clients, genuine graduates, educational institutions, and the public sector. Employers suffer labor high turnover and cost of replacing, loss of patronage and revenue, possible lawsuit, and reputation damage (Eckstein, 2003). The genuine graduates, on the other hand, are robbed of opportunities, and educational institutions also suffer their names being dragged in the mud.

In the light of the problems mentioned above, it is reasonable to pursue a system of certificate verification that is effective, efficient, trustworthy and seamless to use for institutions and employers. In this study, the challenges faced in the conventional verification system will be explored, and how these challenges can be addressed in an alternative system will be examined.

1.2 Research Objectives

This study aims to explore the current certificate verification systems for an understanding of its underlying issues and then develop a framework for its optimization through the adoption of blockchain technology. More specifically, the following objectives have been drafted:

1. Explore the current certificate verification system and the factors that prevent it from being effective, efficient, and convenient.
2. Describe how a blockchain-based solution can enhance the current certificate-verification process.
3. Examine the factors that can hinder the use of blockchain technology.
4. Analyze the impact of the blockchain-based solution on the stakeholders of the verification systems.
5. Develop a framework for the implementation of blockchain technology for certificate-verification systems.

Exploring the causes of the problems highlighted in Section 1.1 above is fundamental to understanding how the technology can be used to improve the system. Without adequate knowledge, there will be no basis for the adoption of an alternative method. The blockchain technology will, therefore, enhance the certificate-verification systems by saving time, reducing cost, and making the process seamless. Besides, the factors that can obstruct the system needs to be examined and correctly understood to consider possible ways to improve it. Lastly, we must consider the stakeholders regarding the impact the technology will have on their duties. Such an approach is extremely crucial to the success and acceptance of the technology.

1.3 Context

The credential is a broad term that refers to educational certificates, degrees, certifications, and government-issued licenses. Credentials confirms that the holders have mastered a skill, attained an educational qualification and has the right to carry out activities. Credentials also have actual financial rewards in the world of works. Even though the terms are often interchanged, Association for Career Technical Education made a distinction among the different credentials. An academic degree, being the subject under focus here, is awarded a graduate after completing a program or courses of study spanning over multiple years at a higher educational institution (ACTE, 2018). The term certification, according to Grech & Camilleri (2017), endorses an assertion. In their analysis, they identified that a certification process includes the: 1. The claim – a statement that affirms a fact; 2. The issuing body with the responsibility to examine and confirm that facts it is attesting to are true. Evidence backs up a claim and often indicate the manner through which the claim is validated; 4.A recipient – the person on whom the claim is conferred; 5. A certificate which testifies about the issuing body, the holder, the claim and also points to the evidence; 6. Lastly, every certificate must include some form of signature that only the issuing body can append as their unique identifier.

To adequately illustrate the interactions between the actors (recipient and issuer) and the variables in the certification process, we use the Signavio application to draw a Business Process Model and Notation (BPMN) in Figure 2. A BPMN is a graphical presentation of the activities plan in a process from start to finish. It is used to graphically provide a simple understanding of rather complicated and technical operations. Thus, the BPMN

legend in Figure 1 below is first presented to explain the meaning of each symbol that will be seen in Figure 2 and subsequent Figures.

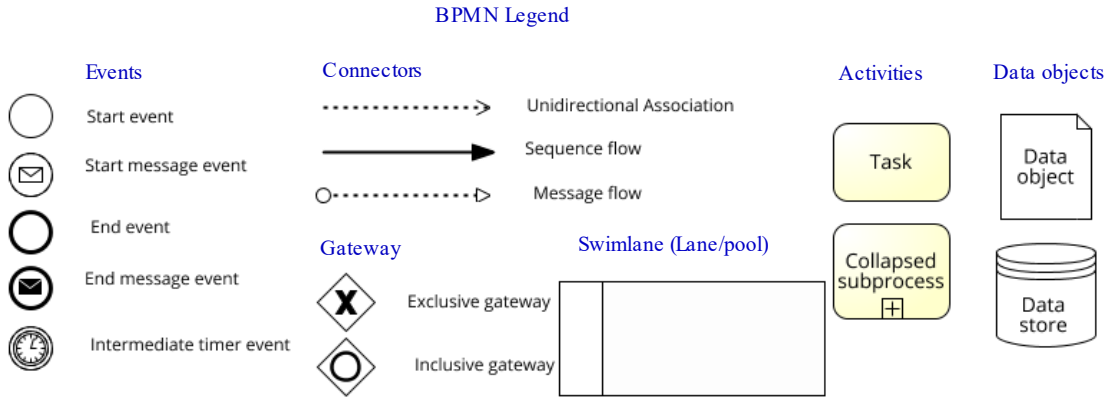

Figure 1: Business process model and annotations legend, source: author.

Following the Signavio BPMN tools, the *start event* in Figure 1 launches a process that causes the first action. It leads one through a sequence of activities to the *end event*, which signifies the completion of the possible activity sequences, marking the goal of the entire process. The *start message event*, on the one hand, shows the receipt of a message for action from an outside actor, and the *end message event*, on the other, is a simple way of showing that a process ends with sending out a message. The *intermediate timer event* indicates the time lag within a process; for instance, a time delay before an activity takes place. More so, the three basic connectors, namely sequence flow, message flow, and association, are used to connect different elements on the diagram. Whereas the *sequence flow* specifies the order of the elements, the *message flow* establishes the flow of communication, and the *unidirectional association* defines the information flow.

Additionally, the *exclusive gateway* shows the point where only one path can be followed per time where multiple alternatives are presented, and the *inclusive gateway*, on the contrary, splits a sequence flow to several paths. Similarly, the *task* node depicts the minute steps in a process. When the *collapsed subprocess* is used, it enhances clarity by representing details that are not visible on the diagram. Also, the *data objects* are generally used to convey information during the process. However, the data store holds information explicitly in the long term for update or retrieval. Lastly, the swimlane represents both grouping elements, namely, pools and lanes. Pools define the boundaries of an organization where the lanes typify roles within an organization.

Based on the understanding of a BPMN discussed above, Figure 2 here describes a certification process. The recipient initiated the process by desiring a certificate and went further to apply for admission to the issuer institution. The latter starts with a message event by the receipt of the application. The process continues with parallel tasks from the issuer "accepts student" with a corresponding task "gains admission" on the recipient lane up to the point where issuer "examines student" and the recipient "takes qualifying exams." At the exclusive gateway, the process can either follow the path to *notification of disqualification* (denoted by an end message event)/*no certificate is received* – or – *issues/receives a certificate* where the process comes to a completion. The certificate repository is an essential component of the process where certificates are stored and retrieved for such reasons as certificate verification.

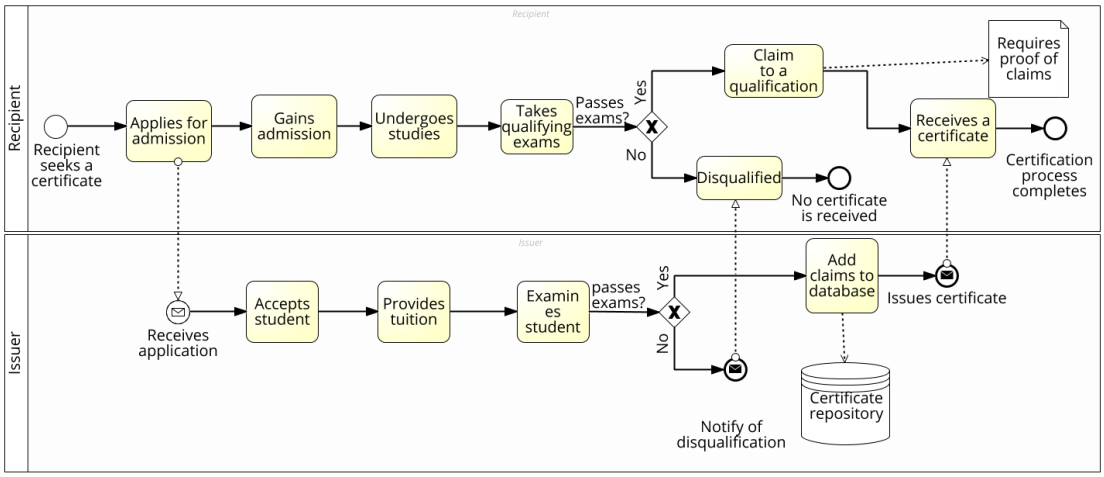

Figure 2: The process model for a certification system, source: author.

The genesis of widespread academic fraud in Nigeria can be traced to the early 1970s when the award of contracts to persons without educational qualifications became prevalent. Funds were disbursed to these contractors who could not deliver and were not called into question. Within a short space of time, these contractors became super-rich. These contractors sought for ways to legitimize their wealth and resorted to obtaining credentials. However, some of them patronized fraudulent means. Soon, unemployed youths, undergraduates, and potential graduates learned that intellectual prowess was not required to get rich and that there was no need to study hard, instead seek connection and then get credentials by any means (Odetunde, 2008). Onwudebelu et al. suggest that to ensure proper records are kept, introducing electronic records alongside paper records is a logical choice. They also added that digitalizing students' academic records would

enhance the longevity of records, prevent alteration, and ease retrieval of such records (Onwudebelu et al., 2013).

Academic fraud is the intentional misrepresentation of academic achievements that has a potentially detrimental effect on other parties (Du Plessis et al., 2015). Academic fraud consists of a wide range of dubious activities in the academic parlance, among them is degree forgery. The latter can be the mutating of the content of a certificate that originated from a legitimate source to suit the holder. Another type of fraud is that the certificate origin and content are both fake, which may, however, be difficult to spot (Ghazali & Saleh, 2016a). A further definition of counterfeit degrees is given by Bowes (2018), who describes it as a certificate obtained from a fake institution – diploma mills – bearing a genuine institution but is not issued by the alleged institution.

Various sources of a fake degree include unaccredited degree-awarding institutions, degree mills, and corrupt officials in educational institutions (Garwe, 2015). A particularly worrisome form of academic fraud in recent times emanating from the activities of diploma mills and their accomplice, accreditation mills. Degrees are advertised in periodicals and are marketed on a large-scale (Eckstein, 2003). According to Cohen and Winch (2011), diploma mills are online entities that offer nothing more than substandard or fake degrees in exchange for payment. Diploma mills typically go by such names as universities but are in the business of selling false certificates for profit (Attewell & Domina, 2011).

According to WENR, the anecdote for degree forgery or counterfeit is a secure authentication procedure(Trines, 2017). Verification is for Ghazali & Saleh, (2016b), the process of confirming that something is original. Degree verification is the process that proves the authenticity of a graduate degree by using a proven technique. (Balsubramanian et al., 2009) considers document verification as the steps taken to ascertain that documents received from an owner are genuine and that the owner is legitimate. Du Plessis et al. (2015) provide explanations of a degree verification as confirming the authenticity of the certificate and the qualification and the legitimacy of the issuing body at a given time.

Degree verification seeks to track a certificate to its source, the means of issuance, and other details about the basis of issuance (Ghazali & Saleh, 2016a). Certificate verification clears doubt about the indicated institution, whether the institution has issued them and whether the issuing institution is authentic, This invariably authenticates the issuing institution and the qualifications they offer. The essence of verification is also to ascertain that a degree has not been modified by the holder and whether it was genuinely issued to the holder (Du Plessis et al., 2015).

Electronic verification is the automation of some of the processes of verification through appropriate tools (Brdesee, 2019). Bowes defines electronic verification as a "verification through a web-interface without creating a centralized database to ensure data privacy." It operates within a digital certification ecosystem and facilitates an automatic authentication of a degree by a third party without the intermediation of the issuing institution (Ghazali & Saleh, 2016b). Through this medium, authentication can be accomplished instantly, which saves time for all parties, and certificates are shared more easily and securely.

An online certification system is a system database that can accommodate three groups of users – the issuing institution, the degree holder, and the verifier. An institution issues a digital degree to a graduate after they have fulfilled the academic requirements. The student, on the other hand, enquires into the database to access and share the electronic certificate. At the same time, the verifier also enquires into the system to authenticate the degree (Swetha & Priya, n.d.)

Blockchain technology can be loosely described as a distributed ledger technology (DLT). The distributed ledger technology promotes, within a network, the recording of transactions, tracking of assets, and the sharing of the same in a decentralized way (Manav Gupta, 2017). The term asset refers to both tangible and intangible. This further suggests that anything of value can be tracked using blockchain. Holbl et al. (2018) explain that blockchain technology, also called a distributed data store, is the sequential record of data in blocks and that the blocks link up to form a ledger. Blockchain is a means of storing and distributing information securely among transacting parties with absolute transparency and void of any central control. Blockchain technology emerged from the combination of software engineering, distributive computing, cryptographic science, and

economic game theory. The functionality of blockchain draws on all these areas to facilitate its natural immutability and adaptiveness. This provides the grounds for the security of digital assets as well as the decentralization network of participants (Sultan et al., 2018).

1.4 Summary

This chapter discussed briefly how relevant an academic certificate is and how certificate forgery is increasing and that blockchain technology can adequately address this issue. We discussed the problems of the current solution to certificate forgery; next, we stated the objectives and established the context for which the concepts in subsequent chapters should be understood.

2. Related Work

An understanding of related studies is critical to research in setting the foundation for the ensuing investigations. Such understanding fosters knowledge of what is already achieved and the knowledge gap that the current research should fill. This chapter aims to present background studies and to explore further the reviews that are directly related to the objectives of this paper. This background study is sectioned into three parts. While the first part in Section 2.1 explains fundamental issues to this thesis, the second part in Section 2.2 discusses the blockchain technology, and last being Section 2.3 is the theoretical framework.

2.1 Earlier Studies

The earlier studies will elaborate on themes bordering around certification (since certificate verification exists within the certification ecosystem) in the first segment and the blockchain technology in the second segment. The topics discussed in the first segment include the certification system, paper-based certificates, non-blockchain digital certificates, and verification systems. In contrast, the second segment comprises the blockchain technology: its concept, components and operations, types, features, and the suitability of blockchain technology to the verification systems and potential use cases in education.

2.1.1 Certification System

Any entity can issue a certificate to anyone to testify about anything. However, Grech & Camilleri (2017) observed that for such a certificate to be acceptable and worthy of trust by a third party, certain conditions must facilitate its trustworthiness. They identified the following:

- **Method for Identity-Verification**

They noted that the identity of who is involved in the transaction – the issuer and the certificate holder – must be valid to create trust. The identity of the issuer is often verified

by identity documents such as a certificate whereby third parties are involved. In Nigeria, such a third-party entity with authority to certify a university is the National University Commission (NUC).

- **Standardized Processes for Issue and Certification**

Third parties need to have an absolute trust in the procedures the issuing body follow in reaching their conclusions. Grech & Camilleri posits that all certificates within a certification system must be issued in a predictable way and with equity. This means that certificates are issued to any recipients once and only when they satisfy the requirements stipulated in the documented standards.

- **Mechanisms for Regulation and Assurance**

After the standards for certificate issuance are laid out, Grech & Camilleri added that every party needs to uphold the principles guiding such standards as it applies to each one. To make the system trustworthy, a mechanism for checking every member involved acts per the obligations of the standards, and if not, to reveal (and possibly sanction), the defaulter must be inclusive of a certification system.

- **Security Features**

It is against the security features embedded on a certificate that a verifier checks to determine that a certificate has not been forged. How institutions prevent certificate forgeries include 1—integrating on the certificate physical tamper-proof elements such as signatures, watermarks, features unique to the issuer only; 2. Maintaining a database of issued claims on a central registry database of the issuer wherewith any verifier can consult to authenticate a certificate.

- **Accessibility**

According to Grech & Camilleri the ease of accessing the claim on a certificate connotes that 1. The certificate recipient must hold a copy of the certificate; 2. Third parties should be able to access the certificate easily; 3. The certificate should provide information about verification procedures, standards, and processes of issuance of the certificate, 4. Information on the certificate must be clear, easy to use, human and machine-readable

2.1.2 Paper-based Certificates

Most degree-awarding institutions currently issue paper-based certificates, which is a physical certificate made of paper, to graduates. Nguyen et al. (2018) note that forgery challenge stems from the certificate designs and the verification process. They observed that the paper-based certificate, despite its weaknesses, is still more secured and more resistant to forgery since certain unique features can be embedded in the design of the paper certificate. While on the flip side, it is difficult to identify the counterfeit when the paper-based certificate has been forged. Also, the possibility of collision between the verification officer and the academic fraudsters to perpetuate and conceal a dishonest act cannot be ruled out. In more specific terms, the limitations of the paper certificate include:

- Possibility of forgery: Every paper certificate is vulnerable to counterfeiting. In most cases, the quality of forged certificates is practically the same as the original owing to the high-tech printing and photocopying machines. Technological advancement has made it extremely easy to make a counterfeit certificate (Ghazali & Saleh, 2016b)

- Paper certificates are vulnerable to natural disasters such as floods, fire outbreaks, and war. It lacks security to certificate and therefore be easily lost or damaged (Swetha & Priya, n.d.)

- Reapplying to replace lost or damaged copy is time-consuming and often requires an in-person application.

- The database of the issuing institution is single points of failure. In the event of any problems, the opportunity of verification would be lost even though the certificate might still be valid (Grech & Camilleri, 2017)

- The verification process is often manual and lacking in efficiency and effectiveness;

- Once a certificate has been issued, it is challenging to revoke, except the holder is made to give up ownership (Arenas & Fernandez, 2018).

2.1.3 Non-Blockchain Digital Certificates

The alternative solutions digitize the paper certificate for an easier and automatic issuance to overcome the shortcomings of the paper-based certificates. Consequently, the digitizing of certificates lessens the crude activities involved in the issuance of paper-based certificates such as sourcing materials, printing, and sealing (Nguyen et al., 2018). Grech and Camilleri also emphasized that this format requires fewer resources for issuance, maintenance, and use, relatively secure from issuer-fraud, and easy to check the authenticity against the database, depending on the standards adopted in the system design.

While the digital form of certificate tolerates lost or damaged certificates since it can be easily copied and pasted in a different location, this ease of duplication is one of the reasons the digital certificate cannot be widely adopted. Also, the issues of transparency, reliability, and trust in paper-based certificates are present in digital certificates. (Nguyen et al., 2018).

Grech and Camilleri (2017) also buttress that in the absence of digital signatures, forging a digital certificate is overly easy and that when a digital signature element is added, a third-party must be consulted to uphold the integrity of the transaction. Such involvement yields much control to the third party, which can be exploited. Additionally, maintaining a secure database for the records requires highly sophisticated backup systems that are not immune to failures and large-scale data breaches. It is thus susceptible to destruction and failure, which may render the certificate useless as they hold no value without the database.

2.1.4 Verification system

Due to the possibility of forgery, the issuing institutions are under an obligation to maintain a verification unit within the institution to curb instances of fraud of their certificates, which can threaten their integrity. The institution keeps a central registry to answer queries about the genuineness of a certificate and its content and whether it rightly belongs to the holder (Ghazali & Saleh, 2016b).

A verifier who seeks to ascertain that the genuineness of a certificate can take either of the two approaches; 1. send inquiries to the issuer institution; 2 approach an intermediary organization that maintains a secondary database on behalf of the universities or is in the business of investigating degrees. Either approach often attracts a fee from the employer, which can be a significant amount of money if there are numerous certificates to verify. This extra cost can discourage the practice of verifying every certificate. Thus, certificate forgery may continue to go unchecked (Hall, 2017).

Every verification system inherits the shortcomings of the prevalent certification system in an institution. Typically, a verification system persists so long as the issuing institution endures for preserving and archiving the students' records. While it is expected that the owners of certificates will keep their copy securely, however, there are chances that occurrences will negatively impact on the security of the certificates in the institution and in the custody of the bearers. Social unrest, for example, can jeopardize the safety of academic records causing them to become unavailable or damaged. In such an event, there may not be the possibility of verifying a qualification (Hall, 2017).
Nguyen et al. (2018) identify the issues with the traditional verification process that spawns its high level of inefficiency and ineffectiveness. Since the verification processes are predominantly manual, they are often:

- Deterrent: the verifier (employers) are not able to personally verify the certificates applicants present since the secret element that distinguishes a genuine certificate from the counterfeit is with the issuing institution only. To verify the certificate, they must reach out to the issuing instruction, seeking for verification of certain certificates and pends the recruitment process awaiting the outcome of the verification request (Nguyen et al., 2018);

- Time-consuming: When the verifiers decide to follow through with the process, they spend so much valuable time on the process, from the time they reach out to the university, to the time before they get a reply from the institution.
- It is a robust and tedious exercise for the university and expensive to the verifying company;
- Inadequacies in the system could permit a forged certificate to go unnoticed;
- Constitutes an extra burden on the issuing institution;

- And human capital intensive.

2.2 Blockchain Technology

Blockchain first made a public appearance through an unknown entity by the name of Satoshi Nakamoto in 2008, who released a paper that improved the functionality of electronic cash through a peer-to-peer network, which he identified as Bitcoin. He sought to resolve the shortcomings of mediating financial institutions in the electronic transfer of funds. He proposed a secured cryptographic system of payment with a feature that makes it impossible to reverse transactions, thus preventing fraud and reducing the cost of transacting (Nakamoto, 2008). Bitcoin was the first use case of blockchain. The latter, therefore, must not be mistaken for bitcoin as it is the structure on which Bitcoin application, as well as other applications such as Ethereum and Smart contracts, are developed. Beyond cryptocurrency, it has gained prominence and is continuing to find new applicability in various fields due to its decentralization and immutability features (Budhiraja & Rani, 2019). Its common areas of application include the financial sector for cryptocurrencies, in the health sector for managing patient records, in the public sector for land registry, and are gradually becoming popular in public procurement and the educational sector to mention a few. Blockchain is a significant disruption in the world of technology.

Blockchain, also called the Distributed Ledger Technologies (DTLs), makes it possible for parties that do not trust each other to exchange digital data or value on a peer-to-peer fashion without third parties (European Commission, 2019). Value could constitute money and land titles, while data can be medical records and certificates. According to Yang et al., (2018), the Distributed Ledger Technologies had been proposed since the 1990s and is fit for use in any system that can be managed through a distributed platform. For clarity, DLTs are a category – to which blockchain belongs – of databases that are used to record, share, and synchronize data among a wide range of computers and participants. While DLTs are not all blockchain, the latter is different from the other DLTs by the way it deploys cryptography in recording and synchronizing data into a chain of blocks (European Commission, 2019). Any update on the database is guided by the underlying principles and are shared within the parties (Bhatia & Wright de Hernandez, 2019).

2.2.1 Blockchain Workflow and Components

This subsection is intended to provide in-depth knowledge of blockchain components and their functionalities for a better understanding of the entire mechanism. An overview of the workflow in the blockchain is given before discussing the details in subsequent sub-subsections. Figure 3 below, therefore, briefly highlights key procedures starting with signature generation. The signature generator consisting of Cryptography and Data Encoding is used to generate digital signatures. It requires cryptographic keys, such as the private and public keys, and follows a set of rules (Geldenhuys & Hoffman, 2012). The private key encrypts a message that is broadcasted on the network, as explained in Section 2.2.1.1. When this transaction request is made, the nodes (as in Section 2.2.1.2) verify the transaction as discussed in Section 2.2.1.3, in line with the consensus model (as in Section 2.2.1.4) agreed in the network. After that, a block (described in Section 2.2.1.5) is created to publish the validated transaction. The block creation and other components are explained in the subsequent sections.

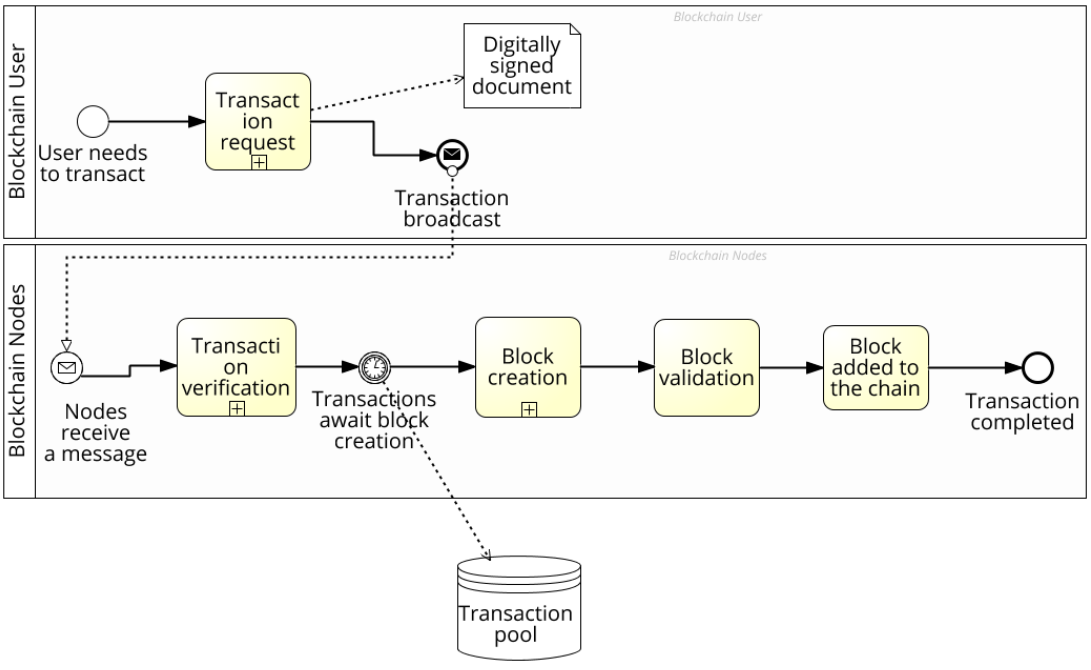

Figure 3: Workflow of a transaction in the blockchain, source: author.

2.2.1.1 Transaction Request

Transactions are data (usually the message) that are entered into the network. The messages may constitute inputs to or outputs from computer programs. Also, the contents of the message may be encrypted or maybe a link to an encrypted data in another digital location. The transaction request in Figure 3 is symbolized with a collapsed subprocess to exclude specific details that cannot be captured in the diagram. This step is often characterized by hash generation, message encryption, and digital signing using a private key after which is broadcasted on the network. Following this step is the action of other nodes in the blockchain users' lane, as in Figure 3(Murphy, 2016) (Ismail et al., 2019).

2.2.1.2 Nodes

The computer system representation of a blockchain participant is referred to as a node. Alammary et al explained that every node in the network keeps a copy of transactions and that a node also records the transactions in its ledger after it gets a consensus from other nodes in the network. A node publishes to the other nodes, any transactions its user (human) initiates in the network and routinely confirms that the copy of the ledger it holds is the same as other nodes on the network (Alammary et al., 2019).

2.2.1.3 Transaction Verification

Blockchain deploys digital signature through cryptography to confirm that a transaction is authentic. The signing of transaction in the request process is accomplished through a private key as users possess a pair of private and public keys. While the private key is confidential to the user and used to sign any transactions in a process that encrypts the message, the encrypted message is published to the entire network. Again, this is shown in Figure 3 to be a collapsed subprocess because it involves a set of activities from the peers who validate the user that makes a transaction request and verify the message using the public transaction key. The verification process checks to ensure that the message has not been tampered with (Zheng et al., 2017). A transaction that is validated successfully is authentic and held in the transaction pool, pending its addition to the ledger on the block. It is thus represented as an intermediate timer event in Figure 3.

2.2.1.4 Consensus Algorithms

Many nodes participate in a network and are assumed to be unreliable. The consensus algorithms support reliability in a network by ascertaining that subsequent nodes are

indeed the original version and guard the system against being hijacked and forked by malicious groups. Yang et al. pointed out that before any transaction is recorded in the blockchain, decentralized scrutiny is performed to give no opportunity to illegal transactions to materialize (Yang et al., 2018). The consensus mechanism is a ruleset that guides the participants in the verification of transactions, validation, and addition of transaction blocks to the blockchain (European Commission, 2019). A particular consensus model may be selected from among the different types that exist, including Proof of Work, Proof of Stake, Round Robin, Proof of Authority/Proof of Identity, and Proof of Elapsed Time (Yaga et al., 2018).

2.2.1.5 Block

Yaga et al noted that a block in the chain is made up of block header and the block body that records transactions on the ledger in their order of occurrence. Information relating to each block (block metadata) is found on the header that often includes a time-stamp, a hash representing the data of the block, the hash of the preceding block's header, the block size. It may also contain the cryptographic nonce in the case where a hash puzzle has to be cracked to publish a node (Yaga et al., 2018).

A block exists within a distinct network and follows the rules set by the members of the network. It ensures the accuracy of time and order of transactions before they are included on the blockchain. Through the hash function, every succeeding block reinforces the authenticity of the preceding block and, in extension, the whole blockchain. The procedure makes blockchain tamper-proof, hence the immutability feature (Manav Gupta, 2017).

2.2.1.6 Block Creation and Validation

Transactions that have been validated by the nodes are held in a memory pool pending addition to the block. The addition of transactions into a block must be undertaken by only one participant and is extremely difficult to determine from among many distrusted participants. This decision is, therefore, based on the set of rules that govern the participants, such as Proof of Stake and Proof of Work. This step is also a collapse process in Figure 3 because the node that creates and publishes a block in a Proof of Work Model, for instance, must first solve an intensive mathematical puzzle, the "work" being the solution to the puzzle. Publishing a block in the Proof of Stake model depends on the

amount of stake a user has on the entire network because it is believed that the user with an enormous investment on the network will most likely want the good of the network. After creating a block, a transaction is added to the block, and all nodes agree by validating the block. Once the blockchain updates - which occurs very regularly - no change can be made on the transaction (Greg Walker, 2015) (Yaga et al., 2018).

2.2.1.7 Chaining of Blocks

The information of preceding blocks – in the form of a hash value – contained in the header of each succeeding block links up the blocks to make a blockchain, leading to the "transaction completed" end event in Figure 3. Each new block continues to carry the hash of the preceding block to form one whole network. Any change to a block changes the hash value of the block and must change the entire network of blocks, which does not occur without notification to all the nodes. As soon as a modification message is detected, this can be rejected, which keeps the blocks unaltered (Yaga et al., 2018).

2.2.1.8 Hash Function

A hash likened to a human fingerprint is a unique identity for each digital data on the blocks and a critical component of blockchain technology that is applied to many operations. Hashing is the technique of transforming any data input through mathematical computation into an output of hash values within split seconds. The same input will generate the same output each time to confirm the genuineness of the data, but any little disparity in the input would produce a different hash value. The output does not give any clue to the inputted data. The hash that has been entered on the distributed ledger is a proof that a document exists while the content of the document can only be accessed through public/private key functions (European Commission, 2019) (Yaga et al., 2018).

2.2.1.9 Wallet

Anyone who seeks to perform any activity on the network, private or public, will need access to the network. A software application such as desktop applications, smartphone applications, and digital wallets, serve to mediate between the users and the blockchain technology. A blockchain wallet allows an individual to send and receive digital assets, securely store private keys, public keys, and connected addresses. It can be installed directly on a system or used from a browser (Grech & Camilleri, 2017) (Yaga et al.,

2018). A graduate, for instance, must access the network through a wallet to receive from the issuer and share with an employer, his digital certificate.

2.2.2 Types of Blockchain

According to Fernández-Caramés & Fraga-Lamas (2018), blockchains are categorized based on data management, data accessibility, and the participation of each user. The three main categories which Li et al., (2019) provide include the public networks, private networks, and the consortium networks with varying levels of decentralization:

- Public networks – permissionless This type of network is the typical blockchain, completely decentralized, and all data stored in the blockchain is publicly accessible to every node. Data usage is not restricted in any way. To make sure the network is secure, the consensus protocol mostly in use on this network is the Proof of Work. The computational difficulty discourages the proliferation of counterfeit blocks.

- Public networks – permissioned (Consortium). According to Li et al, a consortium blockchain is built on a public network but allows only a specified set of nodes. While all nodes may not be able to take part in the validation of transactions, all nodes may participate in safeguarding the network, and data availability are limited. This may comprise a group of organizations.

- Private networks. As a closed network, only selected users can join, read, write, and audit the blockchain. The validation of transactions is faster and cost-effective than the public network. However, the decentralization feature of blockchain is compromised.

Zheng et al. took a slightly different approach to distinguish the types of blockchain. They spelled out, in a precise format, the properties that set the different blockchains apart, as represented in Table 1. According to Zheng et al., determining the rule set by which the network operates is a distinguishing factor where the private blockchain, for instance, involves only participants in an organization. Also, permission to read is not the same for all the blockchain types. Similarly, the question of whether records are unchangeable depends on the type of blockchain that is being operated. It could be possible to alter a private blockchain, for instance, because access control is restricted to a few specific

participants on whom the authority over the network is vested, explaining why it is much less decentralized as well. Furthermore, the efficiency differs in the network types. Operating a permissionless consensus, the public network is typically slow due to the intensity of the mathematical computation performed in the PoW consensus to publish a block, unlike the consortium blockchain that functions through a permissioned consensus requiring a different model to publish a block and is thus more efficient.

Property	**Public blockchain**	**Consortium blockchain**	**Private blockchain**
Consensus determination	All miners	The selected set of nodes	One organization
Read permission	Public	Could be public or restricted	Could be public or restricted
Immutability	Nearly impossible to tamper	Could be tampered	Could be tampered
Efficiency	Low	High	High
Centralized	No	Partial	Yes
Consensus process	Permissionless	Permissioned	Permissioned

Table 1: Comparisons among the public, consortium, and private blockchains, source: (Zheng et al., 2017).

2.2.3 Features of Blockchain

Blockchain features a decentralized and tamper-proof database that is highly secure and transparent. Also, the history of a transaction can be traced, an important feature that could bring many benefits to a certificate verification system. These key characterizes are further discussed below**.**

2.2.3.1 Decentralization

In any system, it is necessary to ensure the validity of transactions. In a centralized system, a third party is charged with the responsibility of validating transactions, resulting in additional costs and impediments of the intermediary. The blockchain, however, rules out any intermediation by a third party and instead transacts on a peer to peer basis whereby records are stored on every node on the network. The consensus algorithm is deployed To ensure the regularity of data in the blockchain (Zheng et al., 2017a). Many studies agree with the point made in Yaga et al. that the greatest benefit of blockchain technology is its decentralized structure (Yaga et al., 2018).

2.2.3.2 Tamper-evident

After the conditions of a transaction have been agreed upon, no participants can alter the record. If any situation such as error and change of decision necessitates reversal, there must be a new transaction in such a way that both transactions exist and are visible to all participants. Thus, any change to a transaction leaves a trail (Manav Gupta, 2017).

2.2.3.3 Immutability

The concept of immutability suggests unchangeability. Practically, a transaction that has been created in blockchain cannot be easily modified since it is distributed among nodes in different locations. Its characteristic tamper-evidence lends to its immutability. Attempts to modify the data from a single node can be interpreted by other users as a dishonest act and an attack, and will be stopped (Grech & Camilleri, 2017)

2.2.3.4 Transparent

The public blockchain is accessible to all participants who have an internet connection, to read, update the ledger in line with the existing consensus mechanism. In this context, no transactions are concealed nor vague to participants, and they can trust and audit the system as they wish. However, in a private blockchain, only predetermined participants can access the messages (European Commission, 2019). Murphy indicates that the level of transparency necessary for use may be the criteria for the choice of a blockchain type with regards to the legal and regulatory matters that must be considered (Murphy, 2016).

2.2.3.5 Provenance

Another important feature is the ability to trail a transaction to its origin on the blockchain technology. If there is any need to see how the ownership of an asset has evolved with time, participants can find out on the platform (Manav Gupta, 2017). Sultan et al. (2018) maintain that provenance is established by the transparency of the technology.

2.2.3.6 Security

Typically, the triad of confidentiality, integrity, and availability defines security in information systems. Confidentiality refers to the protection of most sensitive data from access by unauthorized accesses. At the same time, integrity ensures that data are not

modified by unauthorized persons, and the possibility of undoing the modifications done by such persons, and availability is that data can be accessed when necessary. The blockchain technology provides the means for maintaining the privacy of data through digital signatures, the immutability of records stored on the blockchain ensures the integrity of data. Since records on a blockchain are distributed over many nodes, an attack on one of the nodes does not affect information availability (Fernández-Caramés & Fraga-Lamas, 2018).

2.2.4 The Suitability of Blockchain Technology to the Certification System

Several studies have identified how to determine the applicability of the technology to a system. Researchers suggest a decision-making process whereby certain propositions are considered before deciding whether the adoption of blockchain is relevant. A decision may be made after considering the answers: "Is there a requirement for a database with multiple writers? Is there the possibility of mistrust between these multiple writers? Will there be interactions between the transactions written by multiple writers? And are intermediaries - gatekeepers - required for verification?"(Hall, 2017).

- The blockchain technology is suitable for databases with different writers – entities – who create transactions that alter the database. Continuous postgraduate education, as well as the increasing popularity of short course programs, gives rise to the need for different educational institutions to maintain a record of an individual's qualifications into each of their databases.

- Since multiple entities are writing to the database, some level of mistrust must exist among them. Trust for one another is fostered by mutual recognition, which is not feasible in this era of global higher education and a wide range of education providers. This, therefore, rules out the possibility for trust among the writers.

- Blockchain technology is also relevant for the interaction of the records that are generated from different databases. While the records exist in distinct databases, there is a need to connect in diverse ways, such as in Credit Accumulation and Transfer Systems (CATS).

- Lastly, Hall (2017) elaborates that whether there is a need for a third-party intermediary for verification can be considered first by deciding who the primary

parties are, then the purpose and nature of the third-party intermediation. In the certificate verification system, the student and the employer constitute the principal actors, while the issuing institution's role only adds value to the transaction. Hence, the use of blockchain would be beneficial for the automatic reconciliation of the different databases, more cheaply, and quickly without requiring a trustworthy third party.

Figure 3 below is a comprehensive flow diagram that supports determining the appropriateness of blockchain application and the type of blockchain that is necessary depending on the needs of the institution. Each decision point is represented by an exclusive gateway to show the path that must be followed. According to the diagram, even if multiple writers trust each other but do not have a common interest, they will need a third party. If they need a third party but cannot trust any, then they can consider a blockchain and a preferable consensus mechanism. Additionally, the access right the writers may have and whether the records should be made public determines the type of blockchain to deploy. Whereas the public blockchain can be used when access right is unrestricted, and the transaction can be public, the consortium blockchain can be considered where there is an access control and involves more than one institution.

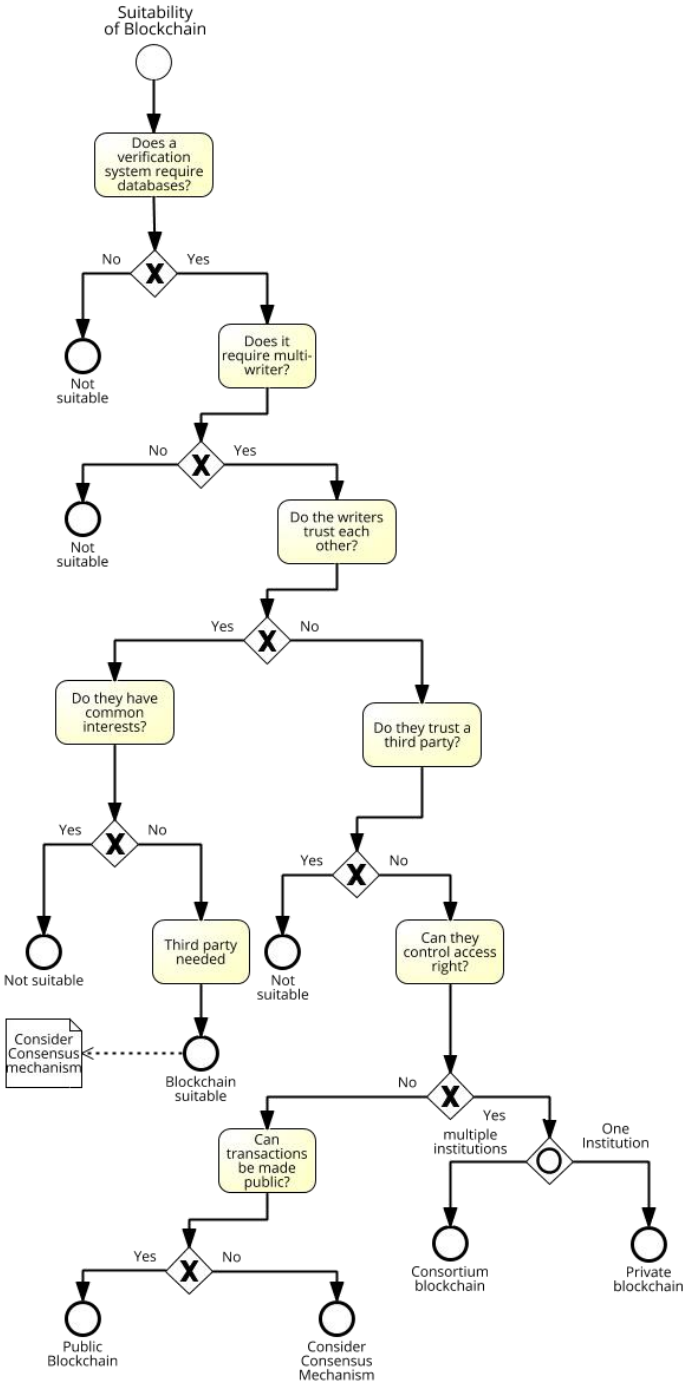

Figure 4:Determining the suitability of blockchain, source: author.

2.2.5 Potential Uses of Blockchain in Education

The technology is beneficial to a wide range of industries, including the educational sector. Beyond certificate verification within the sphere of education, Grech & Camilleri, (2017) have identified the many other uses for which blockchain can be applied. They

also explained the current state of the suggested use scenarios, described the possible ways of applying blockchain, the advantage of doing so as well as the requirement for the application. Some of these are presented in Table 2 below**.**

Usage scenarios	**Current State**	**Description**	**Advantages**	**Prerequisite**
Permanently secure certificates	Certificates are in paper or electronic format using public key infrastructures, requiring PKI intermediaries. The verification system can be destroyed.	Issue digital certificates, store the digital fingerprint of the certificate on a public Blockchain for easy authentication.	Securely and permanently stored on the blockchain. Verifiable anytime, any day. No additional cost once issued.	Issuance and verification software such as the Blockcerts is required.
Verify multi-step accreditation	Employers and educational organizations need to verify the quality of the certificate issuer.	The accreditation organization puts its digital signatures onto the blockchain to show that the issuer institution is certified by the authority.	Organizations easily check the pedigree of the issuing institution. Visualize the accreditation chain.	Accrediting organizations publish the accrediting certificates (or the signatures of those certificates) on a blockchain.
Automatic recognition and transfer of credits	No meta-data standard to describe ECTS or EQAVET, no standard database for storing ECTS, and no standardized way to automatically store ECTS or EQAVET.	Educational organizations that use credits to award learning (such as Higher Education Institutions using ECTS, or vocational institutions using ECVET), would award and transfer credits on a custom-Blockchain.	Proofs of the validity of certificates stored on the blockchain. Certificate stored on the blockchain. No need for the creation of “backpacks” to store the certificates. Educational history is instantly visible and verifiable.	There should be a standard for credits. Creation of a custom-blockchain for this purpose Acquire software to interact with the blockchain. Mass of institutions should participate.

Usage scenarios	Current State	Description	Advantages	Prerequisite
Automatic recognition and transfer of credits	No meta-data standard to describe ECTS or EQAVET, no standard database for storing ECTS, and no standardized way to automatically store ECTS or EQAVET.	Educational organizations that use credits to award learning (such as Higher Education Institutions using ECTS, or vocational institutions using ECVET), would award and transfer credits on a custom-Blockchain.	Proofs of the validity of certificates stored on the blockchain. Certificate stored on the blockchain. No need for the creation of "backpacks" to store the certificates. Educational history is instantly visible and verifiable.	There should be a standard for credits. Creation of a custom-blockchain for this purpose Acquire software to interact with the blockchain. Mass of institutions should participate.
Lifelong learning passport	Only Open Badges offers a verifiable record of experience and credentials.	Learners store evidence of formal and non-formal learnings.	Instantly verifiable CV with evidence of all learning and employment. Reduce CV fraud. Reduce the workload of organizations in verifying CVs.	Creation of a verified digital federated identity. Creation of a blockchain. People upload claims. Several users (nodes) confirm the claim. Claim receives a trust score.
Tracking intellectual property and rewarding use and re-use of that property	Costly endeavor ran by specialized organizations. Too complex for self-publishing authors. Minimal tracking on the use of intellectual properties.	Educators announce the publication of open educational resources on the blockchain—record references.	Eliminate intermediaries. Allow anyone to publish openly and keep track of re-use without limitations. Enable metrics-based decisions about the material to use.	Announce a publication on the blockchain. Add a link to the resource. Announce reference material, create an award system for educators on the platform based on the level of re-use.

Usage scenarios	Current State	Description	Advantages	Prerequisite
Receiving payments from students	Students pay for their studies using a specified currency	Students would provide payments for studies via blockchain-based cryptocurrencies.	Take away all the barriers associated with paying fees, especially cross-border studies.	Institutions and students should have wallets for the cryptocurrency.
Providing student funding	Students are funded through the Voucher system and may be subject to conditions. Tracking compliance with the conditions often demands significant administration.	Give vouchers to the student on the blockchain. Vouchers can be programmed to release tranches of funds based on the fulfillment of certain conditions.	Decrease the bureaucracy required to manage the voucher system. The system could be linked to students' loans.	Software to build a smart contract and upload to the blockchain (Ethereum supports this). Include data sources from where smart contracts know when conditions have been fulfilled.

Table 2:Potential cases of blockchain in education, extracted from (Grech & Camilleri, 2017).

The usage scenarios in Table 2 highlight real examples of areas in the educational sector where the blockchain technology is currently minimally or never applied. As we shall consider in more detail in Section 2.2.1, some early adopters have already begun to permanently secure certificates on the technology. The Table also draws attention to the current state of the different usage scenarios, explaining the method currently implemented in these areas and their shortcomings. For example, the verification system for the current formats of certificate issuance can be easily destroyed. Meanwhile, such certificates can be issued in digital format and the fingerprints recorded on the blockchain with the advantage of security and permanence of such records with no extra cost after issuance. The prerequisites specifically suggest the conditions that must be fulfilled to deploy the technology for each usage scenario. The Blockcert or similar application, for instance, must be used to manage blockchain-based certificates.

2.3 Theoretical Framework

As Li et al., (2019) rightly observe, researches of blockchain in education are merely emerging, devoid of mature use cases and theoretical backings. Thus, finding a comprehensive applicable study on blockchain-based verification systems is difficult. Nevertheless, a few early adopters that have implemented automatically verifiable, tamper-proof digital certificates are hereby examined. This is intended to provide insights into proven methodologies to further guide the recommendations for adoption in Nigerian institutions and institutions in other developing countries.

2.3.1 Adoption of Blockchain Technology for a Certificate Verification System

According to Grech & F. Camilleri (2017), a blockchain-based solution for certificates can be applied in two different manners that limit the amount of space it consumes. Depending on the purpose which the institution seeks to achieve, certificates can be recorded in plain text on the blockchain to make a database that is publicly available or store only the hash of certificates to protect the digital certificate issued to students. Typically, the process involves the certificate issuer (a university), certificate recipient (the student), and the verifier. The records are usually stored and accessed over a blockchain-based software such as the Blockcerts.

Blockcerts, the first remarkable instance of storing the hash of diplomas on blockchain, was developed by Learning Machine in conjunction with the MIT Media Lab. It is the only free, open-source standard for issuing and verifying certificates. Through its source code, institutions can develop their application for certificate issuance and verification. Recipients, on the other hand, can download the application on their iOS and Android devices to access a collection of their academic records. The application enjoys a wide adoption owing to its easy interoperability and avoidance of vendor lock-in. The wallet application is integrated into the software to encrypt students' data. Student shows ownership right on a certificate by generating a unique numerical code with which they share their verifiable, tamper-proof, virtual certificates with potential employers free of charge and with no involvement of an intermediary (Martin Garriga et al., 2018). On the other hand, third parties can confirm the genuineness of the certificate by entering the Uniform Resource Locator (URL) of the certificate into an MIT-hosted portal (Arenas & Fernandez, 2018).

Another notable blockchain-based platforms for certification systems include: Open Certificate – an Attore's certificate-issuing platform that enables an institution to issue a certificate directly on Ethereum blockchain through smart contract; Gradbase – specifically designed on Blockchain Bitcoin for the verification of academic records (Arenas & Fernandez, 2018); Stampery is based on the bitcoin blockchain and used for time-stamping and data verification (Sánchez De Pedro et al., 2016) OpenBlockChain, Open badges, BCDiploma and EduCTX (Gresch et al., 2019). With these software applications, the early adopters here presented can deploy the technology:

- **The Republic of Malta**

In the belief that blockchain can transform the education systems, Malta began to partner with Learning Machine Technologies since 2017 on a trial project that enables higher education and vocational students to access and retrieve educational records through the blockchain technology (Visram, 2018). Through its Ministry for Education and Employment, Malta is the first implementer of blockchain-based credentials using a Federated Issuing System. This system affords them with an analytical view of their progress in the educational sector. It also allows Maltese learners and workforce to have their records of lifetime learning in one storage, prove their ownership as well as share them with anyone from anywhere in the world for free. This saves employers time and money during verification, helps institutions curb fraud and save their brands from reputation damage (Learning machine, 2019). As of 2018, several institutions in Malta namely: the Institute for Tourism Studies (ITS); the National Commission for Further and Higher Education (NCFHE) (Grech & Camilleri, 2017); the Malta College for Arts, Sciences, and Technology (MCAST); and the Ministry for Education and Employment (MEDE) issued certificates to four secondary schools (CryptoNinjas, 2019).

- **University of Nicosia**

The University of Nicosia has the first experience in the world over for the adoption of blockchain for an academic certificate, issuing certificates that are instantly verifiable with the Bitcoin blockchain. Such certificates were first issued in 2015 to students upon their successful conclusion of the course "Introduction to Digital Currencies," the first university course on cryptocurrency. In 2017, the institution

launched a campus-wide Bitcoin blockchain-based certificate, which it had developed as an open-source and has been deployed by other institutions too. The British University in Dubai (BUiD), for instance, was the first in the country and third in the world to issue self-verifiable blockchain smart certificate through the technology of the University of Nicosia to the graduating set of 2017 (UNIC, n.d.)

- **Massachusetts Institute of Technology**

During 2017, MIT introduced digital diplomas to a special set of students cutting across the Undergraduate, Masters, and Ph.D. degree programs. Tamper-proof academic records stored on the bitcoin blockchain that can be shared peer-to-peer and easily verified were issued. Earlier on, in 2016, Learning Machine and MIT Media Lab were involved in an experimental project on Blockcerts; however, by 2018, the project was officially launched campus-wide. The MIT Registrar – Mary Callahan – had sought to provide student-owned records; once the development came to her knowledge, she seized the opportunity to fulfill her promises (Learning machine, 2019).

- **Central New Mexico Community College**

No other community college had issued secure digital diplomas to students except the Central New Mexico Community College. In December 2017, the college issued a digital certificate to the graduates of their Ingenuity programs through the Blockcerts mobile application. By the Summer term the same year, about 300 diplomas were issued to the Ingenuity students. Subsequently, the college proceeded to exploit the digital certificates in phases over all the various programs, and in August 2018, all students had the option to receive their certificates through the Blockcert application.

- **Ngee Ann Polytechnic (Singapore)**

In 2018, Ngee Ann Polytechnic - one of Singapore's tertiary polytechnic schools - in partnership with Government Technology Agency (GovTech) first began to test the use of OpenCerts for digital certificate issuance and verification. After the pilot program was successfully implemented with the first batch of recipient graduates, it became the catalyst for the entire education sector in the pursuance of a national project. Opencerts is one of Singapore's initiative to foster Smart Nation. The

SkillsFuture Singapore (SSG), Government Technology Agency (GovTech), Ngee Ann Polytechnic (NP), and the Ministry of Education (MOE) jointly manage its implementation. In September 2019, the minister of education announced adoption for all graduates, with eighteen institutions currently participating (Ngee Ann Polytechnic, 2019).

- **National Research and Education Network of Greece (GRNET)**

According to (Gresch et al., 2019), the National Research and Education Network of Greece stores the hashes of diplomas in a blockchain to secure the data of its students. It aims to establish a mechanism for verifying the diplomas of its students on Cardano blockchain to replace the manual process of verification and prevent the incidences of fake certificates. The GRNET project has a different approach from Blockcerts because it stores hashes of certificates and the verification system. The verification system consisting of the verification requests, the outcome of the request, and the feedback system for the requester are stored.

The high prevalence of certificate fraud and the heightened need to protect their brands have led several institutions to develop an interest in the blockchain technology for issuing student certificates. While this is not exhaustive, Table 3 here illustrates that several institutions in various countries have considered and are currently running a pilot project with blockchain for certificate verification. The Table indicates the presence of many other vendors besides Blockcerts and that for the most, the technology experiments on academic certification systems.

Institution	Country	Use	Service providers
Delhi University	India	Digital certificates	IndiaChain
Indian Institute of Technology	India	Digital certificates	IndiaChain
Pohang University of Science and Technology	South Korea	Digital certificates	ICONLOOP
Polytechnic University of Cartagena (UPCT)	Spain	Digital Certificates	UPCT & Decision Habitat
RMIT University	Australia	Microcredentials and online short coursed	Credly
San Antonio Catholic University	Spain	Digital certificates	UPCT & Decision Habitat

Institution	Country	Use	Service providers
Southern Alberta Institute of Technology (SAIT)	Canada	Digital certificates	On-Demand Education Marketplace (ODEM)
Southern New Hampshire University	USA	Certificates and Competencies	Learning machine
Synergy University	Russia	Students information and Certificates	Bitfury
Tec de Monterrey	Mexico	Academic records	Sony Global Education, IBM Blockchain
University of Bahrain	Bahrain	Digital certificates	Learning Machine
University of Basel	Switzerland	Digital certificates	Proxeus
University of Melbourne	Australia	Digital certificates	Blockcerts
University of Murcia	Spain	Digital certificates	UPCT and Decision Habitat
The University of St. Gallen	Switzerland	Digital certificates	Proxeus

Table 3:Blockchain pilot project for educational institutions, source: author

2.3.2 Impact of Blockchain on Certificate Verification Systems

The old method of certifying and verifying qualifications that were designed and used when a few privileged members of the society attended the university can no longer meet the needs of the present day. Blockchain technology offers unlimited potentials that could have an extensive relevance in education, as the subsequent paragraphs will highlight.

The blockchain technology is primarily characterized by decentralization. Through the adoption of a peer-to-peer distributed system in the stead of a central database, the single point of failure and bottlenecks of a centralized system can be prevented, thus greatly scaling down the error margin in the system.

Also, there is the benefit of reliability. Records in blockchain maintain immutability and can persist for an extended period. Thus, any party can confirm the authenticity of records and be sure of its integrity (Cristina Turcu, Cornel Turcu, 2019). Owing to the permanence of records on the blockchain, this ability to verify certificates holds even if the issuing institution no longer exists.

An equally significant benefit is improved system security and fraud prevention. The cryptographic protocols on the blockchain provide the possibility of a more secure certificate records when it has been added on the blockchain as a transaction. With the

cryptographic signatures, it is difficult for impersonation of records or to claim records from an institution where the certificate did not emanate (Ghazali & Saleh's 2016a).

In the same token, efficiency is another point to consider. Blockchain greatly improves time efficiency by eliminating any middleman for verification. While the waiting time before a verifier gets a response from an institution is reduced to zero, the institution also saves time and can re-harness manpower for a more productive task.

Additionally, issuing digital certificates on the blockchain provides an effective verification process. By purpose, verification is meant to authenticate the genuineness of a certificate. However, due to human negligence, a fake certificate may pass unnoticed. Also, it is cost-effective for both the institution and the verifier. It reduces the costs associated with a physical certificate format such as the maintenance cost for the repository, and the verification fees verifiers pay is eradicated.

Lastly, it turns over the ownership control of certificates to the recipients. Ownership means that holders can keep and share their digital certificates with whoever and whenever they wish. Owners can manage their credentials seamlessly in a wallet.

2.3.3 Insights Gained from Early Adopters

This section brings together lessons learned from reviewing the early adopters of blockchain technology for certificate verification. It summarizes the points to consider before integrating it into the traditional process with regards to initial scope, operation, existing relevant applications, and expertise.

Firstly, the Initial scope is an important factor. In the cases of early adopters that have been examined, starting with a pilot project is the common trend. Keeping the scope small will enhance a manageable start and allow the institution to test run with fewer resources. It will also give the human resources the time to practice in preparation for the possibility of a larger-scale adoption.

Secondly, operating in parallel with the old process can be beneficial. Piloting with a project suggests that the new system runs in tandem with the old system. While the new technology is being tested, the old system is still very important to provide data feeds for the prototype and to endure the maturity of the new system.

Thirdly, taking advantage of already existing relevant applications can be effective in keeping the cost of implementation low. Instead of building an application in-house from scratch, most of the early adopters found it appropriate to make use of an open-source standard. Blockcerts, for instance, is an open-source that allows an institution to exploit while maintaining complete ownership.

Lastly, institutions can leverage the expertise of blockchain specialists through partnership. This is crucial in getting the project right from the first attempt, saving institutions the stress of excessive errors.

2.4 Summary

The main parts of this chapter include the earlier studies and the theoretical framework for this study. We examined previous studies in the certification system, paper-based certificates and their limitations, non-blockchain digital certificates as well as verification systems and their shortcomings. Also, we reviewed the blockchain technology, its components, operations, types, and features. We establish the suitability of blockchain for certification systems and its potential uses in education. In the theoretical framework Section, we studied the early adopters of blockchain for verification systems, and there we observed the impacts of applying the blockchain technology to verification systems. Lastly, we gained insights from the early adopters for the adoption of blockchain technology in Nigeria.

3. Research Methodology

3.1 Introduction

From the beginning of the study, we made it clear that the problem of inefficiency, ineffectiveness, and inconvenience is observed in the current systems of verification of certificates and that this research seeks to explore the situation, understand it and recommend the adoption of blockchain technology in the systems. Having examined past documents on this subject and identified the knowledge gap that exists, we seek to close the gap by this research. This chapter is, therefore, designed to provide details regarding the modalities of this research.

3.2 Research Questions

The main objective of this study, from the on-set, was to explore the current systems and propose a model for the adoption of blockchain technology to enhance the certificate verification systems in Nigerian higher educational institutions and extension, other developing nations. The study so far reveals that there is a real need for an improvement in the systems of verifying academic certificates and that different educational institutions around the world are constantly finding new and better ways of sharing information about the authenticity of graduates' certificates. It shows the diverse ways that technologies have been deployed as well as the suitability of blockchain technology for this purpose. In connection with the central objective, this study proceeds to address the main research question:

How can Blockchain Technology Enhance the Certificate Verification Systems in Universities?

To provide a focus for the work and the structure for finding information, the researcher has broken the main question into manageable sub-research questions, denoted by SRQ subsequently.

SRQ1: How to establish the implications of blockchain technology on academic certificate verification systems?

SRQ2: How to determine the benchmarks for assessing the benefits of applying blockchain technology for certificate verification systems?

SRQ3: How does the application of blockchain technology for academic certificate verification affect the system stakeholders?

Each of these sub-questions will be further elaborated into more specific questions to allow us to obtain more direct information that addresses the subject.

SRQ1 is further expanded thus:

- What is the present condition of the certificate verification systems before the application of blockchain technology?
- What will be considered as an enhanced certificate verification system by applying the blockchain technology?
- What aspects of the system need to be enhanced by the application of blockchain technology?

These set of questions relating to sub-question 1 aims to promote a better understanding of the current situation, the aspect of the current system that should be enhanced as well as the features that indicate an enhanced system. By this exploration, we recognize the gap in the current system that the blockchain technology needs to fill.

SRQ2 are also broken down as follows:

- What are the principal indicators of effectiveness in the certificate verification process resulting from the application of blockchain technology?
- What are the indicators of efficiency in the certificate verification process?
- What can be considered as a convenient certificate verification system?

By these questions, we will discover how to evaluate the enhancement the application of blockchain technology would bring on the certificate verification systems.

Lastly, the SRQ3 is also divided into more comprehensive details:

- What are the roles of the primary stakeholders in the current system of certificate verification?
- What aspects of primary stakeholders will be enhanced by the application of blockchain technology?

These questions seek to highlight the advantages, if any, the application of blockchain technology would bring to stakeholders.

3.3 Case Study Design and Selection

In seeking to successfully achieve the objectives of an exploratory study such as this, Runeson et al. (2012) asserted that the case study design is most appropriate. They also reviewed the definitions of a case study, and the common understanding is that a case study investigates contemporary phenomena in their context. This highlight shows that this design fits well for the collection of data from a contemporary case. More so, the research question type also plays a major role in the selection of the design. Since this study employs exploratory research questions characterized by "how" and "what" for a contemporary subject such as the adoption of blockchain technology in certificate verification systems, the case study design is proper to use.

Case study, as Yin (2009) describes, is an empirical inquiry that studies a contemporary phenomenon thoroughly and without separating it from its real-life context. This study is appropriate when the phenomenon cannot be satisfactorily distinguished from its context. He further stressed that a case study is carried out with a desire for in-depth knowledge of a current issue. This sets the case study apart from every other type of design.

Yin (2009) further identified two variants of case study research to include the single and multiple-case studies while Gustafsson, (2017) elaborated on their differences. Gustafsson explained that a multi-case study should be considered when the purpose of the research is to understand the differences between cases and that multi-case study analyses data within each case and across the cases. A single case study, on the other hand, is suitable when the intension is to study a single thing or single group. Siggelkow, cited in Gustafsson (2017), claimed that a single case more richly describes a phenomenon. Besides, a single case allows a researcher more time for observation than a multi-case and thereby produce an extra and better theory.

This research is studying the subject of adopting blockchain technology for certificate verification systems with a focus on the Nigerian case. Considering the above explanation about when to use the case study design and the description of the case study types, this study, therefore, adopts the single case study design.

3.4 Data Collection Procedures

According to Kabir (2016), data collection is one of the most important and challenging phases of research. It is common for all research work in any field even though the technique may differ. The essence of any data collection is to obtain appropriate evidence that culminates into data analysis and subsequently resolve the problem under study. To this effect, he further noted that accuracy during data collection should be targeted during data collection.

Kabir (2016) noted that data collection involves the gathering and measuring of data on a subject following established guidelines that help a researcher to answer formulated research questions, test hypotheses, and assess results. The definition emphasized that the information that has been gathered should help to answer research questions. This implies that an effective data collection procedure should answer the research question.

For data collection, Verne et al. cited in Runeson (2012) suggested three principles, namely: the use of multiple sources of data; Creation of a case study database, and validation and maintenance of chain of evidence. These principles partly touch on triangulation, which is the "use of several data sources, and several types of data source, in order to limit the effects of one interpretation of one single data source. (Runeson et al., 2012) The triangulation of data supports the reliability and validity of a research outcome.

To ensure enough coverage of data sources, this research sources data from existing documents and interviews with relevant persons. Besides the method triangulation, the discussions implemented source triangulation by interviewing by obtaining different perspectives on the subject. This is explained further in the subsequent section.

3.4.1 Document Review

Document review **is** a thorough analysis of existing literature on a topic. Through the review of documents, a researcher becomes abreast of the knowledge gap on the topic, which then informs or justifies the need for a new inquiry. A researcher needs enough review of documents to be able to solid paper since previous research will establish the bases for such writing. Also, enough document review shows the readers that a writer has

enough knowledge of the discourse, which enhances a writer's integrity and credulity of the findings (Denney & Tewksbury, 2013).

According to Denney and Tewksbury (2013), review begins with a general view of the topic to a more specific focus on the research questions the writer is set to address. This is especially important for qualitative research. Hence, in this research, which seeks to address how the adoption of blockchain technology can enhance the certificate verification system, the literature review began by discussing the certification system with different certificate types, the blockchain technology and its components, workflow, features, and other subtopics. Then in the theoretical framework, we discussed examples of the adoption of blockchain for verification systems and the lessons learned.

Documents were gathered from scholarly articles and books, essays, trade journal articles, reports, national and international newspapers and magazines. Talking about document sources, finding proper pieces of literature to detail the Nigerian situation with regards to certificate verifications was particularly challenging, so, documents found on that sub-topic were few. Also, grey literature was consulted in cases where an academic journal that addresses the theme could not be found. The target dates of document inclusion documents were from the years 2010-2020. However, earlier documents were also used where later documents were not available.

3.4.2 Interviews

Interviews were also used as a method of data collection in this research. The interview has to do with contacting, seeking, and getting responses to research questions from certain participants. Interviews can be Structured, Semi-structured, or Unstructured. the semi-structured interview has an interview guide such as a list of questions and topics that should be covered in the interview. The questions often contain mostly open-ended questions and give room to variants in responses(Kabir, 2016).

This research used the semi-structured interview type to elicit responses from participants. The interview questions comprised mostly open-ended and few closed questions, allowing for the detailed expression of answers and any additional inputs. Measures were taken to foster the validity of responses.

Responses were sought from a total of sixteen (16) respondents from four different regions of Nigeria – the Middle Belt, South-eastern, Southwestern, and the South-south.

Also, two different perspectives were obtained in the interview – verification staff in Nigerian universities as well as company personnel who are involved with the verification of new staff certificates. Due to the geographical locations of the interviewer and the interviewees, interviews were conducted over the phone and recorded. The audio records were transcribed and added to the RQDA[1] software for analysis.

3.5 Analysis Procedures

According to Runeson et al. (2012), through data analysis, we understand exactly what happened in the case. The understanding of the case helps the researcher to draw patterns and conclusions from the data. Some important points Runeson et al. highlighted include that the researcher should present sufficient information concerning every step of the study and important decision taken, and the analysis process is a series of iterations and not a linear.

This research adopted the Clarke's and Braun's six (6) phases analysis procedures which include (Terry et al., 2017):

1. Familiarising with the data. This step involved transcribing from the audio record, which we highlighted in the previous section into text files, then the reading of the texts over and over for acquaintance.
2. Generating codes: the author labeled important parts of the text files through the RQDA software tool. Some segments of the data had multiple codes as necessary.
3. Constructing themes: the author examined the codes to identify relevant themes and did group them
4. Reviewing potential themes: the author again examined the potential themes against the codes and against the data set to ensure the correctness of theming.
5. Defining and naming themes. The review of the themes led to defining and naming from which the thematic plots emanated.
6. Producing the reports: the author selected the most relevant extracts for the report writing about the research question and the literature from that we see the conclusions.

[1] HUANG Ronggui (2016). RQDA: R-based Qualitative Data Analysis. R package version 0.2-8. http://rqda.r-forge.r-project.org/

3.6 Validity Procedures

Runeson et al. (2012) stated that validity implies the trustworthiness of the outcomes and to what extent the results are not distorted by the subjective views of the researcher and further noted that this criterion must be considered through all phases of the research. Shenton (2004) provided that the validity of a study can be checked against credibility, transferability, dependability (reliability), and confirmability.

3.6.1 Credibility

Shenton provided guidelines for achieving credibility. Some of the criteria he shared include:

- The study must achieve what it is actually intended for. To do so, it must follow well-established methods such as data collection and analysis methods.
- Triangulation involves various methods and sources of data collection. Shenton also suggested that the investigator may seek respondents from persons who deliver a service and from the service users.
- Iterative questioning during the interview to elicit a detailed response from participants is another technique he mentioned,
- Member checks during the interview and after transcription were also recommended to ensure the accuracy of the data.

This study adopted the necessary measures to achieve the conditions that have been described and is therefore credible.

3.6.2 Transferability

This refers to the extent to which the findings of the study can be applied to other situations. Though we are not sure whether the findings here can be transferred to a dissimilar case than the Nigerian context, but we have provided a sufficient description of the case under study to enable any other investigator to determine whether the findings can be transferred. However, in a similar context as Nigeria, this study satisfies the transferability criteria.

3.6.3 Reliability

Reliability requires that the researcher keeps a chain of evidence. The chain of evidence refers to presenting sufficient information about the study documents and procedures. The essence is for an alternative investigator to repeat the research and should get same results. Given that the trail of information has been provided, this study can be repeated.

3.6.4 Confirmability

Confirmability means that findings must reflect the ideas and experiences of respondents rather than the preferences of the researcher. Through all the phases in the research, we observed that the confirmability criteria were fulfilled. One of such criteria is triangulation which we discussed earlier. This research conforms with the conditions for confirmability.

3.7 Summary

This chapter elaborated on the approach adopted for this research. Detailing how the research questions were developed, it discussed the case study as a suitable design for the thesis. It went on to explain how the data for the research were gathered and how the data collected were analyzed with Clarke and Braun's six phases procedures. Lastly, we reviewed how the validity of the research is achieved.

4 Results

4.1 Introduction

This chapter of the study sets out in detail the case and subject selected as well as the data that were collected. It provides an in-depth understanding of the analysis of the interviews conducted using RQDA software. Further, in presenting the outcomes of the interviews, it submits a full explanation of the results.

4.2 Case and Subject Description

The verification of the certificates of Nigerian graduates is solely carried out by the registry division of issuing institutions through the exams and records unit. The registry division, headed by a Registrar, plays an essential role in collaborating with academic departments, other special units of an institution and external bodies to serve students, staff, and external bodies. The registry department is segmented into different units that include the academic affairs unit. The academic affairs unit, on the one hand, comprises the senate, admissions as well as the exams and records while the exams and records sub-unit, on the other hand, is responsible for coordinating the university exams and keeping of student records. Universities rely on this department for the credibility of the certificates that they issue and the verification of the same (Okebukola, 2017).

Nigerian university certification systems are predominantly paper-based and, by extension, the verification systems too. What this means is that certificates are issued and stored in paper format and retrieved manually. Even though the Nigerian Universities Commission Database (NUCDB) – a public-private partnership by Nigerian Universities Commission (NUC) and GUCCI-CHIS – was introduced in 2008 to enhance data availability and management in the universities and, to curb fake certificate incidences, it is still at the stage of providing basic functions such as capturing students biodata, course registration and management of students credit unit (Onwudebelu et al., 2013). The manual way of retrieving student information for verification results in inefficiency of time, ineffectiveness, and a cumbersome process.

The rigor associated with this process consequently deter several recruiters from verifying certificates, especially if they have numerous candidates from a wide range of institutions

all over the country. While they continue with a candidate in good faith, the certificates may not always be genuine. The failure to verify encourages fake certificates. Higher institutions, on the other hand, always verify certificates of students who seek to further studies. Thus, an efficient, effective, and convenient verification system is crucial to check fake certificates.

This study sought to understand the challenges in the current verification system fully, discover how the application of blockchain technology can improve the existing systems, examine the factors that can militate against the successful implementation of the technology and in the end develop a framework to guide the adoption of the technology for the verification of certificates. For this purpose, the researcher requested and collected the views of sixteen (16) interviewees through semi-structured interviews. The interviews were conducted with persons who have direct interactions with the current system from the Middle Belt, South-western, South-eastern, as well as the South-south regions of Nigeria to establish the validity of responses and wide coverage within the case. They include several assistant registrars, heads of IT support for Exams and Records unit, administrative officers of universities; the human resource managers and compliance officer of corporations; and a university degree holder-blockchain expert.

4.3 Presentation of Findings

This section explores and provides explanations for the outcomes of the data that have been gathered and analyzed from the interviews. The preceding chapter contains details about the interview technique; however, it is worth highlighting here that the interview questions comprised open-ended questions sectioned into seven (7) parts. The first section sought to know the respondents with regards to their background as a means of evaluating the reliability of their responses, and subsequent sections were designed to elicit responses that are consistent with the research questions. The audio records of the interviews were transcribed to texts as compatible with RQDA software. Following the transcription was the addition of the text files to RQDA software and the application of codes to the same. The encoding system reflects a blend of inductive and deductive procedures. In other words, codes generated predicated on the research questions as well as the issues that emerged from the data collection. Subsequently, the codes were categorized to set them into thematic areas, as shown below:

01_Understanding Current System

02_Aspects to improve

03_Enhanced Verification System

04_Hinderances to Blockchain

05_Tackling Problems to Blockchain

06_Evaluation Criteria

07_Blockchain Impacts on Stakeholders

4.3.1 General Description of the Respondents

This section is a brief review of the respondents selected to participate in the interviews. As mentioned already in section 4.2, the respondents selected for this research included persons who have direct interactions with the systems in their daily activities. The first section of the interviews was designed to obtain information about the positions they held and their roles.

The discussions that ensued revealed that the respondents have had years of experience in roles that afford them a significant level of engagement in the systems of verifications. For instance, the HR manager has had twelve (12) years of dealings with the verification of candidates' certificates. Also, the respondents from the universities have had at least two (2) years of experience in handling certificate verifications. It could thus be concluded that the respondents are well-informed and would make meaningful contributions to the study.

4.3.2 Establishing the Implication of Blockchain Technology

In part, the core objective of this study was to explore the current systems of verification and understand the underlying issues in order to identify how the blockchain technology can enhance the systems. In looking to achieve the objective, one of the sub-research questions is – how to establish the implications of blockchain technology on academic certificate verification systems? To further narrow out the research and obtain clearer information, the SRQ1 was broken further into: "what are the present circumstances in the certificate verification systems before the application of the blockchain technology?" "what will be considered as an enhanced certificate verification upon applying the blockchain technology?" and "what aspects of the system will be enhanced by the application of blockchain technology?". These sub-questions made up the interview

questions from which precisely defined answers were obtained, coded, and grouped into themes as earlier presented in Section 4.3. The themes, which are the results of the interviews, are therefore discussed in detail in the following paragraphs.

4.3.2.1 Understanding the Current System of Verifications

An understanding of the current system is essential to the introduction of any enhancements. Thus, it is necessary to address the question, "what is the present circumstances in the certificate verification systems before the application of the blockchain technology?". The earlier phases of this work reviewed the literature concerning the modalities in the current verification systems. This section checks the applicability of the same with the case of Nigeria through the results of the interviews.

Findings support that degree certificates in Nigerian universities are predominantly paper-based. Accordingly, a physical storeroom with file cabinets must be set up for the storage of all the paper certificates alongside some sort of digital storage. The digital storage is achieved differently in various institutions. They scan individual certificates and save the same electronically, while some simply register certain data items for each certificate into the system. For the retrieval of certificates during a request for verification, respondents explained that an officer of the exams and records unit must go to the file cabinets in the storeroom and search for the requested certificate amongst a pile of other certificates. One respondent emphasized that despite the electronic storage, they still refer to the cabinets for certainty.

Additional significant points from responses were the form of application, line of communication, and data sharing in the current system. To verify, the verifier either visits in person/by proxy; or through a third-party organization (who charges a fee)*;* or by an email with ample waiting time for feedback. The email application follows a line of communication that begins from the registrar to the head of the unit records officer, and then the officer and back to the registrar. For the verifier that contacts through an email, the feedback entails scanning a copy of the certificate and emailing back to the entity; or by post through a courier service, especially between institutions. The application of technology in the current systems is at its lowest level. The standard form of ICT facilities deployed include emails, a server, a primary database, and internet services. Among the interviewed universities, there was only one instance of the e-verification system (through a client/server network). Even though the manual process is a major problem, respondents

also pointed out that the manual processes result in the following problems that further weaken the systems: a. Apathetic verification officers, b. Low staff motivation c. Non-Conducive Environment, d. Work overload

4.3.2.2 Aspects of Current System to be Enhanced

Manual procedures: as explained above, all the manual processes of storing certificates, applying for verification, retrieving certificates, and sharing the feedback need to be enhanced. Many participants submitted that these procedures are the major reasons for delayed delivery. For instance, a respondent who is a recruiter submitted that one of the problems in the current system is the line of communication in the verification process and that most institutions fail to reply to a verification request. The manual procedure is characterized by: a. delayed response b. delayed delivery and c. clients' dissatisfaction.

High Cost: the evidence gathered also posits that the current system is expensive to the university and verifiers. The three recruiter participants stressed how they spend enormously to verify each certificate in the current system. One of the respondents shared that verifying four certificates from one of the universities costs about One Hundred and Twenty USD and that the high cost precludes start-ups from verifying certificates. One of them explained that due to the stress and time wastage involved, her company outsources verification and pays as high as 30% of the new hire's annual salary as a service charge. Meanwhile, the university spends so much stationeries and other administrative expenses.

Cumbersomeness: each respondent described the process of verifications as inconveniencing. It is typically tedious for the university staff during certificate retrieval and involves long protocols and waiting time for the verifier. A respondent even mentioned the health hazards this process poses by inhaling the dust that accumulates on the files over time.

Inefficiency: the majority of the interviewees declared that inefficiency is an overarching issue in the current system. Some respondents used the word as an all-inclusive term for all the shortcomings within the system, highlighting various issues. One of the respondents pointed out that an inefficient verification system takes too long to act on and respond to a verification request, and a recruiter added that the manual process does not

allow them to conclude a recruitment process within their target time since they must await a response from the university.

4.3.2.3 Enhanced Certificate Verification Systems

While we already discussed aspects to be enhanced, here we are going to understand from responses what an optimum verification system entails, to determine what gap blockchain will fill.

Accurate information: respondents believe that the verification system should effectively tell apart a genuine certificate from a fake one and should also be void of error during verification since this can be detrimental to concerned parties. From the recruiter's perspective, it should help them make the correct decision to avoid high labor turnover.

Put control on certificate forgery: from a recruiter's perspective is that a proper verification system should deter candidates from parading fake results.

Convenient: most of the respondents stated that the verification should be stress-free and allow them to achieve verification with minimal efforts such as a few mouse clicks and void of all the current protocols.

Cost-effective: from findings, the verification staff thinks the system should save them the cost of printing certificates and other administrative expenses. At the same time, the verifiers believe that the system should save them the cost of traveling to the institution and service charge they pay to intermediary firms, among others.

Easy retrieval of certificate: respondents highlighted that an enhanced system should shorten the time it takes to retrieve information about a certificate.

Persistent: certain respondents commented about the continuity of certificate information in an enhanced system. A university staff observed that if their electronic storage device got damaged, they should still have their information intact in an improved system.

Reliable: some respondents stated that an enhanced system is free from certificate mutation and system hack.

Time-efficient: Most respondents indicated that this would be a significant benefit of an enhanced system as a specific respondent asserted that verification should be achieved *within* 24 hours maximum.

Transparent: While a university staff explained that no officer would claim sole right over the flow of information using passwords in the enhanced system, a recruiter believed that they would be able to access the information about candidates' certificate more readily. No candidate will be able to claim qualifications they do not possess.

Value for money: a respondent who is an HR personnel opined that even if they paid for verification in an enhanced system, he would be happy to do so when he can get the value for the money.

4.3.2.4 Hindrances to Blockchain Adoption

Respondents identified the following issues as potential problems to the successful adoption of blockchain:

Poor ICT facilities: a recurrent theme among respondents was the lack of or inadequate ICT facilities and how it affects the efficiency of the verification systems. The interview results revealed the lack of adequate ICT facilities such as the internet connection and resources; and the use of obsolete technologies. They indicated that poor internet connectivity constantly interferes with their job, regularly bringing their responsibilities to a halt abruptly.

Poor digital skills: In the same vein, some respondents do not think that there are enough digital skills to manage any technological updates in the system. While a few respondents affirmed that they are highly skilled in the use of ICT technologies, most of the respondents from the exams and records unit possess average to necessary digital skills. They communicated expertise only in basic skills such as the use of word processor, email, and file attachment.

Inadequate funding: In the results, respondents highlighted that any advancements in the system for better service are contingent on the availability of funds. A respondent explained that IT advancement requires a considerable capital "to get a good one working" and that most times when the server or Wi-Fi is down, and nobody cares, it demoralizes him. Much like a general challenge in the university system, another

respondent labels inadequate funding as a significant problem to the service delivery in the verification systems.

Inadequate electric power supply: Interview results showed that the power supply continues to be an issue of high priority in Nigeria due to the irregular supply. According to respondents, while the universities try to provide electricity through generating sets, this only increases the administrative cost. A respondent asserted that the situation often ground activities of the unit when they need to scan, type, and email feedbacks to verifiers. Then they stated that the frequent seizures of power supply might hinder the successful adoption of blockchain technology.

The burden of digitizing certificates: The difficulty of "converting the previously documented records that are in the analog forms to digital form" was a cause for concern to several respondents. They pointed out that records date back to the 1980s. To achieve this feat, certain respondents believed investment in appropriate equipment would be necessary.

Ignorance of blockchain: Results from the interviews confirmed a profound lack of awareness about the technology. A respondent called attention to the possibility of graduates not appreciating a digital certificate issued on blockchain because they need to have a physical certificate that can be seen by their aged and illiterate parents.

Resistance to change: Though viewed from different angles, an extensive analysis of the results indicate that many respondents consider this phenomenon to be a severe threat to the adoption of the blockchain. This can play out in the way the custodians of the system may oppose any modifications to what they are used to. Some of the identifiable reasons from the findings include: the unwillingness to give up control and access to information; fear of displacement if they become redundant; another respondent mentioned technophobia, that is, fear of how the technology might cause changes; and then corruption and bureaucracy because some top management staff makes money from the current system was another factor.

4.3.2.5 Remedy to the Problems to Blockchain Technology Adoption

Blockchain propaganda: as a remedy to the problem of ignorance, some respondents suggested a sustained effort to educate individuals, boost the awareness of university policymakers and systems custodians, and the wider network of stakeholders. For the

policymakers, a respondent stated that the objective of the campaign would be to get them to buy into the idea.

Digitize certificates: Admitting that it will take extra efforts, respondents thought that digitizing the old records would facilitate the adoption of blockchain and allow the full benefit of the technology for verification.

Generate funds internally: As various respondents acknowledged that the government could not provide everything, applying ingenuity to solving the problems of the poor funding is another remedy the data collection highlighted. A respondent outlined the different avenues to achieve this. First, he said students would not mind taking ownership of their certificates and may be willing to pay a token through the purchase of a scratch card to access the certificate. Secondly, scholarship boards seeking to verify a students' performance profiles could pay for the university scratch card for this. Lastly, he mentioned that the university could also harness the support of the alumni who can offer substantial assistance if there is a genuine commitment to optimize the system through technology.

Human resource training and upskilling: several responses during the interview stressed the importance of training the staff in preparation for the technology. Also, a critical analysis of the findings in this regard suggests that upgrading the skills of staff for more productive roles will solve the fear of displacement.

Cheaper licenses to ISPs: Almost all the participants stressed the need to upgrade the internet connectivity. However, a respondent draws attention to the main problem, which he said is the high cost of licenses to ISPs and that if the relevant authority reduces such cost, ISPs will provide better and affordable services.

Provision of electric power supply: the issue of power supply received special attention from all participants, and some of them suggested the use of various means such as solar panel and power generating set to enhance the power supply if blockchain must thrive.

Section overview

The findings on the implication of blockchain technology buttress the points we highlighted earlier in chapter 2. In Section 2.1.4 of the literature review, we observed that the verification systems inherit the problems of the certification systems. For

instance, if the certificate is paper-based, there must be physical storage, a manual retrieval as well as issues relating to the sharing of the verification outcome.

Also, in Section 2.3.2, we examined the impacts of blockchain technology on certificate verification systems. Such include reliability through the immutability of the system, scaling down the error margin in the system, time efficiency since the waiting time for a response from the institution would be zero, productivity, effectiveness by accurately detecting any fake certificate as well as cost-effectiveness. Again, the interview responses validated these points.

Further, the insights gained from early adopters in Section 2.3.3, would be able to address some of the potential hindrances to the blockchain that have been highlighted. For instance, on a small scale, a pilot project could run alongside the current system for a period.

We have thus explored the current systems of verification, its gaps, and how the blockchain technology can enhance the same. We will, therefore, go on to the next section to examine the benchmarks for evaluating the verification system after the technology has been adopted.

4.3.3 Measuring the Effects of Blockchain

As the previous section indicated how the adoption of blockchain technology would enhance the current system, the basis for measuring its significance becomes essential to this study. The findings here are gleaned from the responses to the questions: “what are the principal indicators of effectiveness in the certificate verification process?” “what are the indicators of efficiency in certificate verification process?” and “what can be considered as a convenient certificate verification process?” which were derivatives of the research question: How to determine the benchmarks for assessing the benefits of applying blockchain technology for certificate verification process?

4.3.3.1 Evaluation Criteria

Inputs were sought from respondents through interviews regarding how to measure efficiency, effectiveness, and convenience in the systems of verification. When asked how to evaluate the systems, some respondents said they did not have well-established indicators for evaluation in their units. However, every participant had an idea about how the verification system should be assessed.

Effectiveness

- **Accuracy**: Respondents noted how closely the facts about a certificate match the report from the verification of a certificate is a highly sensitive element in the system. According to the responses, the key reasons why accuracy is important is that every verification exercise puts the image of the institution at stake; informs the decision of verifiers as well as affects the certificate holder severely if the wrong report is issued. If a system is effective, then it should be accurate. Similarly, recruiters want to be able to make accurate decisions about their hires to reduce labor turnover and all the costs that go with that
- **Reliability:** as deduced from responses, reliability is closely related to accuracy and refers to the capability of a verification outcome to represent the facts about a certificate. While inaccuracy is a product of unintentional errors, unreliability stems from the intentions to misrepresent the truth. Reliability can, therefore, be a yardstick for measuring the effectiveness of evaluation. A respondent explained how this could play out:

" What I can do is to pally up with whosoever is in my school or whosoever is in that school because of the level of corruption here, and say, "I have sent the following certificate to so and so institution if they call, please get me someone that can answer the call and tell them the verification is true and that's all."

- **Lesser cost:** A respondent clearly described that an effective system means to spend less for verifications.

Efficiency

- **Lesser verification time**: Several respondents described the basis for assessing efficiency as how quickly they can carry out their responsibilities. A few others relate it to meeting timeframes stipulated by the institutions.
- **Feedback:** Again, many respondents believed that the quality of service could be judged from the feedbacks of users. They added that by their complaints or recommendations, how well a system is doing can be measured.
- **The volume of verifications**: For the evaluation of efficiency, three respondents expressed the view that the turnover of verifications performed at a given time is a yardstick. One of them said they often have a high volume of verifications and that every quarter; they check how much was completed. Another person said they register every verification, and that would give them the figure if necessary.

- **Quality assurance**: One respondent mentioned that quality assurance might be necessary to measure the system where a database application is in use. He explained that this would be able to test the resilience and security of the systems.

Convenience

- **Stress-free verification process:** respondents consistently spoke about ease in contrast to the tediousness of the current system. The recruiters, for example, seek an easy way to verify certificates with minimum distractions from their core duties. A respondent who currently visits the institution by proxy during verification desires that "a click of a button should "get it done right inside the office rather than wasting days. It could, therefore, be inferred that a smooth, seamless process defines a convenient system.
- **Easy retrieval of certificates.**

4.3.4 Impacts of Blockchain Technology on Stakeholders

The current section provides answers to the research question, "How does the application of blockchain technology for academic certificate verification affect the key stakeholders of the system?". The question was intended to explore the potentials of blockchain technology to impact the stakeholders of the verification system positively. For this purpose, the question was further broken into the following: "Would you consider yourself as a stakeholder in the verification system?" "How do you think the use of blockchain technology will impact your duties?"

During the introductory discussions and from the responses to the question "Would you consider yourself as a stakeholder in the verification system?" we established the roles of each participant which comprised twelve (12) exams and records staff who authenticate certificates, three (3) HRs/representatives who request verification, and one (1) blockchain expert who has also had direct interaction with the current verification system. Below is how blockchain technology would impact the key stakeholders:

Assurance: A recruiter noted that graduates whose certificates could not be verified within the probation period due to the sluggishness of the existing systems had their contract terminated even though it does not always mean that the new hire's certificate is fake. It can be inferred from here that when blockchain turns over the ownership control of certificates to the graduates, this will be assured to the graduates.

Better decision: for the recruiters, they believe the integration of blockchain into the verification systems would enhance their candidate selection.

Increased productivity: most of the resource persons thought that if they are relieved of some of their activities after blockchain is used to automate the verification processes, they would have time to face weightier matters in the scheme of operations.

Working remotely: some participants expressed the possibility of working remotely once blockchain is adopted for their work.

Reduce contact with clients: the existing system works better with in-person visitation to the institution. A respondent did indicate that some verifiers can be extremely difficult and that the technology would reduce the need for contact with verifiers.

Overall, all respondents showed enthusiasm and interest in the research as they made valuable contributions to answering the research questions. The perspectives on the issues reflected that respondents have detailed knowledge of the subject and the willingness to share their views constructively. This chapter and the entire research would be vacuous without their insights.

4.4 Summary

The chapter started by describing the case and subject under study. Next, it provided a detailed description of the interviewees to demonstrate the validity of their contributions and afterward was the presentation of findings from the interviews. Table 4 presents a summary of the findings based on each sub-research questions. The SRQs were further broken down into simpler questions. The simplified questions further formed the interview questions from which answers were obtained.

Research questions	Findings from interviews
SRQ1: how to establish the implications of blockchain technology on academic Certificate verification systems?	
What is the present condition of the certificate verification systems before the Application of blockchain technology?	• Paper-based certificates with physical storeroom and file cabinets • Certificates are retrieved from piles of files. • Application for verification is in person, by proxy, email or a third-party firm • The long line of communication from registrar to an officer • Information is shared in person, email, or courier. • Minimal use of ICT
What will be considered as an enhanced certificate verification system by Are you applying the blockchain technology?	• Has high accuracy • Puts control on fake certificates • Convenient • Cost-effective • Easy retrieval of certificate • Persistent • Reliable • Time-efficient • Transparent • Gives value for money
What aspects of the system need to be enhanced by the application of blockchain technology	• The manual procedures characterized by delayed response delayed delivery and client's dissatisfaction • High cost: administrative expenses to universities and of verification charge to verifiers. • Cumbersomeness • Inefficiency
Blockchain technology adoption	**Hindrances** • Poor ICT facilities • Lack of digital skills • Poor funding • Poor electric power supply • The burden of digitizing certificates • Ignorance of Blockchain • Resistance to change caused by fear of displacement, technophobia, seeking control, and corruption. **Remedy to hindrances** • Blockchain propaganda • Digitize certificates • Generate funds internally • Human resource training and upskilling • Cheaper licenses to ISPs • Provision of electric power supply

SRQ2: How to determine the benchmarks for assessing the benefits of applying blockchain Technology for certificate verification systems?	
What are the major indicators of effectiveness in the certificate verification Systems?	• Accuracy • Reliability • Lower cost
What are the major indicators of efficiency in the certificate verification systems?	• Lesser verification time • Feedbacks • Volume of verification • Quality assurance of the system
What can be considered as a convenient certificate verification system?	• Easy retrieval of certificates • Stress-free verification process
SRQ3: How does the application of blockchain technology for an educational certificate verification system affect the stakeholders of the system?	
What are the roles of the primary stakeholders in the current system of certificate verification	• Graduates are the certificate holders and the subject of verifications • Recruiters or representatives are verifiers • Issuing institution verification staff examine the authenticity of certificates
What aspects of primary stakeholders will be enhanced by the application of Blockchain technology?	• Assurance to graduate new hires • Recruiters: better decision and increased productivity • Verification staff: Increased productivity, the possibility of working remotely, reduce contacts with clients

Table 4: Summary of findings, source: author.

5 Conclusions and Future Work

5.1 introduction

This chapter brings us to the outcome of the study. Having gathered a broad knowledge from reviewing relevant documents and conducted interviews with participants on the research questions, we will proceed to consolidate the findings and provide guidance. More so, the chapter addresses the implication of the results, limitations of the study, and possible areas for future research.

5.2 Summary of Findings and Recommendations

The essence of this study was to acquire a full understanding of the existing verification systems in Nigerian universities and the issues that undermine efficiency, effectiveness, and convenience. The objectives of the study are the bases on which the researcher developed the research questions. The research questions, in turn, determined the approach for the exploration, as we conducted interviews to obtain answers. We observed from findings that the paper-based certificate means that the verification systems are mostly manual and that the issues currently undermining the systems stem primarily from the manual procedures of certificate storage and retrieval, line of communications, means of sharing information among institutions, and verifiers. The processes overwhelm and culminate in work overload for the verification staff.

Results also indicated that such issues would jeopardize attempts for any improvements in the systems as a lack of digital skills, poor ICT infrastructures, inadequate electric power supply, insufficient funding, and resistance to change. Respondents clearly stated that staff resists change for reasons ranging from the fear of technology, the fear of redundancy and job loss, unwillingness to give up control, and for the profits they make from the current system.

The Blockchain technology, characterized by decentralization and immutability, offers an efficient and convenient system for verifying certificates stored therein. However, for its successful adoption, specific measures need to take effect. Therefore, we consider the following guidelines for the adoption of blockchain technology for verification systems in Nigerian universities.

5.2.1 Establish the Interconnectivity of Universities' Databases

Whereas the adoption of blockchain technology in any sector requires interoperability of record systems, universities in Nigeria maintain students' database in silos. The Republic of Malta, for instance, uses a Federated Issuing System, which allows them to have an overview of their progress per time. The databases of different departments within a university should be linked up internally. Then the databases of various institutions should also be interoperated such that a single query can access multiple databases. National Youth Service Corps (NYSC) will also benefit from this upgrade during the mobilization of graduates for service. NUC, overseeing and regulating all universities, already established NUCDB in 2008, and the system only takes the biodata of students in individual institutions. NUC should review the workability of the NUCDB, ensure that the databases of various universities interoperate, and take appropriate measures to enforce it effectively. This would involve blockchain experts, universities, and NUC.

5.2.2 Establish a Common Standard for Certificates

Every university in Nigeria currently includes disparate features and information set on student certificates. However, it will significantly enhance the interoperability of databases if universities agree on a standard for the information contained in the on-chain certificates all over. The uniformity of standards would impact on such elements as the student identifiers and security features and provide uniformity. Hence, the standards should be clearly defined through adequate deliberations among relevant bodies and stakeholders of the systems. This will require deliberations among the university managements, NUC, technical experts, and certification professionals.

5.2.3 Enact a Consultative Council

Decision-makers must be exposed to different perspectives on the adoption of the technology for the successful implementation. The author, therefore, recommends that a consultative council should be set up and should be made up of blockchain experts and professionals in diverse fields as well as the end-users who understand the old system. Decision-makers should be able to make an informed decision based on their knowledge of the benefits, the risks, and the possible ways to mitigate the risks from adopting the technology.

5.2.4 Leverage on Collaborations

In all the examples of adoption we examined, there were some forms of collaboration with relevant bodies. Collaboration is the mutual support participatory organizations provide each other to achieve a common goal. It is characterized by the partnership. Initiators need to define participation criteria. There could be different levels of involvement. However, the author would recommend the involvement of a wide range of participants, including NUC, the university managements, blockchain experts, system users, developers, major service providers such as the ISPs, and the university trade unions as they often wield tremendous power over the affairs of the university. The involvement of blockchain technological experts is very vital. The expertise and experiences in a collaborative relationship can form a solid start for the implementation. The channel of communications and connections this creates would address the problem of resistance as trust is built. This collaboration will also be necessary to determine whether there are needs for new regulatory frameworks to sustain the project.

5.2.5 Run a Pilot Project

We observed from the early adopters that they began with a pilot project before embarking on a campus-wide implementation. One of the reasons to start with a pilot project would be to understand the workings of the technology with as manageable risks as possible. Also, it will provide significant stakeholders with hands-on experience with the technology and a chance to get useful feedback about any changes that may be required. If there were any cases of failure, the institutions would fail small and quick enough to make amends. The performance benchmarks we obtained during the interviews can be applied as well to test the project. This will require expertise, funds, and necessary infrastructures, and would involve all stakeholders and the experts.

5.2.6 Establish Diversified Income Sources

Participants raised concerns about the increasing financial needs of the universities with no corresponding increase in subventions. Meanwhile, the provision of infrastructures and other requirements for further development hinges on the availability of funds. Bearing this in mind, universities need to come up with the finances to sponsor their comparative strengths. For instance, unique annual events with staff, students, sponsors, and alumni would create an avenue to harness the power of social capital and promote community building. After that, they could develop a brand to enhance the loyalty and

support of fans for their projects. Also, the university can present individual projects to sponsors according to the interests of the sponsors or offer them various ways to give and then make sure to be accountable.

5.2.7 Upskilling and Staff Retraining Strategies

Staff kick against new technology because, as they rightly fear, it may result in their displacement. Staff care about and want to keep their means of livelihood. This paper recommends that the universities should make concrete plans for training and skill upgrade and then redeploy. Instead of retrenching the previous staff and employing skilled hands, the universities should develop feasible and effective upskilling and retraining strategies. A culture of encouraging and teaching new skills to employees before and parallel to implementing new technologies and redeploying them into new career paths instead of redundancy would reduce resistance to change. Some strategies could include micro-learning platforms, mentorship, and ample opportunity to apply new skills.

5.2.8 Review the Regulatory Policies for ISPs

The current regulatory policies for ISPs do not promote affordability and good quality internet. The high cost of internet service and poor internet penetration is traced to the ISP regulatory policies in operation. It is in the jurisdiction of the Nigerian Communication Commission (NCC) to review the existing policies and ensure that affordable and quality internet access all over Universities in Nigeria is prioritized and considered as an essential service. Some ISPs have exited the Nigerian IT sector due to the high cost of license renewal. With the cost of operating in the industry, ISPs are not motivated to invest in infrastructure to improve the quality of service. The action of NCC in this regard will foster the adoption of blockchain technology in the universities, by extension, address the problem of inefficiency. This study recommends for the review of the policy and that the federal government needs to intervene if necessary.

The table below summarizes the recommendations, the parties involved, and the requirements. In the table, the recommendations are described vividly, the concerned parties to and the necessary conditions for each recommendation are also stated.

Framework for Blockchain-Based Verification Systems in Nigerian Universities			
Recommendations	**Description**	**Parties**	**Requirements**
Interconnectivity of Universities' Systems	the interconnectivity of university databases such that a single query can access multiple databases.	NUC, universities, experts, NYSC	Interconnection of databases of departments and all universities.
Establish a Common Standard for Certificates	universities agree on a standard for the information contained in the on-chain certificates all over.	NUC, expert universities, certification professionals.	Deliberations
Consultative Council	Expose decision-makers to different perspectives on the subject.	Experts, professional, end-users, decision-makers	Discuss extensively on all aspects of the technology, periodic meeting.
Leverage on Collaborations	. Collaboration is the mutual support participatory organizations provide each other to achieve a common goal.	NUC, universities, ISPs, Experts, system users, university trade unions	Different channels of communication
Run a Pilot Project	Start implementation on a small scale to understand the workings of the technology.	Experts and all stakeholders	Funds, expertise, Infrastructures
Establish Diversified Income Sources	Universities need to come up with the finances to sponsor their comparative strengths.	Universities, alumni, sponsors, students, the wider society	Annual events for all stakeholders create a brand, present sponsors with projects
Upskilling and Staff Retraining Strategies	Instead of retrenching and employing new hands, the universities should develop feasible and effective upskilling and retraining strategies	Universities staff, Expert trainers	Micro-learning platforms, mentorship, opportunity to apply.
Regulatory Policies for ISPs	Review the existing policies to ensure affordable and quality internet access in all universities is prioritized.	Government, NCC, ISPs	Cheaper licenses for ISPs, lower operational costs

Table 5: Summary of the recommendations, source: author

5.3 Impact/Implication of Study

This study thoroughly examined the existing certificate verification systems in Nigerian universities with the intent of discovering the problems. Next, we explored the use of blockchain technology in tackling the issues and then developed the guidelines for the adoption of the technology in the case of Nigeria. The study equally described the features of optimum verification and highlighted specific areas in which enhancement through the application of the technology is required. In the context of Nigeria, this study explains a new means of accomplishing effectiveness, efficiency, and convenience in the verification of certificates.

While the cases of certificate forgery become widespread and seek for a permanent answer, this research presents the guidelines for bringing about the most needed change in the systems.

5.4 Limitations

Even though this research was committed to following the recommended rigorous methodological path, it is not exempted from the failings associated with this research design. There are often doubts about the process of analyzing qualitative data since it is based on the researcher's judgement and understanding, unlike the set of rules and formulas used in quantitative data analysis (Patton, 1999). There is the possibility of distorted views on the data during analysis with its influences on the conclusions.

There are several contrasting views about the transferability of findings and conclusions from a qualitative study. The positivists are concerned about the inability to apply the results of qualitative research to a broader population. However, Stake and Denscombe in Shenton (2004) argued that the possibility of transfer should not be dismissed entirely. Another group of researchers believes that it is left for the reader to decide the transferability of the study and that an author should provide sufficient contextual information. Hence, this study has provided enough contextual information but cannot infer that the findings can be transferred.

Due to the geographical location of the author at the time of carrying out the research, physical presence at the participants' universities was not possible. Resorting to emails, she wrote to about thirty (30) Universities in Nigeria who hardly replied except for four (4) of them. The researcher had to employ personal contacts to establish contacts with eight (8) respondents from various universities. Also, only three (3) verifiers could be contacted for a different perspective, even though more were sought. This was because most employers that were contacted said they do not verify certificates. Lastly, one verifier and blockchain expert was found. Thus, getting respondents for the interview was extremely challenging.

5.5 Future Research

Further studies to understand the implications of adopting blockchain technology will be necessary to enhance implementation. The universities need to know how the adoption of blockchain would impact their privacy, database rights, and other confidential information. This knowledge would be necessary to identify what guidelines and policies need to be enforced to prevent violation of privacy.

The study focused on the Nigerian context; as such, the findings here may not be transferable. There is the possibility that similar research on other developing countries would yield different outcomes. For transferability, further study in more cases will be appropriate and is encouraged. Also, this study may be repeated, with the help of the evidence provided to check its validity.

This study fulfilled the objective of establishing a framework for the adoption of blockchain technology for certificate verification systems but does not address the technicalities of implementation. To facilitate the creation and implementation of the solution, we suggest a different research design. While adoption resolves how universities can accept and integrate the technology into their processes and subsequently provide more efficient, effective, and seamless services, research for actual implementation would address how to install and configure the technology as well as training staff on the operations to enable productivity.

Seeing that new policies will be necessary to drive the successful implementation of the technology and to reduce resistance to new technologies in the future, we will suggest a study on how to enforce policies in the universities consistently. Such research can explore the causes of a low level of policy compliance and how to improve the same in universities.

References

ACTE. (2018). What Is A Credential? *The Association for Career and Technical Education*, 2. www.acteonline.org.

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

Arenas, R., & Fernandez, P. (2018). CredenceLedger: A Permissioned Blockchain for Verifiable Academic Credentials. *2018 IEEE International Conference on Engineering, Technology, and Innovation, ICE/ITMC 2018 - Proceedings*. https://doi.org/10.1109/ICE.2018.8436324

Attewell, P., & Domina, T. (2011). Educational imposters and fake degrees. *Research in Social Stratification and Mobility*, *29*(1), 57–69. https://doi.org/10.1016/j.rssm.2010.12.004

Balsubramanian, S., Prashanth Iye, R., & Ravishankar, S. (2009). Mark sheet verification. *2009 3rd International Conference on Anti-Counterfeiting, Security, and Identification in Communication, ASID 2009*, 4. https://doi.org/10.1109/ICASID.2009.5276942

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

Bond, F., & Blousson, G. (2015). *Blockchain, academic verification use case*. https://s3.amazonaws.com/signatura-usercontent/blockchain_academic_verification_use_case.pdf

Bowes, P. (2018). *Curbing university degree and certificate forgery with cutting edge*. pitneybowes.com/in

Brdesee, H. S. (2019). An Online Verification System of Students and Graduates Documents and Certificates : *International Journal of Smart Education and Urban Society*, *10*(2), 1–

18. https://doi.org/10.4018/IJSEUS.2019040101

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.

Christopher Odetunde. (2008, July 18). THE STATE OF HIGHER EDUCATION IN NIGERIA. *Niger Delta Congress*, 1–5. http://www.nigerdeltacongress.com/sarticles/state_of_higher_education_in_nig.htm

Cristina Turcu, Cornel Turcu, I. C. (2019). Blockchain and its Potential in Education. *International Conference on Virtual Learning*, *1*(1), 8.

CryptoNinjas. (2019, February 25). *Malta rolls out Blockcerts blockchain credentials in education/employment » CryptoNinjas*. CryptoNinjas.Net. https://www.cryptoninjas.net/2019/02/25/malta-rolls-out-blockcerts-blockchain-credentials-for-education-and-employment/

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

du Plessis, L., Vermeulen, N., van der Walt, J., & Maekela, L. (2015). *Verification of Qualifications in Africa* (Issue January). http://www.saqa.org.za/docs/genpubs/2015/Verification of Qualifications in Africa.pdf

Eckstein, M. A. (2003). *Combating academic fraud : towards a culture of integrity*. International Institute for Educational Planning.

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

Fernández-Caramés, T. M., & Fraga-Lamas, P. (2018). A Review on the Use of Blockchain for the Internet of Things. In *IEEE Access* (Vol. 6, pp. 32979–33001). Institute of Electrical and Electronics Engineers Inc. https://doi.org/10.1109/ACCESS.2018.2842685

GARWE, E. C. (2015). Qualification, Award and Recognition Fraud in Higher Education in Zimbabwe. *Journal of Studies in Education*, *5*(2), 119. https://doi.org/10.5296/jse.v5i2.7456

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

Ghazali, O., & Saleh, O. S. (2016a). A Graduation Certificate Verification Model via Utilization of the Blockchain Technology. *Journal of Telecommunication, Electronic and Computer Engineering*, *10*(3), 6.

Ghazali, O., & Saleh, O. S. (2016b). *Cloud Based Graduation Certificate Verification Model*. *December*, 978–993.

Grech, A., & Camilleri, A. F. (2017). *Blockchain in Education* (Issue June). https://doi.org/10.2760/60649

Greg Walker. (2015, February 26). *What's inside a Block on the Blockchain?* https://learnmeabitcoin.com/beginners/blocks

Gresch, J., Rodrigues, B., Scheid, E., Kanhere, S. S., & Stiller, B. (2019). The proposal of a blockchain-based architecture for transparent certificate handling. *Lecture Notes in Business Information Processing*, *339*, 185–196. https://doi.org/10.1007/978-3-030-04849-5_16

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

Hall, M. (2017). THE BLOCKCHAIN AND THE FUTURE OF CREDENTIALING. *Research Hub*, 18.

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

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

Learning machine. (2019). *Verifiable Digital Records*.

Li, C., Guo, J., Zhang, G., Wang, Y., Sun, Y., & Bie, R. (2019). A blockchain system for E-learning assessment and certification. *Proceedings - 2019 IEEE International Conference on Smart Internet of Things, SmartIoT 2019*, 8. https://doi.org/10.1109/SmartIoT.2019.00040

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

Martin Garriga, Arias, M., Alan De Rensis, Li, R., & Wu, Y. (2018). Blockchain based Academic Certificate Authentication System Overview. *In Proceedings of Sample Conference*, 8. https://intranet.birmingham.ac.uk/it/innovation/documents/public/Experiments/Blockchain-based-Academic-Certificate-Authentication-System-Overview.pdf

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

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

NationalStudentClearingHouse. (2016). Your Organization's Reputation on the Line: The Real Cost of Academic Fraud. In *National Student Clearing House*. www.nscverifications.org

Ngee Ann Polytechnic. (2019). *MEDIA RELEASE: CONVENIENT & SECURE AUTHENTICATION OF EDUCATION & TRAINING CERTIFICATES THROUGH OPENCERTS* .

Nguyen, D. H., Nguyen-Duc, D. N., Huynh-Tuong, N., & Pham, H. A. (2018). CVSS: A blockchainized certificate verifying support system. *ACM International Conference Proceeding Series*. https://doi.org/10.1145/3287921.3287968

Okebukola, P. A. (2017). *The Registry as the Heart of the University System : Making it Beat Efficiently*. 1–9.

Onwudebelu, U., Fasola, S., & Williams, E. O. (2013). Creating Pathway for Enhancing Student Collection of Academic Records in Nigeria – a New Direction. *Computer Science and Information Technology*, *1*(1), 65–71. https://doi.org/10.13189/csit.2013.010108

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

Poorni, R., Lakshmanan, M., & Bhuvaneswari, S. (2020). *DIGICERT: A Secured Digital Certificate Application using Blockchain through Smart Contracts*. 215–219. https://doi.org/10.1109/icces45898.2019.9002576

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-in-software-engineering-guidelines-and-examples/oclc/828789615&referer=brief_results

Sánchez De Pedro, A., Stampery, C., Iván, L., & García, C. (2016). *Stampery Blockchain Timestamping Architecture (BTA)*.

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

Srivastava, A., Bhattacharya, P., Singh, A., Mathur, A., Prakash, O., & Pradhan, R. (2019). A Distributed Credit Transfer Educational Framework based on Blockchain. *Proceedings - 2018 2nd International Conference on Advances in Computing, Control and Communication Technology, IAC3T 2018*, 54–59. https://doi.org/10.1109/IAC3T.2018.8674023

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

Swetha, N., & Priya, S. (n.d.). Online Certificate Validation Using Blockchain. *Special Issue Published in Int. Jnl. Of Advanced Networking & Applications (IJANA)*, 132–135.

Talib Visram. (2018, July 18). Malta wants to become "Blockchain Island" . *CNNMoney*.

Terry, G., Hayfield, N., Clarke, V., & Braun, V. (2017). Thematic Analysis. In *The SAGE*

Handbook of Qualitative Research in Psychology Thematic Analysis (p. 32). SAGE Publications Ltd. https://doi.org/10.4135/9781526405555

Trines, S. (2017). Academic Fraud, Corruption, and Implications for Credential Assessment. *World Education, News + Reviews*, 1–10. https://wenr.wes.org/2017/12/academic-fraud-corruption-and-implications-for-credential-assessment

UNIC. (n.d.). *Blockchain Certificates – Institute For the Future*. Retrieved March 19, 2020, from https://www.unic.ac.cy/iff/blockchain-certificates/

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. 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

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

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*. https://doi.org/10.1109/BigDataCongress.2017.85

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017b). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017*, 557–564. https://doi.org/10.1109/BigDataCongress.2017.85

Appendix

Appendix 1: Interview Questions

Section 1: Introductory discussions

1. Please can you 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 verification

4. How do you keep the record of graduates' certificate?
5. How do you share a graduate's information with an entity that seeks to verify a graduate's certificate?
6. Can you complete a verification process even if you are unable to ascertain all the necessary information about a graduate's certificate?
7. What is the essence of certificate verification which you carry out?
8. How do you access information about a graduate's certificate from another institution?

Section 3: Questions about the digitalization of workflow in the verification system

9. How would you describe your computer skills? Basic (), Average (), Highly skilled ()
10. What form of ICT do you currently deploy in the verification process?
11. What do you know about electronic verification?
12. Is electronic verification necessary? If yes, please explain why. If no, please explain.

Section 4: Questions about the challenges in the current system

13. What do you perceive as the challenges with the current system of verification?
14. How are the problems in the current system being tackled?
15. What would you consider as an inefficient verification system?

16. What aspect of the current system do you think needs to be improved for more effectiveness?
17. Would you say your clients are usually pleased with the current process? YES (),

    NO ()

    a If YES, how can you tell when they are pleased?

    b If NO, what are the reasons they are not pleased?

Section 5: Understanding the respondents' knowledge base of the technology

18. What do you know about blockchain technology? **(I would explain briefly if the interviewee does not know about blockchain. Based on the explanation, we would have further discussions in this section).**

19. Do you think that it will benefit the verification processes in your unit if blockchain technology is integrated? Yes () No ()
    a. If YES, please kindly explain how it can benefit your processes.

    b. If NO, please give reasons why you think it will not benefit your processes?

20. What do you think might be the major problems with the application of blockchain technology into the verification systems?
21. How do you think the problem(s) could be tackled?

Section 6: Questions about the evaluation of the current system

22. Are there specific bases for evaluating efficiency in the current system of verifying a certificate? YES (), NO ()
    a. If YES, please mention the basis for evaluation?
23. 28. Are there specific bases for evaluating the effectiveness of the current system of verifying a certificate?
    a. If YES, please mention the basis for evaluation?

24. How do you think the quality of services provided can be measured if blockchain is integrated into your processes?
25. Which part of the verification process do you think will be most affected by the introduction of blockchain technology?

Section 7: Questions about the impact of blockchain on stakeholders

26. Would you consider yourself as a stakeholder in the verification system?

27. How do you think the use of blockchain technology will impact your duties?

Appendix 2: Links to the Interview Audio and Transcriptions

Link to audio records
https://drive.google.com/drive/u/1/folders/1u9O9p0fWxeL8A5o7E-KLMsN3hzuWygOf

Link to transcriptions:

https://drive.google.com/open?id=1l_omjhS8-uLr_A4KN14X3XspalChoUrZ

Appendix 3: Thematic Plotting of Code Categories