Adoption of Blockchain for Academic Document Fraud Detection, Verification and Locker for Ethiopia

Gadise Adeba Gerbi

A Thesis Submitted to the Department of Computer Science and Engineering

School of Electrical Engineering and Computing

Presented in Partial Fulfillment for the Degree of Masters of Science in

Computer Science and Engineering

Office of Graduate Studies

Adama Science and Technology University

October 2021

Adama, Ethiopia

Adoption of Blockchain for Academic Document Fraud Detection, Verification and Locker for Ethiopia

By

Gadise Adeba

Advisor

Biruk Yirga(Ph.D.)

A Thesis Submitted to the Department of Computer Science and Engineering

School of Electrical Engineering and Computing

Presented in Partial Fulfillment for the Degree of Masters of Science in

Computer Science and Engineering

Office of Graduate Studies

Adama Science and Technology University

October 2021

Adama, Ethiopia

Declaration

I hereby declare that this Master Thesis entitled **"**Adoption of Blockchain for Academic Document Fraud Detection, Verification and Locker for Ethiopia**"** is my original work. That is, it has not been submitted for the award of any academic degree, diploma, or certificate in any other university. All sources of materials that are used for this thesis have been duly acknowledged through citation

Gadise Adeba _____ _____

Name of the student Signature Date

Recommendation

I/we, the advisor(s) of this thesis, hereby certify that I/we have read the revised version of the thesis entitled **"**Adoption of Blockchain for Academic Document Fraud Detection, Verification and Locker for Ethiopia**"** prepared under my/our guidance by Gadise Adeba submitted in partial fulfillment of the requirements for the degree of Master's of Science in **Computer Science and Engineering.**

Therefore, I/we recommend the submission of revised version of the thesis to the department following the applicable procedures.

Biruk Yirga(PhD)	_____	_____
Major Advisor	Signature	Date
_____	_____	_____
Co-advisor	Signature	Date

Approval Page

I/we, the advisors of the thesis entitled **"**Adoption of Blockchain for Academic Document Fraud Detection, Verification and Locker for Ethiopia**"** and developed by Gadise Adeba, hereby certify that the recommendation and suggestions made by the board of examiners are appropriately incorporated into the final version of the thesis.

Major Advisor	Signature	Date
Co-advisor	Signature	Date

We, the undersigned, members of the Board of Examiners of the thesis by Gadise Adeba have read and evaluated the thesis entitled **"**Adoption of Blockchain for Academic Document Fraud Detection, Verification and Locker for Ethiopia**"** and examined the candidate during open defense. This is, therefore, to certify that the thesis is accepted for partial fulfillment of the requirement of the degree of Master of Science in **Computer Science and Engineering**.

Chairperson	Signature	Date
Internal Examiner	Signature	Date
External Examiner	Signature	Date

Finally, approval and acceptance of the thesis is contingent upon submission of its final copy to the Office of Postgraduate Studies (OPGS) through the Department Graduate Council (DGC) and School Graduate Committee (SGC).

Department Head	Signature	Date
School Dean	Signature	Date
Office of Postgraduate Studies, Dean	Signature	Date

ACKNOWLEDGEMENTS

First and foremost, I give all honors and praise to God and his mother for all of their many blessings and for giving me the strength, the perseverance and the determination to fulfill this dream. I would like to thank my thesis advisor Biruk Yirga(PhD) for his encouragement, guidance and kindness .Words are not enough to express my profound gratitude for his help and motivation. I appreciate his brilliant insights and extraordinary ability on the area of Blockchain Technology and his thoughtful direction and the freedom he gave me to explore by interests. He supported me in the best possible way throughout my studies.

The completion of my thesis in its present form is the result of the support and help of many institutions and people. There are many people that I would like to thank for their inspiration, collaboration, help, advice, support and friendship throughout my research work. I am grateful to RiftValley University for financing my two-years-long study at the Adama Science and Technology University. I am also thankful to the Adama Science and Technology University for giving me the study chance. I am grateful to all students that participate during survey and also Registrar officers and Human Resource officers.

Most importantly, I am eternally grateful for my family for their unconditional love, steadfast support and unselfish sacrifice throughout my life. Thank God that I come from a family that believes in prayer. I love them endlessly.

Contents

LIST OF TABLES

LIST OF FIGURES

LIST OF ACRONYMS

DLT-Distributed Ledger Technology

DPOS-Delegated Proof of Work

ECBC-Educational certificate block chain

ECTS-European Credit Transfer and Accumulation System

EVM-Ethereum Virtual Machine

HR-Human Resource

IoT-Internet of Things

MOOC-Massive Open Online Courses

MSP-Membership Service Provider

PBFT-Practical Byzantine Fault Tolerance

POS-Proof of Stake

POW-Proof Of work

VCG-Vickrey-Clarke-Groves

ABSTRACT

An academic certificate is given to a person who has completed a certain course of study. In many countries, this academic certificate or degree can be used as verification of an applicant's qualification for a job. Despite the fact that it is not exhaustive, it is a great initial step in the selection of candidates for organizations during recruiting. While certificate ownership has many advantages, not everyone is willing or able to get them through legal means. The phenomenon of fraudulent degrees affects every field of endeavor. In 2017, for example, it was revealed that 40,000 persons in a single city had entered the Indian work force with forged documents. In addition, a survey conducted in Ethiopia over the last six years revealed that 3,200 civil servants with falsified academic credentials were hired in government organizations in Ethiopia's southern region. Prioritizing these degree fraud issues and updating the underlying systems is one way to approach them. The blockchain distributed architecture, which allows for the immutable and secure storing of academic credentials, appears to be a suitable solution. This could be a useful technique to obtain document traceability, possibly leading to the verification becoming totally digital and automated. The goal of this study is to determine the scope of academic document difficulties in Ethiopia and whether blockchain technology may help solve them. As a result, the premise is that blockchain systems could be a good fit for Ethiopian Academic Document Verification. A survey and interview were done to validate the concerns with academic documents and elicit requirements for a document verification system. It was able to propose and develop a prototype implementation of a blockchain architectural solution utilizing these criteria, with the goal of determining whether the gathered needs are practical to achieve.Hyperledger Fabric Blochchain framework is used for building a network. The proposed system contains mainly two parts, Front End (Web Application Layer) and Backend (Blockchain Layer).The Web Application gives universities, and potential employers an interface to accomplish tasks like issue academic documents, exchange transcripts and verifying certificates.This study was limited to the verification of academic certificates. Further research, particularly in nations like Ethiopia, is required, including the verification of passports, house blueprints, bank statements, and birth certificates.

Keywords: *Academic Certificate, Fraud Detection, Document Verification, Blockchain, Hyperledger Fabric*

CHAPTER ONE

INTRODUCTION

1.1. Background

Education is crucial for a country's development. A significant investment in human capital is necessary to accomplish long-term economic success. Education may boost people's productivity and innovation while also encouraging entrepreneurship and technological advancements(Ge & Hu, 2021). It is also critical for a country's economic and social advancement, as well as income distribution. An academic certificate is given to a person who has completed a certain course of study. In many countries, this academic certificate or degree can be used as verification of an applicant's qualification for a job(Shah & Kumar, 2019).

The importance of an academic credential cannot be overstated. A degree can potentially open up new prospects for a better life, equipping an individual cognitively and socially to live a more meaningful and fulfilling existence. It is often a distinguishing element among a group of people, classifying them into different social strata and economic statuses. Despite the fact that it is not exhaustive, it is a great initial step in the selection of candidates for organizations during recruiting. While certificate ownership has many advantages, not everyone is willing or able to get them through legal means.

Credential falsification has already become widespread around the world, including Ethiopia. Fake degrees are a problem in every field. For example, in 2017 it was revealed that 40,000 people in a single city had entered the Indian labor force using forged documents(Trines, 2019.). In addition, according to a survey done in Ethiopia during the last six years, 3,200 civil servants with forged academic qualifications were hired in government institutions in Ethiopia's southern region(Behak,2020).

Certificate forgery is used by those who want to improve their lives without having to pay for, time, or effort that a real certificate requires. Furthermore, today's means and opportunities for obtaining a fraudulent degree are unprecedented(Attewell & Domina, 2011). However(Eckstein, 2003) argues that the failure of institutions and organizations to check degrees and credentials is the main reason why academic fraud in the form of phony documents is on the rise. Employers and other authorities must be able to detect degree fraud in order to verify the credibility of an academic degree. Verifying the status and authenticity of a diploma

is challenging with today's centralized databases, and blockchain technology offers a viable solution(Awaji et al., 2020a).

Blockchain technology has emerged as a critical mechanism for tamper-proof digital data, and it is quickly gaining traction in a variety of fields. According to(Poorni et al., 2019), blockchain is a decentralized communication and data management system that is still in its early stages and does not require the use of a trusted third party. Various parties can provably transact on the technology without resort to a central authority, even if they do not trust themselves. According to(Srivastava et al., 2019), blockchain addresses certificate verification issues by providing verifiable digitally time-stamped documents that are resistant to change. The blockchain, which was once connected with virtual currency, has quickly acquired popularity in a variety of other fields. On the blockchain, transactions can be initiated and validated without the requirement for a controlling authority. This is its distinct selling factor. To this purpose, studies have found that blockchain technology has the ability to adequately address the problem of certificate authentication.This study can help Ethiopia by using blockchain technology as a platform for degree fraud detection and verification.

1.1.2. Motivation

Degree fraud is a developing problem that requires immediate attention. In recent years, the fake replication of certificates has expanded dramatically, posing a threat to education policy stakeholders. Fake credentials are an urgent problem in Ethiopia that must be addressed in order to ensure the national education system's reliability. According to a study presented by the Ministry of Education (MoE) to the House of People's Representatives (HPR) when delivering a nine-month performance report, there are bogus degree holders working in government institutions. In recent years, the Oromia Regional State Civil Service and Human Resources Bureau revealed that it had conducted a screening of educational documents of employees in the region in partnership with the Information Network Service Agency (INSA). Out of the 8,300 employees, 6,400 admitted to possessing forged documents and apologized.

Fake degrees are widely used to acquire unfair advantages, with the goal of acquiring unequal access to professions that need competence, honesty, and trust. According to survey(MoE,2019), 77%of employees are using forged documents, implying that they have been working without the necessary expertise and competence for the job. This can cause both direct and indirect harm to the country. As a result, a system such as degree fraud detector and verifier based on blockchain is required to end the situation.

1.2. Statement of the problem

People frequently fabricate false certificates to conceal their academic qualifications since they are so valuable. According to (Cohen & Winch, 2011) there are currently 2 million phony degree certificates in circulation in the United States, as well as 300 illegitimate universities. The United States has the most phony institutions in the world, according to(Share et al., 2014), followed by the United Kingdom, which has roughly 270 false institutes. According to Healy (2015), up to 35% of candidates in Australia faked their academic credentials in order to gain jobs. Most candidates lie about at least some aspect of their educational credentials and experience. According to(Garwe, 2015), academic degree fraud costs employers over $ 600 billion each year. Fake academic certificates can be obtained from five (5) different sources. 'Degree Mills,' for example, are places where phony credentials are created and sold to clients(Garwe, 2015), ‘Fabricated Documents' that represent a fictitious degree or institute, ‘Modified Documents' that are changes in legitimate documents such as enrollment, graduation dates, grades, course content, date of birth, specialization, and so on, and ‘In-House Produced' which are fake documents fabricated by legitimate institution employees and printed on authentic paper and bearing the Academic certifications provided by unregistered institutions lack official authority to grant such credentials and make baseless claims concerning recognition and accreditations. The above data suggest that the problem of fraudulent certifications has reached critical and alarming dimensions, and that it must be addressed immediately.

People will most likely stop fabricating credentials if verification becomes more common among institutions and employers. To tackle the threat, certificate verification regulations and practices are evolving. Electronic certificate verification is gaining popularity and being used in several organizations. By searching an institution's database, the automated method allows for seamless and instant verification of certifications. To verify a certificate, an employer may not need to contact the institution directly.

In Ethiopia, on the other hand, the certificate forgery problem is worsening and will likely endure without a trustworthy way to validate certificate assertions. The Addis Ababa City Transport Authority recently announced that it had fired numerous employees who were found to be working with forged credentials (Behak, 2019). Furthermore, a survey undertaken over the last six years indicated that a total of 3,200 civil officials with forged academic qualifications were hired in government institutions in Ethiopia's southern area.

Employers face significant worker turnover and replacement costs, as well as a loss of patronage and revenue, the possibility of a lawsuit, and reputation damage.Given the aforementioned issues, it is reasonable to seek a certificate verification system for institutions and employers that is effective, efficient, trustworthy, and easy to use.

Blockchain technology has lately surfaced as a potential means of validating the document verification process, as well as a powerful tool for combating degree fraud and misuse. As a result, the goal of this research is to create a blockchain-based platform using the Hyperledger Fabric framework used to detect degree fraud in Ethiopia.

As a result, the following questions should be addressed by this research:

- What challenges can students face after graduation as a result of paper certificates in Ethiopia?
- How might a blockchain-based solution improve Ethiopia's present academic certificate issuance and verification process?

1.3. Objectives

1.3.1. General Objective

The General Objective of this study is to explore the underlying problems in Ethiopia's current academic document issuance and design a model for detecting degree fraud and verifying academic documents.

1.3.2. Specific Objectives

The following are the study’s specific objectives:

- To study about Ethiopian graduate and undergraduate students' opinions on using Blockchain technology to issue and manage certificates and degrees.
- To assess the issues that having graduated students may experience if they receive a document certificate rather than an electronic version.
- To examine the most recent research trends and the underlying implementation of blockchain-based certificate verification systems in higher education.
- To research the best methods for using blockchain technology to detect degree fraud.
- To provide a design for Academic Degree Verification based on blockchain technology.
- Create a prototype for the proposed architecture implementation.

- To assess the proposed framework utilizing security themes that are frequent in degree fraud detection and verification systems.
- To make recommendations for future work on the use of blockchain for certificate verification that is feasible.

1.4. Methodology

A number of measures must be taken in order to create a better blockchain-based degree fraud detection system. In order to attain the above-mentioned goals, the following procedures have been taken.

1.4.1. Literature Review

Research papers, books, journal articles, and other published publications are consumed in many ways. The literature review is carried out for a variety of reasons. Relevant studies in document verification are studied in order to choose the best blockchain architecture for the research. In general, a thorough review of the existing literature has been conducted on the following important points:

- Security themes for academic document verification
- Efficient Blockchain Framework and Platforms

1.4.2. Data Collection

Surveys and interviews were the two methods we used to collect information. We also go over how the data will be collected and analyzed. One of the objectives of this research is to assess how graduates think about using Blockchain technology to issue, maintain, and verify certificates and diplomas. The investigation also involves registrars and human resources to see their personal perspectives and level of awareness of Blockchain technology.for conducting survey and interview, the researcher used Convenience sampling technique.

1.4.3. Tests used in the Study

We used two tests to examine the data for the survey.

1.4.3.1 Descriptive Statistics

The essential elements of the data study were briefly explained using descriptive statistics analysis. Descriptive statistics(HOLCOMB, 2020) is a method for organizing and summarizing data.

- **Chi-Square**

Chi-square is a method for analyzing group differences and determining whether or not there is a dependent variable(McHugh, 2013). The study analyzes the association between the participants and their demographic data using the Chi-square test.

- **Sentiment Analysis**

Sentiment analysis is a tool that uses written language to describe the participants' feelings, attitudes, and opinions(Liu, 2012). The major purpose of this test was to determine the emotional mode behind the said statements in order to assess the participants' views on Blockchain adoption.

1.4.4. Implementation Tools

Selecting a suitable implementation tool is critical for a smooth course of action. The researcher mostly employed the instruments provided in Table 1 in this investigation.

Table 1: Implementation tools used for the study

Tool	Used for
Chiq-square	Survey analysis
Sentiment Analysis(Azure Machine Learning studio)	describe the emotions, attitudes, and opinions, of the participants
Hyperledger fabric framework	Building blockchain network
Embedded javascript(EJS)	Distributed Application interface Design
Goalang	Smart Contract implementation
Hyperledger Caliper	To test the performance of proposed model

1.5. Scope and limitation of the study

In this study, permissioned blockchain technology was adopted to design Academic certificate verification system which can help countries like Ethiopia by providing a decentralized, shared, Transparent, secured and easily accessible academic record repository. This study includes the development of a smart contract with the corresponding Hyperledger Fabric node topology. The ledger was created to store document-related transactional data from Ethiopian academic institutions, as well as to execute smart contracts in the form of transactions to manage both assets and participants' identities.

The process of creating an electronic document and uploading it to a server is not addressed in this research. External systems are responsible for developing their own integration modules.This study considers only verifications of academic certificates given at the end of completing Degree programs. It doesn’t consider in verification of short term trainings.

1.6. Significance of the Study

According to various studies, the issuing authorities of the certificate are often compromised for the student data protection credentials, with roughly one million students graduating each year. Because there is no effective anti-forge system, events that cause the graduation certificate to be forged are common. These findings can be utilized to identify all issues that students and businesses have with paper certificates, as well as to remedy the problem while security concerns remain. Blockchain is one of the most recent data security technologies available. The block chain's immutability aids in resolving the problem of certificate forgery. Potential employers, who can verify the information provided by students on the spot.

1.7. Organization of the Thesis

The following is the thesis's structure. The background, motivation, problem statements, research questions, objectives, methodology of the study, scope, limitation of the study, and significance of the study are all presented in the introductory part. The second portion of this paper presents a literature review. First, a review of the literature on fraudulent activities for creating degree fraud. Second, it presents about blockchain technology and its characteristics. Third, existing blockchain-based solutions and how they protect certificate systems against fraud. Following the literature study, Academic document issues validation and requirements elicitation is presented on chapter 3.chapter four presents the proposed blockchain-based academic degree fraud detection model. The proposed design is prototyped in chapter five and the study's conclusion and recommendations are presented in chapter six.

CHAPTER TWO

LITERATURE REVIEW

2.1. Overview

Degree certificates are awarded once degree programs are completed and are considered proof of completion of the corresponding degree programs. As a result, businesses rely on degree documents to verify applicants' educational backgrounds. Similarly, verifying degree documents is required when applying to other educational institutes for higher education. Because of the importance of degree documents, con artists are attracted to them and are motivated to use them to obtain jobs or admissions. Understanding linked studies is crucial to research since it lays the groundwork for subsequent inquiries. Such knowledge creates awareness of what has already been accomplished as well as the knowledge gap that ongoing research should address. This chapter will present background research and delve deeper into the reviews that are directly connected to the Study's goals.

2.2. Degree Fraud

Because of the increased demand for degree certificates in the employment market, degree fraud has become a global phenomenon. This problem of false diplomas does not only affect higher education; it affects students from high school to doctoral level. Degree fraud causes enormous harm to society and the economy as a whole. It has a direct negative impact on universities whose degrees have been forged, students who buy forged degrees knowingly or unintentionally, and companies who hire that degree holder based on their trust in those credentials. When a fake diploma is generated, it misrepresents the academic institute and, as a result, harms the institute's reputation.

A fake degree is a fraudulent or inferior academic degree that is used to provide the appearance of true academic performance(Baum, 2014). A degree mill is an organization or individual that sells or offers academic degrees or certificates for a price without the students completing necessary studies or coursework. Degree mills are institutions or entities that do not have the required accreditation. A non-existent degree offered by a university or organization is also referred to as a fake degree. When a false degree holder applies for a job, he may state his degree or provide a certificate that appears to be authentic, despite the fact that he never attended that university.

Some students, intentionally or unconsciously, purchase fraudulent degrees from degree mills in order to gain the benefits of having a degree. A person may mention a degree certification on his resume or application without having completed or even attended that degree. When applying in a foreign country, the applicant may use a copy of the original document that has been incorrectly translated.

Although false certificates are a worldwide issue, it is difficult to determine how fraudulent university administrators register or maintain bogus or illegitimate results in an approved university's official information system. This is one of the key reasons why detecting degree fraud is a difficult undertaking. This method is largely dependent on someone's credentials investigation experience and a trusted network of professionals throughout the world who are knowledgeable in document verification(Koenig Edward,2012). On the one hand, if the diploma is falsified outside of a legal institute or provided by a diploma mill, it is rather easy to identify the diploma mill with minimal examination. If the certificate is faked from a legitimate institution, however, it is more difficult to detect. Several actors at an institute, such as students, teachers, the registry office, and other information systems, can be involved in the production of illicit certificates. There is no simple way for outsiders, or even insiders, to validate each actor's contributions to the diploma process. In most circumstances, a company will send an email or contact the registry office to verify the authenticity of a job applicant. If certain unscrupulous officials have recorded bogus grades in the information system, the university registry office will respond positively to the certificate's authenticity(Moore, 2009). In some nations, a teacher's recommendation letter may be prejudiced or based on a personal relationship. As a result, the issues are complicated. As a result, a potential employer and admissions office face a hurdle in trusting any entity participating in the university degree process and verifying all achievements.

We've made a list of techniques to make a false certificate depending on our degree fraud literature review. This listing would be used to determine how current blockchain-based certificate systems combat fraudulent activities. Table 2 presented some of common fraudulent practices involved in the creation of a bogus diploma(Moore, 2009).

Table 2: The Possible Fraudulent practices involved in the creation of a bogus diploma

Acts of Fraud	Fraudulent practices involved in the creation of a bogus diploma	Actor(s)
Activity 1	Even though the student did not attend or complete the degree there, the certificate is added to his or her CV .	Student
Activity 2	By using identical paper and unique security characteristics found in the original paper certificate, the student creates a counterfeit paper copy of the original paper certificate	Student
Activity 3	A student purchases a certificate from a diploma mill or a non-accredited university	Student, diploma mill
Activity 4	The student adopts a fictitious translation of the original document	Student
Activity 5	With the help of corrupt officials, a student can transform a work credential or life experience into academic credit for an accepted university degree(Moore, 2009)	Student, university officials
Activity 6	To confirm the legitimacy of the counterfeit certificate, corrupt authorities alter students' academic information such as enrolment date, course completion date, and grade in the study data management system(Mikroyannidis et al., 2019)	university officials

2.2.1. Sources of Degree Fraud

According to(Garwe, 2015), there are five different sources for degree Frauds,namely, Degree Mills, Fabricated Documents, Modified Documents, In-House Produced, Translations.Table 3 presents the summary of degree fraud sources.

Table 3: Sources of Degree Fraud(Sayed, 2019)

No.	Degree Fraud Source	Descriptions	Actor(s)
1	Degree or Diploma Mill	It's a business or organization that poses as a higher education institution but sells fraudulent academic degrees and credentials for a charge(Cohen & Winch, 2011).	Corrupt University Officials
2	Fabricated Documents	A phony degree or institute is represented by a fake academic certificate.	• Student • Degree mill institutions
3.	Modified Documents	Changes in enrollment, graduation dates, grades, course content, date of birth, and specialization are all examples of legitimate papers that can be modified(B.melby,2021)	Student
4.	In-House Produced	Fake documents created by staff of real institutions and printed on genuine paper with the institution's seals, stamps, and signatures	Corrupt University Officials
5.	Translations	An academic document that has been incorrectly translated to meet the needs of an employer(Ghandour et al., 2019)	Student

2.3. Blockchain Technology

Blockchain refers to data storage that uses an innovative data structure, and blockchain technology refers to the mechanism or methods, computer programs, architecture, and network that keep the blockchain running(Share et al., 2014). In other words, Blockchain technology is a new technique of storing data in a decentralized and distributed database in a collaborative manner. The technology that underpin blockchain were developed in the 1980s and 1990s, but it wasn't until Satoshi Nakamoto's whitepaper Bitcoin: A Peer-to-Peer Electronic Cash System in 2008 that the term "blockchain" became famous(Ge & Hu, 2021). In his article, even Satoshi avoided using the term "blockchain." He proposed a distributed public ledger system in which

legitimate transactions are stored in blocks that are cryptographically chained together based on computational evidence, eliminating the requirement for trust or trusted third parties like as financial institutions.

The innovative digital currencies Ethereum, Bitcoin, and Litecoin are built on the blockchain technology. The use of blockchain technology behind these cryptocurrencies is because the nature of the system's design can eliminate the need for any middleman, such as a bank, to provide trust and security in transactions. It can check transactions, such as the double-spending problem, establish business rules through smart contracts, and preserve legitimate transaction records in a decentralized system's cryptographic chain of blocks(Curmi & Inguanez, 2019).

2.3.1. The Blockchain Architecture and Workflow

Before getting into the specifics of the blockchain workflow, this sub-section include an overview. As a result, starting with signature generation, Figure 3 below shows important procedures. Digital signatures are created using a signature generator that combines Cryptography and Data Encoding. It follows a set of rules and requires cryptographic keys, such as private and public keys. The private key is used to encrypt a message that is sent over the network. When a transaction request is issued, the nodes verify the transaction using the network's agreed-upon consensus mechanism. After that, a block is constructed to broadcast the transaction that has been validated. In the following sections, we'll go over how to make blocks and other components.

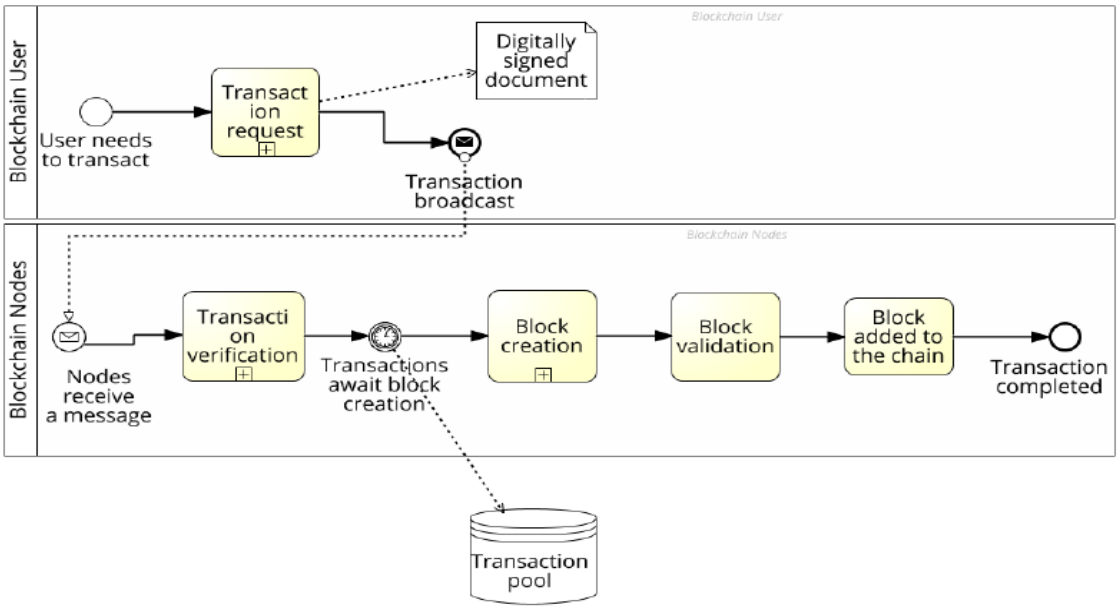

Figure 1: Workflow of a transaction in the Blockchain(Innovation, 2001)

- **Transaction Request**

Data, typically the message is entered into the network as a transaction. The messages could be used as inputs or outputs by computer programs. The contents of the communication may also be encrypted, or the message may contain a link to encrypted data stored in another digital place. Figure 1 depicts a transaction request with a collapsed subprocess to avoid capturing specific details that aren't visible in the diagram. This step is usually marked by hash generation, message encryption, and digital signing using a private key, following which the message is transmitted over the network. The action of other nodes in the blockchain users lane comes next as shown in Figure 1.

- **Nodes**

A node is the computer system representation of a blockchain participant. highlighted that every node in the network stores a copy of transactions and that after receiving consensus from other nodes in the network, a node likewise records the transactions in its ledger. Any transactions that its user (human) initiates in the network are published to the other nodes, and a node routinely verifies that the copy of the ledger it has is the same as the other nodes on the network.

- **Transaction Verification**

To verify that a transaction is genuine, blockchain uses cryptography to create a digital signature. Users have a pair of private and public keys, therefore signing transactions in the request process is done with a private key. While the user's private key is kept private and is used to sign any transactions in the process of encrypting the message, the encrypted message is broadcast to the entire network. Because it involves a collection of actions from the peers who validate the user who submits a transaction request and verify the message using the public transaction key, this is illustrated as a collapsed subprocess in Figure 1. The verification step makes sure the message hasn't been tampered with in any way. A transaction that has been successfully validated is authentic and is maintained in the transaction pool until it is added to the block's ledger. As a result, it is depicted in Figure 1 as an intermediate timer event.

- ## Consensus Algorithms

A network contains many nodes, all of which are expected to be unreliable. Consensus methods ensure network dependability by ensuring that subsequent nodes are truly the original version, as well as protecting the system from being hijacked and forked by malicious parties. Before each transaction is recorded in the blockchain,(Curmi & Inguanez, 2019) pointed out that it is subjected to decentralized scrutiny to ensure that no illicit transactions can take place. The consensus mechanism is a collection of rules that leads participants through the process of verifying transactions, validating them, and adding them to the blockchain. A specific consensus model can be chosen from among the various varieties available including, Proof of Work, Proof of Stake, Practical Byzantine Fault Tolerance (PBFT), Delegated Proof of Stake (DPoS) (Innovation, 2001).

- **Proof of Work (PoW)**

In blockchain, the PoW consensus algorithm is the most extensively utilized algorithm. It was invented by bitcoin, and it posits that all peers vote with their processing power by solving PoW instances and building the necessary blocks. Bitcoin, for example, uses a hash-based PoW, which includes finding a nonce value that is smaller than the current goal value when hashed with additional block parameters (e.g., a Merkle hash, the previous block hash).When a nonce is identified, the miner builds a block and sends it to its peers via the network layer. Other network peers can check the PoW by computing the block's hash and seeing if it meets the criteria of being less than the current target value(B.melby,2021). To put it another way, consensus necessitates that the calculated value must be either equal to or less than a specified value

- **Proof of Stake (PoS)**

Instead of solving the PoW, the PoS method requires the node that generates a block to provide proof that it has access to a particular quantity of coins before being acknowledged by the network(B.melby,2021). Because it is considered that persons with more cash are less inclined to attack the network, this method requires participants to confirm possession of a certain amount of currency(Ghandour et al., 2019). As a result, only those who are capable of providing the PoS can take part in the blockchain maintenance process. PoS saves more energy than PoW when it comes to energy consumption.

- **Practical Byzantine Fault Tolerance (PBFT)**

This consensus technique was created to handle Byzantine faults, such as a node's arbitrary behavior, entering and leaving the network at any time, which is common in distributed systems. To deal with Byzantine errors, this approach proposes a state machine replication technique. It uses a state machine replication method that executes read-only operations with only one message round trip and read-write actions with two. It also makes use of a reliable authentication system.

During normal functioning, a technique based on message authentication codes is utilized; public-key cryptography is used only when there are problems(Mikroyannidis et al., 2019).

- **Delegated Proof of Stake (DPoS)**

PoS is a direct democratic process, whereas DPoS is representatively democratic—stakeholders elect delegates to develop and validate a block. The block may be verified rapidly since there are fewer nodes to validate it, which means the transaction can be confirmed swiftly(Selimi et al., 2018).

- **Block**

A block in the chain is made up of the block header and the block body, which records transactions on the ledger in the order in which they occur. The header contains information about each block (block metadata), which typically comprises a time stamp, a hash reflecting the block's payload, the hash of the preceding block's header, and the block size. If a hash puzzle must be broken to publish a node, it may also contain the cryptographic nonce.

A block resides within a distinct network and adheres to the rules established by the network's members. Before transactions are added to the blockchain, it validates that the timing and order are correct. Every subsequent block, using the hash function, verifies the legitimacy of the previous block and, by extension, the entire blockchain. As a result of the technique, blockchains are tamper-proof, resulting in immutability(Shahid et al., 2019)**.**

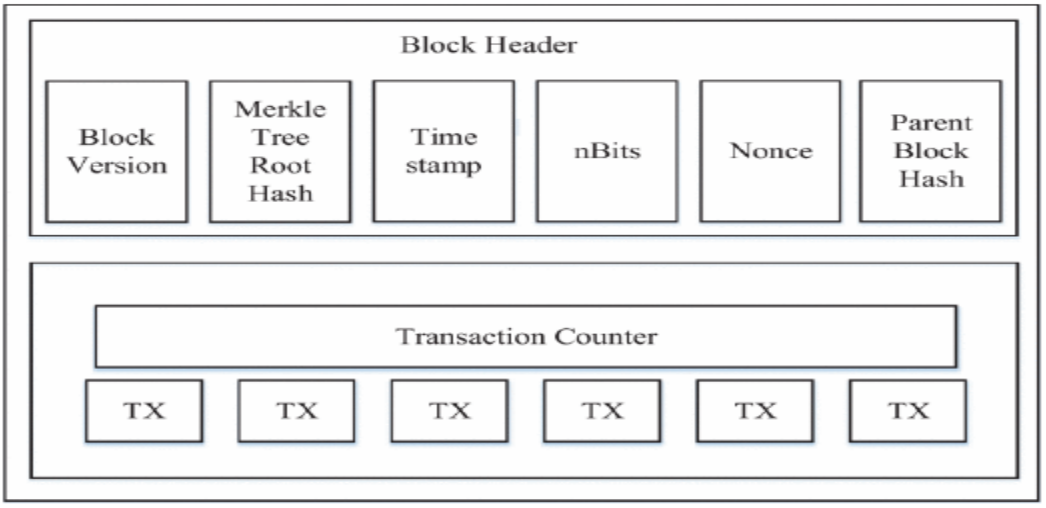

Figure 2: Architecture of a Block(Lu, 2019)

The block header includes(Lu, 2019):

1. Block version: indicates which set of block validation rules to follow.
2. Merkle tree root hash: the hash value of all the transactions in the block.
3. Timestamp: current time as seconds in universal time since January 1, 1970.
4. nBits: target threshold of a valid block hash.
5. Nonce: a 4-byte field, which usually starts with 0 and increases for every hash calculation
6. Parent block hash: a 256-bit hash value that points to the previous block.

The block body is composed of a transaction counter and transactions. The maximum number of transactions that a block can contain depends on the block size and the size of each transaction. Blockchain uses an asymmetric cryptography mechanism for the purpose of validation and authentication of transactions.

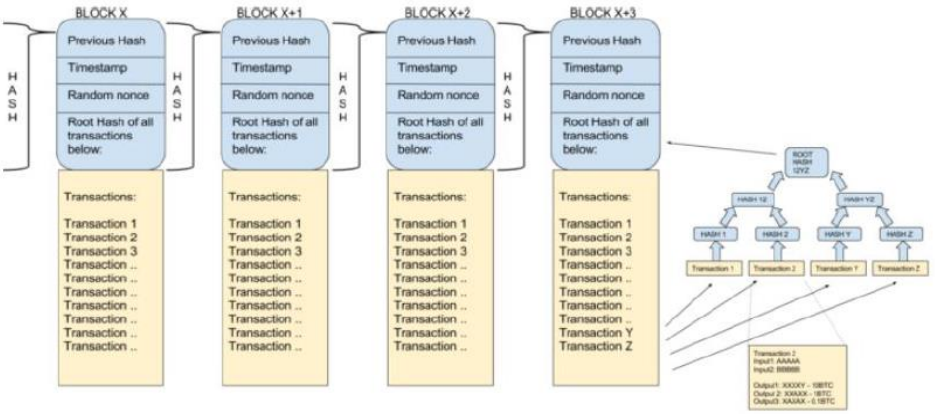

Figure 3: Description of a parent block hash(Mohanta et al., 2019)

- **Block Creation and Validation**

Until they are added to the block, nodes verified transactions are kept in a memory pool. Only one member can add transactions to a block, which is extremely tough to figure out when there are a lot of distrusted participants. As a result, the participants' set of rules, such as Proof of Stake and Proof of Work, are used to make this decision. Because the node that creates and publishes a block in a Proof of Work Model, for example, must first solve a difficult mathematical conundrum, the "work" being the solution to the riddle, this step in Figure 1 is also a collapse process. Because it is assumed that a user with a high stake in the network will most likely want the network's good, publishing a block in the Proof of Stake model is based on the amount of stake a user has in the entire network. Once a block is formed, a transaction is attached to it, and all nodes agree by validating the block. The transaction cannot be changed until the blockchain is updated, which occurs regularly(Mohanta et al., 2019).

- **Chaining of Blocks**

The information from previous blocks – in the form of a hash value – contained in the header of each subsequent block connects the blocks to form a blockchain, culminating to the “transaction completed” end event seen in Figure 1. Each new block carries the hash of the previous block, forming a single network. Any change to a block affects the hash value of the block and must affect the entire network of blocks, which cannot happen without all nodes being notified. When a modification message is identified, it can be ignored, preserving the blocks' integrity(Naumova et al., 2019).

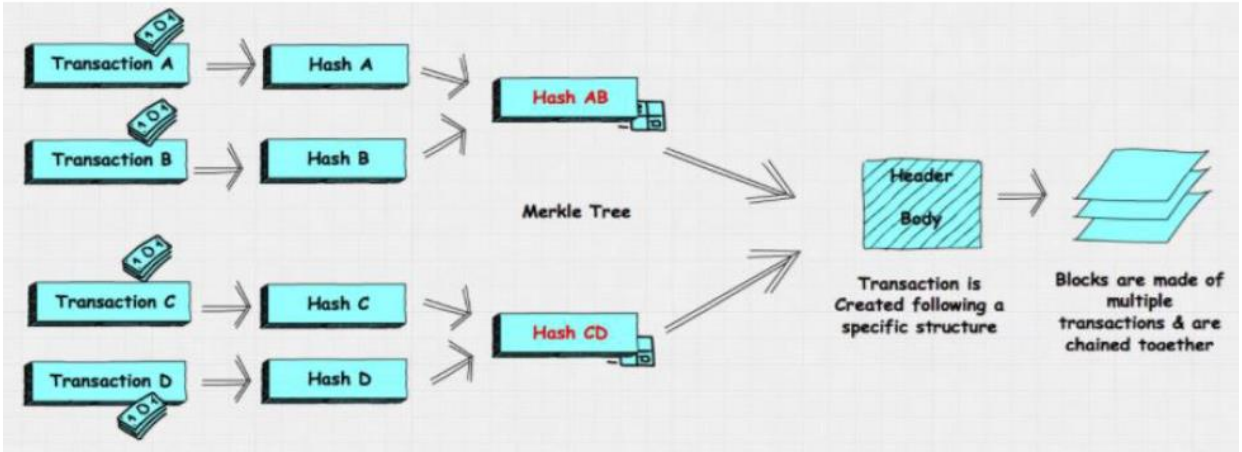

Figure 4: Process of Block-chaining(Naumova et al., 2019)

- **Hash Function**

The information from previous blocks is recorded as a hash value in the header of each future block, forming a blockchain and leading to the “transaction completed” end event in Figure 3. The hash of the previous block is carried by each subsequent block, producing a single network. Any change to a block impacts the block's hash value and must effect the entire network of blocks, which can't happen unless all nodes are notified. If a modification message is detected, it can be denied, preserving the integrity of the blocks.

- **Wallet**

Anyone who wants to participate in any form of network activity, whether private or public, will need access to the internet. Software applications that serve as a conduit between customers and blockchain technology include desktop applications, smartphone applications, and digital wallets. Users can securely store private keys, public keys, and related addresses in a blockchain wallet, as well as send and receive digital assets. It can be downloaded and installed on a computer, or it can be viewed using a web browser. For example, a graduate must join to the network with a wallet in order to obtain his digital certificate from the issuer and share it with an employer.

2.4. Blockchain Characteristics

Researchers have been looking into how blockchain technology may be utilized to improve traditional centralized data storage in recent years. Many sectors have implemented this technology in recent years(Yumna et al., 2019; Zheng et al., 2018) and essential aspects of blockchain technology have considerably improved their services.some of the most important properties of Blockchain are:

- **Decentralized**

The transaction is regulated and validated by a central server or authority in centralized or traditional data storage. Unlike traditional data storage, there is no central authority to control transactions or data in blockchain technology, and a copy of the transaction ledger is distributed and kept across the blockchain network. Thousands of computers in the blockchain network have a copy of data if one node of the blockchain network is destroyed or erased. Furthermore, in a blockchain network, it is almost impossible to modify a specific data in a block.

- **Transparency**

Blockchain technology enables the creation of a decentralized and transparent database of records. Any transaction carried out on a blockchain network is transparent to all network participants. The transactions and transaction history are visible to all users on the blockchain network. For example, Google Docs allows each participant to see all document modifications, including who made them, what they were, and when they were made. The blockchain network, like Google Docs, allows all members to observe all modifications made to the material.

- **Exceptional Availability**

In contrast to traditional or centralized systems, the data saved in blockchain has a very high degree of availability since a copy of the public ledger of all transactions is distributed among users. Thousands of computers in the blockchain network hold a copy of the database records, and each participating computer is accountable for the blockchain database's security and integrity. Even if all nodes in one geographical location lost their copy of the blockchain, other nodes in another location will still have it.

- **Immutable**

Once a transaction has been confirmed and added to the blockchain network, it is permanently kept in the blockchain database. To update the data contained in each block, 51 percent of the blockchain network's nodes or participants must agree and attain consensus(Castro & Liskov, 1999). Due to the large number of members in the blockchain network, it is nearly impossible to persuade them to engage in unethical behavior.

- **Anonymity**

Each participant user interacts with each other using a blockchain-generated address in blockchain technology. This allows blockchain to maintain the anonymity of participating nodes while also allowing transactions to be executed in secret. Each participant has a private and public key in this system, which uses asymmetric cryptography for digital signatures. The public key in the blockchain network is visible to all and is known by all participants, and it may be used to trade data between users. Information about the user, such as their name, email address, and phone number, is converted into a cryptographic hash value. This hash value is a one-of-a-kind token that is recorded on the blockchain and allows data to be kept private because hash values are nearly irreversible.

- **Auditability**

All transactions with timestamps can be validated and stored using blockchain technology. This allows any user with the appropriate permissions to verify and track all prior records, including the genesis block. In the Bitcoin blockchain, for example, the user may recursively track each transaction back to earlier transactions. This will improve the data stored in the blockchain network's transparency and transparency(Cheng et al., 2018).

- **Smart Contract**

A smart contract is an application program that runs on blockchain platform and used to fully replace roles played by central authority in centralized system. code for smart contract script is written by blockchain developers and once programmed, it runs exactly as per specified instruction without any interference of third party. similar to normal contract which is based on legal framework to control each participant to behave according to specified terms, smart contract script run automatically when the conditions in contracts specified by developer are met. If the specified conditions on smart contract script are not met, smart contract automatically prevent or transact out of the agreement. Due to this, smart contract eliminates the centralized party that can responsible to execute processes or functions specified in smart contract script.

2.5. Types of Blockchain

Blockchain technology is divided into three major categories: Public, private, and hybrid Blockchain (M.kurton,2020).

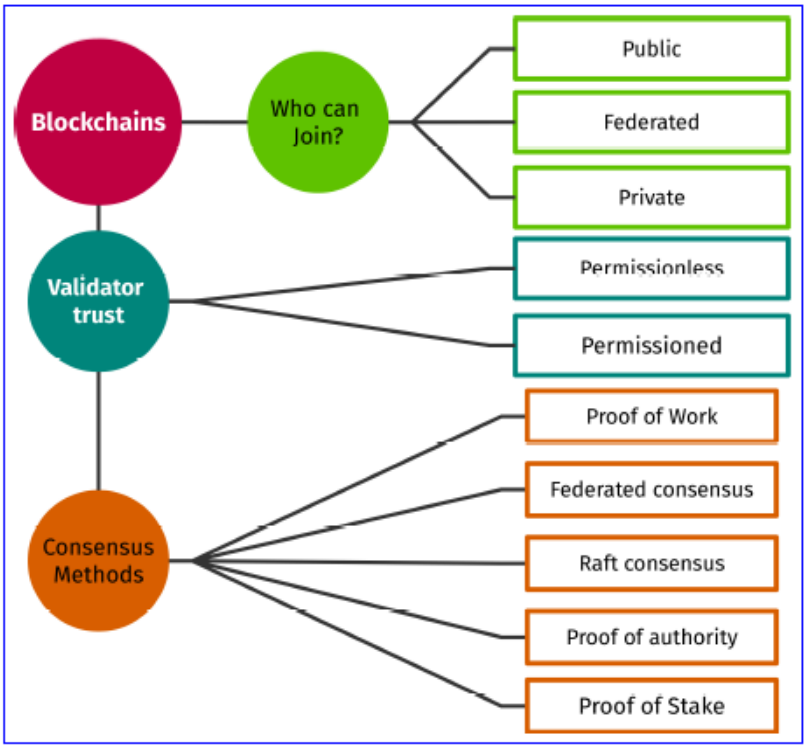

Figure 5:blockchain categorization(Gavofyork, 2020)

A blockchain is a distributed data of records in which the database is organized as a list of sequential blocks with immutable properties.by considering techonolgy used blockchains are mainly divided into three categories(Gavofyork, 2020):

- **Public blockchains (permissionless)**: as the name implies, public blockchain allow anyone to join and participate as users, miners or developers. This blockchain type (gavofyork
- , n.d.)enables all transaction to be transparent among participating nodes and anyone can examine the transaction details. In addition, a public blockchain is a decentralized blockchain type in which no individual nodes can control transactions to be processed or recorded on blockchain database. An example of most widely used public blockchain nowadays is Ethereum.
- **Private Blockchains (permissioned)**: in this type of blockchain, only known parties or users can join the networks. In addition, private blockchain keeps transactions privately and are only available to authorized users to that have privilege to access the network. As compared to public blockchain, private blockchains are more centralized. Most of the time private blockchains are best choice for enterprises that want to collaboration for running business and share data, but at the same time don't want their sensitive business data visible on a public blockchain.an example of private blockchain is hyperledger.

- **Consortium/Hybrid blockchains**: this blockchain type is created by combining the privacy benefits of a private blockchain with the transparency benefits of a public blockchain. Hybrid blockchain provides a significant flexibility for any businesses by making some of data public for sharing purpose among participants and some of sensitive data will be kept private. Ark is an example of hybrid blockchains.

2.6.Blockchain Frameworks

Blockchain frameworks enable developers by providing all required components used for developing blockchain-based applications. In general, existing blockchain platforms can be grouped into three blockchain types namely, public, private and hybrid. Among all platforms used for implementation of blockchain based systems in educational areas, Ethereum is one of the most widely implementation platform in recent years. In this section some of common platforms for implementing Blockchain based projects will be discussed.

Ethereum

Ethereum is a public blockchain platform that provides programming tools to write and run smart contract scripts. It is an open and distributed platform created by Vitalik Buterin in the year 2013 and which enables developers to easily implement and deploy cross industry decentralized applications. For instance, cryptocurrencies can be designed and issued by Ethereum platform. Ethereum also allows implementing smart contracts in a choice of developers programming language interest. common programming language used to write smart contract is soldity6.in Ethereum platform, smart contract enables a blockchain application to represent arbitrarily complex transactions.in addition, ethereum is an open-source that present a package that permits developer to create Distributed application (Dapp).Ethereum and blockchain developers are maintained all the programming tools required to develop blockchain based application using Ethereum Platform. Some of major characteristics of Ethereum are as follows(Sharma & Negasa, 2020):

1) Persistency: data stored on ethereum blockchain cannot be tampered by third parties.
2) Secure: entities maintained a decentralized application in Ethereum platform and errors derived from personnel factors are automatically avoided.
3) Permanent: the services provided by ethereum platform cannot be interrupted because of individual node or computer crash.

Ethereum platform mainly consists of the following three components:

- **Ethereum Virtual Machine (EVM):**
  Similar to java virtual machine (JVM), EVM is the required runtime environment for running smart contracts in Ethereum. In Bitcoin blockchain platform, application developers are provided with a fixed set of commands. Unlike Bitcoin, Ethereum platform allows application developers to run any blockchain systems based on their

interest. Most of application developers are using a high level language called solidity that can instruct the EVM to execute applications.

- **Solidity:** Solidity is the high level object oriented programming language which is similar in programming syntax with javascript. This programming language in Ethereum platform is used to write implementation script of smart contracts. After writing smart contract script using solidity, a complier called solc transforms the solidity smart contract code into bytecode, and then EVM interprets this bytecode. After running bytecode using EVM, compiled instructions are deployed on Ethereum blockchain.
- **Smart Contracts:** among all features of Ethereum platform, the main feature included in a 2015 version is smart contracts. Smart contracts created using the Ethereum platform allows blockchain application developers to implement a distributed applications of various types, to set any instruction in smart contracts including those that interact with other contracts and store data. In addition, it enables developers to prevent contract tampering by copying deployed smart contracts to each node. .in addition to solidity, some of common high-level programming languages used for writing smart contracts on Ethereum platform are Serpent and LLL (Vasin & Co,2015).Figure 6 represents an example of smart contract cryptocurrency transactions deployed by blockchain developers.

Figure 6: an example of smart contract for cryptocurrency transactions(Vasin & Co, 2015)

Bitcoin

Another blockchain platform which is designed based on the concept of cryptocurrency and used to handle only financial transactions is a Bitcoin. Bitcoin is a public blockchain network that is used to process a digital currency called bitcoins. Since Bitcoin blockchain is not a general purpose platform, it is not suitable for building any cross industry applications such as insurance system. In addition, since a block in bitcoin blockchain stores only small amounts of Meta data, this limited space and the low throughput and high delay of the Bitcoin network make it inappropriate for storing any significant amount of Meta data. The Bitcoin network specifically developed for running programs that detail transactions using the bitcoin cryptocurrency.

Hyperledger Fabric

Hyperledger is an open-source project hosted by The Linux Foundation that intends to expand the concept of blockchain so that it may be utilized in a variety of situations. One of the Hyperledger initiatives, Hyperledger Fabric, was originally contributed by IBM and attempts to address some of the open concerns of existing frameworks, such as Ethereum. Hyperledger Fabric is an open source architecture for creating permissioned (private or consortium) blockchains for use in industry, and it has many similarities and differences with Ethereum.Hyperledger has its own kind of smart contracts called chaincode. Chaincode programs, like Ethereum, are event-driven programs that run on the ledger and change the ledger's state when executed, allowing assets to be moved around. It's possible to compare this to a state machine.The language employed in the chaincode, however, is a significant divergence from Ethereum. Go is used to write programs, with support for other languages such as Java.The code is deployed using a Docker container and an isolated VM.The ability to construct smart contracts using general-purpose languages is a benefit and lowers the barrier to entry for using this framework as a blockchain. However, it creates the possibility that the code is non-deterministic, resulting in forks, which is why Ethereum utilizes a language that compiles and runs on EVM.

The way consensus works is another major distinction in the latest revised architecture of Hyperledger fabric, apart from the presence of permissioned channels. The definitions that follow relate to steps in the consensus process that are necessary to comprehend this mechanism.

- **Endorsement**: After verifying the transaction, some endorser stakeholder determines whether to approve or reject it. The endorsement is merely a transaction signature that validates the endorser's decision. Endorsement policies may stipulate that transactions must have a particular number of endorsers in order to be accepted.
- **Ordering**: All transactions collected over a given time period are bundled into a block, which is then sorted and committed in that order.
- **Validation**: Check if a transaction's endorsement policy is satisfied before determining whether the transaction transformation is valid.

Three types of nodes participate in the consensus process:

• Client - sends an endorsement transaction to the endorser nodes.

• Peer Node - peers establish a peer-to-peer gossip network, maintain the ledger's state, and manage the chaincode; they can be individuals or organizations.

– Endorser – simulates transaction execution before deciding whether or not to endorse. Endorsers are always committers as well.

• Orderer Node - the orderer nodes constitute an ordering service; this service employs a pluggable (changeable) protocol to order the transactions received from the peers, produce a block with them, and then broadcast this block to the committers.

The consensus workflow of Hyperledger is as follows in a simplified form:

The transaction is sent to the endorser nodes by the client.

2. Endorser nodes simulate the transaction before deciding whether or not to support it. If they do, they sign the deal and return the client's endorsement.

3. The customer informs the ordering service of his or her approval.

4. The ordering service collects incoming transactions, organizes them into blocks, and then broadcasts them in order to all peers (orderers and committers); the peers then evaluate the transactions and verify their endorsements, applying only those that meet the endorsement policy(Selimi et al., 2018)

R3 Corda

Corda is another open source private blockchain platform which is developed R3 financial institutions in 2015. Implementation of smart contracts in Corda platform enable institutions to directly transact any business transaction by removing costly frictions in business transactions. Additionally, since it is a permissioned blockchain platform, only authorized participants can join and access the data. Privacy can be enhanced by R3 Corda due to a permissioned mode property and also offers fine grained access control to digital records. Initially, Corda is designed to handle the financial transactions. Nowadays, we can apply corda for cross industries such as healthcare, trade finance, supply chain, and government authorities. In recent years companies like Intel and Microsoft are using Corda as a blockchain platform. Table 4 shows a summary comparison of most common blockchain platforms used.

Table 4: Comparison of most common Blockchain platforms used: adapted from(Sharma & Negasa, 2020)

Property	Bitcoin	Ethereum	Hyperledger Fabric	R3 Corda
Application areas	Can be used for Financial Transactions	Can be applied for any industry	Can be applied for any industry	Cross industry
Blockchain Type	Public	Public	Private	Private
Access	Read/write for anyone	Read/write for anyone	Read/write for single organization	Read/write for multiple selected organization
Privacy	No	No	Yes	No
Efficiency	High	High	Low	Higher
Security	Proof of work(Pow)	Proof of work(Pow)	Pluggable Framework	Pluggable Framework
Smart contract	Yes	Yes	Yes	Yes
Governance	Bitcoin developers	Ethereum Developers	Linux Foundation	R3 Consortium

2.7.The Application of Blockchain

The implementation of blockchain is going to have a transformative effect on some use case applications. The first blockchain, bitcoin, was developed to enhance the system for financial applications, due to its transparency as a result of its decentralized principle.Later, more varied

uses of blockchain were developed for financial applications, such as smart contracts, insurance and crowdfunding. Furthermore, as many people are interested in this new technology, the application of blockchain also currently being developed widely for non-financial services like voting systems for governmental affairs. In this regard, we could divide the use of blockchain into two sectors: financial and non-financial services.

2.7.1. Financial Applications

- **Digital Payment System**

This is essentially bitcoin's primary purpose as a digital currency.The introduction of bitcoin ushered in a shift in and disruption of traditional payment systems run by banks and other financial institutions. A digital currency plan combines a new decentralized payment system and a new money into one package. All of the schemes have a publicly available ledger that is shared over a network of computers. The procedure through which users agree on modifications to the ledger (that is, which transactions are approved as genuine) is a major defining characteristic of each digital currency scheme(Sharma & Negasa, 2020).

- **Smart Contract**

A smart contract is a computer application that can perform Commercial transactions and agreements automatically. It also enforces all parties' contractual commitments without the need for an intermediary. A smart contract also allows asset owners to pool their resources and form a corporation on the blockchain, with the articles of incorporation encoded in the contract, precisely defining out and enforcing those owners' rights. Managers' decision rights may be defined in associated agency employment contracts by coding what they could and couldn't do with corporation resources without ownership approval.

- **Insurance**

Blockchain may be used to record any valuable item or property that is impossible to duplicate or destroy. It has the ability to verify ownership and track transaction history. Everledger is a corporation that keeps track of diamond certificates in the form of a permanent ledger. Height, width, weight, depth, hue, and other attributes that uniquely identify the diamond are hashed and recorded in the ledger.

- **Crowdfunding**

Currently, a growing number of companies are using cryptocurrency tokens and blockchain technologies to raise funds for their businesses. The concept is to use blockchain technology to enable crowdfunding sites, eliminating the requirement for a third-party intermediary like Kickstarter or Indiegogo. The firms then raise funding by inventing their own digital currency and offering early backers "cryptographic shares"(Arenas & Fernandez, 2018). In a crowdfunding campaign, investors are given tokens that reflect shares in the firms they are supporting.

2.7.2. Non-Financial Applications

- **Decentralized Governance Services**

The most common application of blockchain in governance is as a notary public. The use of blockchain in notarization protects the document's privacy as well as the privacy of individuals seeking certification. Notary timestamping is taken to a new level by publishing proof of publication using the cryptographic hashes of files in the blockchain(Alpár & Jacobs, 2013). Even the Estonian government, in collaboration with Bitnation, the world's first blockchain-powered virtual country, will begin providing e-residents with a public notary service(Alpár & Jacobs, 2013). The online voting system, often known as e-voting, is another type of governance service that uses blockchain. A central authority is usually in charge of recording, managing, counting, and verifying votes. By allowing voters to keep a copy of the voting record, blockchain-enabled voting (BEV) empowers individuals to perform these duties on their own. Because other voters could see that the record differs from theirs, the historic record could not be modified. Other voters would be able to analyze whether votes were compliant with the criteria, maybe because they had previously been tallied, or because they were not associated with a genuine voter record(Gervais et al., 2016). Illegitimate votes could not be added. In this approach, blockchain technology could help government institutions become more transparent.

- **Decentralized Storage**

In the health and music industries, this approach has been utilized. Blockchain provides a mechanism for storing health data or electronic medical records (EMRs) on the blockchain so that they may be examined while remaining private, with an embedded economic layer to reward for data donation and use(Gervais et al., 2016). Personal health records might be encoded as digital assets and placed on the blockchain like digital currency, taking advantage of the pseudonymous identity programmed into a digital address and its guaranteed privacy

mechanism. On the music industry, on the other hand, blockchain was used to create a comprehensive and accurate distributed database of music ownership rights data in a public ledger. In addition to ownership rights information, smart contracts(Gresch et al., 2019) were used to determine the royalties split for each work.

- **Decentralized IoT**

The use of IoT also poses a number of significant obstacles. One of these is related to the client/server paradigm, which is a centralized ecology. While this architecture has been connecting generic computer devices for decades and will continue to serve small-scale IoT networks as they exist today, it will not be able to meet the expanding needs of future IoT ecosystems. Because of the significant infrastructure and maintenance costs involved with centralized clouds, massive server farms, and networking equipment, existing IoT solutions are costly. It will significantly reduce the costs associated with installing and maintaining large centralized data centers by using a standardized peer-to-peer communication model to process the number of transactions between devices. It will also distribute computation and storage needs across billions of devices that make up IoT networks. IBM has created ADEPT (Autonomous Decentralized Peer To Peer Telemetry), a platform that exploits components of bitcoin's fundamental design to create a distributed network of devices, or decentralized IoT, in collaboration with Samsung.

- **Blockchain in Education**

The blockchain technology has been described as a disruptive technology with the potential to alter the banking and commerce industries. However, in order to realize its educational value, it is necessary to first comprehend its characteristics. The blockchain at the heart of the Bitcoin digital money system is the most well-known, but not the only, blockchain. The ‘distributed consensus' approach is used to determine whether a new block is valid and should be added to the chain. Each block in the blockchain can hold a tiny amount of data (usually up to 1 MB), which could be any material that needs to be kept secure while still being spread. These cash transaction data could be exam certificates or learning records. This data is kept for all participants and may be accessed by anybody with the cryptographic "public key," but it cannot be changed, even by the original author. The data records are timestamped, ensuring a reliable and accurate record of the new information(Baum, 2014).

• **Education Market Analysis**

The worldwide education market is worth $4.4 trillion and is expected to continue to rise. According to a 2015 survey, this market is growing at a rate of over 50% each year in nations like China, India, and Malaysia. Harvard, Yale, and Stanford, three of the top colleges in the world, account for roughly $70 billion, with an average undergraduate tuition of $45,000 and a professorial salary of $200,000. In 2015, the top 100 colleges in the world had an endowment of roughly $433 billion(Baum, 2014).

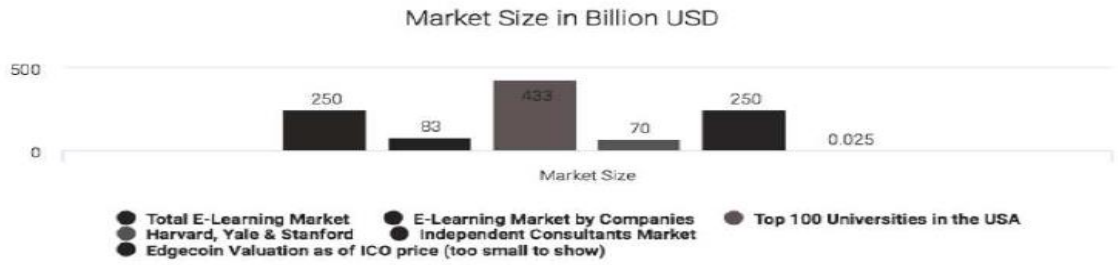

Figure 7: Education market(Baum, 2014)

The Blockchain has the potential to increase educational institutions' ability to support teachers, disseminate knowledge to parents and community members, enable new learning systems, and expand and provide learning opportunities for more students. There are several applications and benefits of blockchain technology in the field of education:

- **Online Education**

Online education, often known as distance learning or electronic learning, is a method of delivering knowledge and facilitating learning that makes use of data and internet technology. A web-based learning technique is what it's called. With the invention of blockchain, a perfect answer to online learning challenges such as legitimacy and protection will be available. Without the requirement for third-party oversight, the Blockchain will also establish non-modifiable learning papers for online education, guaranteeing that course credits are properly acknowledged.

- **Student records**

Academic transcripts are one of higher education's most time-consuming and labor-intensive processes. Before a certified record of a student's grades is available, each entry must be manually scrutinized for legitimacy. Another sort of student record that is frequently requested is course content certification. For each student who requests this record, each sheet should be

signed and stamped (to ensure accuracy). A person could acquire an accurate, authorized record with just a few clicks if material courses and academic successes were maintained on a blockchain .

- **Diplomas and Certificates**

Diplomas and certificates for pupils, similar to grades, could be supplied and maintained on a blockchain. Instead of requiring the agency that granted the diploma to certify a physical copy, employers will need to be directed to a digital certificate. It's also in the works. Because the majority of educational credential administrations are unable to ensure the confidentiality and reliability of student data. Although adopting Blockchain to address trust issues could be a viable solution, it does have limitations that limit its widespread adoption. Blockchain [26] has a low throughput and access time. It prevents users from presenting fraudulent degrees or certificates to potential employers or higher education institutions. Because of ineffective third-party agencies, online education certification is currently a challenge. The academic certificate or document verification system provided by blockchain is a straightforward and fast method of certifying learning outcomes. Even if a student's certificate is lost, it may be feasible to verify it. To protect the data's security and authenticity, the blockchain employs an asymmetric encryption mechanism in cryptography.

2.8. The Challenges

Blockchain is one of an emerging technology that disrupts the way services provided by many companies and facing multiple challenges. However, nowadays blockchain technology is adopted in many enterprises and can be used for conducting any business transactions executed in a company. There are common challenges in adopting this technology for cross industries. In this section, common challenges responsible for slow adoption of Blockchain technology are discussed .

- **Performance**

When a transaction is being processed, a blockchain has to perform the same tasks a regular database does, but it carries three additional burdens as well :

1. **Signature verification**. Every blockchain transaction must be digitally signed using a public-private cryptography scheme. The generation and verification of these signatures is computationally complex. By contrast, in centralized databases, once a connection has been established, there is no need to individually verify every request that comes in.

2. **Consensus mechanisms.** In a distributed database such as a blockchain, effort must be expended on ensuring that nodes in the network reach a consensus. Depending on the consensus

mechanism, this might involve significant back and forth communication and/or dealing with forks and their consequent rollbacks.While it is true that centralized databases must also contend with conflicting and aborted transactions, these are far less likely where transactions are queued and processed in a single location.

3. **Redundancy.** This is not about the performance of an individual node, but the total amount of computation that a blockchain requires. Whereas centralized databases process transactions once (or twice), in a blockchain they must be processed independently by every node in the network, meaning that far more work is done to achieve the same end result.

- **Scalability**

Scalability is one of major blockchain adoption challenge for cross industries. An increase in number of transaction executed in blockchain often leading the blockchain network to become weighty. For instance, the current Bitcoin blockchain storage exceeded 200 GB(R.best,2020). In blockchain network, new transaction is stored in blocks before validation process is executed. By considering number of transactions executed per second as a comparison factor, blockchain networks are much slower than centralized system. For instance, Bitcoin can process 3 to 7 transactions per second. This is mainly due to the original restriction of block size and the time space used to create a new block(R.best,2020).since the capacity in which each blocks have in blockchain is extremely small, various small types of transactions are forced to be postponed as all miners want large transactions with more transaction payment. On the other hand, the use of block with large size can reduce the propagation speediness and direct to branches of blockchain. This poor performance as compared to centralized system can be one of main reason for slow adoption of blockchain technology for companies that process large-scale of data. Therefore, scalability is relatively strong problem.

- **Privacy**

The blockchain network by most people is considered as secured technology that allows users to make transactions with hash signature address instead of real identity. although, a blockchain network can protect a certain level of privacy by using public and private key, a public ledger of transaction is transparent and accessible for every participating users in that network. In addition, each user or node has a copy of public ledger even in private blockchain. For instance, private blockchain is more secured as compared to public blockchain but it does not provide privacy of transactions. Privacy is one of essential feature in many business applications and for enterprises that have sensitive data (for example, trade secret). This public ledger used in

blockchain technology needs to be modified in a way that permits only restricted access by users who are authorized to view it.

- **Lack of Standardization**

The other challenge of blockchain network is lack of standardization. Nowadays, even though there are broad diversity varieties of blockchain networks exist, there are no worldwide standards for running blockchain applications. Having standardization can help in developing more efficient consensus mechanisms used in blockchain platforms and also used for reducing cost required for running blockchain applications. Lack of standardization for blockchain applications is one a difficulty to entry for developers and companies.

- **Consumption of energy**

In a public blockchain, producing PoW blocks costs a lot of processing power and, as a result, a lot of electricity. The computer power is just for this operation, and the findings have no other use than to advance the blockchain.

2.9. Blockchain for Degree Fraud Detection and Verification

Verification of applicant academic certificate or document is a regular and routine process for the employer that offers employment. The employer in most recruitment process takes more time for giving offer letter for qualified and selected applicants for the job even the interview process gets over. The reason behind this is due to the longest time required to verify the applicant certificate. Employer must contact the central certificate issuing authority to verify the originality of the certificate and this process needs extended time to complete recruitment process. the solution for such problems is a decentralized, verifiable and tamper proof blockchain based academic certificate or document storage that can be suitable for third party activities such as authentication or verification of certificate. This can be a perfect solution for degree or academic certificate forgery problems.in addition, blockchain based academic certificate system can maintain transparency of academic documents than can bring convenience for certificate owners(student, trainee) and employers.

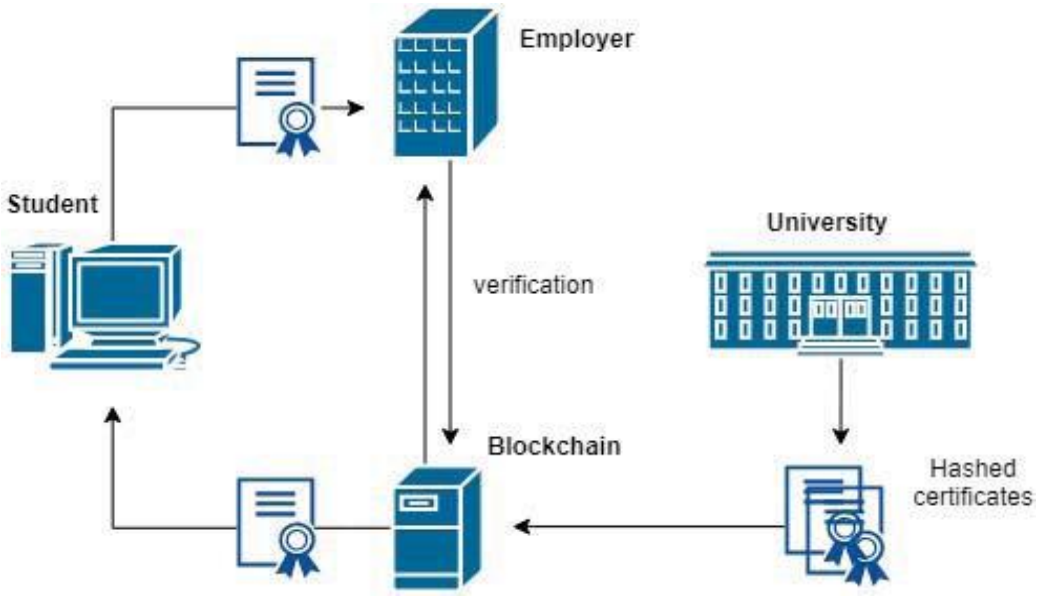

Figure 8: Block diagram of Blockchain based academic certificate verification system(Juricic et al., 2019)

The above figure depicts general blockchain based certificate verification system that is used by Academic institutions or universities, students and potential employers. As shown in figure, any blockchain based certificate verification system mainly contains four components namely; university, employer, blockchain and student The University or academic institution can perform activities such as issue student certificate, hashes certificates and storing hashed value of issued certificate on the blockchain database. Potential employers use this hashed value of certificate to search and verify applicants' academic document directly from blockchain database without any intermediary authority for example issued university or academic institution. Without a central authority or issued university, a student can have a direct access to his own records at any time from blockchain database.

This design has advantages in storing all different types of academic achievement documents in blockchain database while other systems that allows only storing certain kind of academic credentials.For instance, one of practices of academic certificate verification system supports just storing university level achievements. In this architecture, there is no component that depicts how to verify the genuine of academic institution or issued authority. In other words, this system allows employers to validate the genuineness of the certificate without verifying the authenticity of the certificate issued authority. on the other hand, EduCTX(Turkanović et al., 2018) contains a network of official academic document authorities and this academic

certificate authorities can verify the genuine of certificate issuer so that only trusted academic institutions upload and store academic certificates on blockchain database.

2.10. Review of Related Works on Academic Degree Fraud Detection and Verification Using Blockchain

Blockchain technology is an emerging technology and studies on this technology are still very new and expressions of these on the education areas are at the beginning of the age. Since reviewing previously executed blockchain based certificate systems can be important to have a better knowledge about the state of art development status of adopting blockchain technology for academic certificate verification systems around the world. as of studied, some previously developed academic certificate verification systems are already deployed and used in real life(Juricic et al., 2019; Turkanović et al., 2018) and some of them are still in prototype(Arenas & Fernandez, 2018; Sharma & Negasa, 2020).this blockchain based certificate verification systems tried to integrate advantages of the blockchain technology's abilities such as consistency, usability, persistency, security, privacy and access control of academic data.

In this section of the study, some of recent works done on certificate verification using blockchain technology will be discussed. In the first part of this section, some of blockchain based academic certificate verification solutions are explained in detail. Then the comparisons of this recent works are summarized in Table 5. Even though the main goal of these systems is to design and develop more secure and efficient academic document verification system, but they have used different approaches.

A study that proposes a multichain permissioned blockchain platform that implement a specific educational use case for decentralized verification of academic qualifications. The researcher has designed a blockchain based system that can store solid data proofs of digital academic diplomas in blockchain ledger. The authors recommended developing academic credentials verification system that can provide privacy of academic awards and scalability that are easily verifiable and present an opportunity for third parties such as employers to independently verify without central academic proofs(Turkanović et al., 2018).

Another proposed permissioned blockchain-based system allows institution to securely and dependably transfer and verify academic records when the request received from the student. The implementation of proposed system is done by using Hyperledger Fabric blockchain platform. The proposed solution consists of a web application used for executing user requests and Hyperledger Fabric blockchain to store the hash of the records on the blockchain that can be used for verification. this research work proposed a system that can verify academic

documents or certificates and this work can be extended in future by adding automation that can completely eliminate manual efforts and can be integrated with academic institutions application systems to reduce user interaction. In addition, this study can be extended by adding functionality which allows academic institutions to upload transcripts in mass (Badr et al., 2019).

The other Researchers addressed the problem related to academic certificate by developing a distributed blockchain based academic certificate verification that can be used to validate the authenticity of issued certificates. In the first stage of the research authors developed a prototype to register academic institutions, students and empoloyers.in the second step, the proposed system register and store the issued certificate by academic institutions on the blockchain database. This allows any third party for example, employer to verify the authenticity of a certificate independently without central authority or academic institution. The proposed system has not yet examined on how the validity of documents on the blockchain is verified and in future research this needs to be addressed(Curmi & Inguanez, 2019).

Another study designed and developed a prototype implementation to the UZH institution located in Switzerland. The proposed system stores and verifies academic credentials issued by faculties of UZH institutions. In this research work, the authors first determined the requirements of the universities stakeholders that can be important to create the initial prototype used to demonstrate the functionalities. The proposed architecture contains three components namely, issuer requirements, recipient (graduate student) requirements and companies that verify a diploma. The proposed system only used to verify diplomas issued by UZH institution located in Switzerland. Further study needs to be conducted that can include all universities and institutions across the world (Gresch et al., 2019).

Other researchers suggested a novel framework used for making an environment in which individuals can protect their academic credentials and as well as share academic records with others. In this framework, the researcher tried to incorporate the advanced features of blockchain which enables academic instititution to issue academic transcript that can be used to as a verification of success. In addition, this novel framework can offer the equivalent utilities for the after academy education. The proposed framework includes blockchain features like transparency, privacy which is implemented using smart contract, security and access control features(Han et al., 2018).

The other study designed and implemented a blockchain based educational framework that can be used by academic institutions and potential employers or companies. The proposed framework enables potential employers to verify academic credentials and credits of courses

taken by a student registered in academic institution. In addition, the proposed system allocates tokens when a student successfully completed courses. In the proposed system, each transferred credits represented as transactions and stored in blockchain blocks after mining process is completed. This work can be extended by including credits from MOOCs by online platforms without distribution of hard-copy certificates to student address (Srivastava et al., 2019).

The other researchers proposed a blockchain based technique for academic certificate verification that can maintain low latency and high throughput. The proposed technique provides a method that can be used to reduce query processing time. The proposed technique builds a tree structure that enables an efficient query for a transaction and also maintains historical transactions query of an account. The proposed tree structure called MPT-Chain requires short time to modify blocks and can also enable to speed up block verification.

One of the studies designed a blockchain based system that can be used to record all academic credentials achievements. This proposed framework enables students to present academic accomplishments to companies through trusted system. In addition, this platform can provide ability for a student to plan for their future achievements by enabling students to review their learning throughout their career, giving them academic advisors or supervisors or potential employers. In addition the proposed system can facilitate students enrolled in academic institutions by increasing their extra-curricular activities and progress nonacademic skills. Furthermore, proposed system can make easy communication between companies or potential employer, students and academic institutions (Awaji et al., 2020a).

Another study proposed a two stage blockchain based educational framework that is used for employment and skill certification. At the first stage of proposed system, new blocks are created after verification process of educational certificate by trusted organization is completed. In the second stage, the authors employed game based incentive mechanism called Vickrey-Clarke-Groves (VCG) that can be used to support the verifiers to join in the skill verification process. The authors included theoretical proofs and extensive simulations that can be used to show valuable properties and competence of proposed system(Liyuan et al., 2019).

Another study designed and implemented credit based a global higher education platform called EduCTX. This platform is developed by considering the European Credit Transfer and Accumulation System (ECTS). The proposed platform contains a worldwide trusted, decentralized and distributed higher education credit and grading system that enables a student integrated viewpoint for students, universities, potential employers or companies. As a proof of concept, the researchers developed a prototype using hybrid Ark Blockchain.Platform.in the

future, this work can be extended by developing EduCTX platform that uses smart contracts and suitable platform of the blockchain technology (Turkanović et al., 2018).

Several issues in the current higher education credit assigning, recording and presenting system have recognized by authors and they have tried to solve with EduCTX platform. In general, students' completed courses are recorded in a certain data structure in the databases hosted in the data centre of the Higher Education Institute (HEI) which raise several issues, interoperability, transparency, inaccessibility, and difficulty to share the records securely. The proposed system records all information of each completed courses in the blockchain. In addition, unlike(Juricic et al., 2019), EduCTX consists of network of certificate authorities, existing certificate authorities in the network ensures that only the genuine certificate authority can issue certificates.

Another study proposed a blockchain based model to verify and lock document that can enable the document issuer to store digital documents on blockchain database. The proposed system also allows companies to verify the issued document stored in blockchain database.The proposed model is not yet evaluated and is not addressed exchange of academic transcripts between universities. In addition, further study needs to be conducted that allows verification of all kind of documents (Sharma & Negasa, 2020).

Table 5 describes a comparison of related works by using some common desirable characteristics of blockchain based applications. Smart contract column used to distinguish systems that are implemented smart contract with no smart contract. In transparent blockchain system, the academic data recorded by each node and distributed among other connected nodes is visible. Privacy of personal information is concerned with access control related to the use of academic records. If the system is scalable it must be able to support the rising number of academic institutions, students and academic records. In certificate revocation if certificate is canceled, the revocation information should be efficiently and rapidly disseminated to all participants in blockchain network. In consensus based system, new blocks can be added or changes can only possible when majority of nodes in blockchain network reaches on some consensus. Blockcerts can be a common practice for blockchain based digital certificate verification.blockcerts platform allows any users to issue, share, display and verify digital certificates of academic and non-academic achievements. The system is developed in MIT lab and stop fraud and supports to manage wide variety of qualifications. This system is already deployed by MIT and can enable to issue certificates for some achievements(Juricic et al., 2019).

Another practice in digital certificate verification is the EduCTX. It is based on the concept of European Credit Transfer and Accumulation System (ECTS). This system uses blockchain technology to create ECTS based credit assigning and recording system. As studied, in most of current blockchain based architectures, a mechanism for checking genuineness of issuer are not addressed.

Table 5: Comparison of related works on Degree Fraud Detection and Verification

Author	Blockchain platform	Smart Contract	Transparent	Privacy of personal information	Scalable	Certificate revocation
(Awaji et al., 2020b)	Ethereum	Yes	Yes	Yes	no	yes
(Curmi & Inguanez, 2019)	Ethereum	Yes	Yes	No	no	no
(Liyuan et al., 2019)	Ethereum	Yes	Yes	Yes	no	no
(Badr et al., 2019)	Hyperledger Fabric	No	No	Yes	yes	no
(Gresch et al., 2019)	Ethereum	Yes	Yes	Yes	yes	no
(Arenas & Fernandez, 2018)	Multichain	No	No	Yes	yes	no
(Han et al., 2018)	Ethereum	Yes	Yes	Yes	no	no
(Turkanović et al., 2018)	ARK	No	Yes	Yes	no	no
(Srivastava et al., 2019)	Ark	No	Yes	No	yes	no

2.11. Blockchain-Based Document Verification Applications and Platforms

Studies on blockchain technology are still in their infancy, and educational reflections on it are only just getting started. Reviews of existing blockchain-based certificate systems provide valuable insight into the present state of development for blockchain-based certificate systems around the world. Although some are still in the prototype stage, others have gone live and issued certifications using their systems. Previously proposed blockchain-based certificate verification systems attempted to take advantage of blockchain technology's capabilities to deliver academic data with consistency, usability, immutability, security, privacy, and access control. This section analyzes and contrasts some applications and platforms launched to store the academic records,

certificates and diplomas. First, we'll go through blockchain-based practices for academic data. According to(Saleh et al., 2020), Certain key security themes must be addressed by a blockchain-based academic document verification system, including Authentication, Authorization, Confidentiality,Ownership and Privacy of academic Document.

In authentication,sers must be authenticated via the blockchain. Students, universities, institutes, employers, and other users are among the users in this case. For accessing the certificate held on a blockchain ledger, each user will be verified. Users can be authenticated using a username and password, or a combination of authentication methods such as biometrics. For example, if an employer wants to check a certificate, he or she must first join the blockchain, and the receiver must then enable the employer to read and verify the certificate.authorization allows users to perform transactions on the blockchain with the permissions they need. For example, a student may share his or her certificate with a potential employer. After the certificate has been granted, the issuer will give the student complete control over it. The system must authorize all of these actions and functions.the standards for confidentiality include the student's personal information, which can be kept confidential by both the academic establishment and the student. In this situation, the student has the authority to disclose information to third parties (employers) for verification purposes.

The users in the blockchain ledger own a digital certificate. The receiver of an educational certificate owns the certificate entirely. The use of public and private keys is critical here, and they must be shared by all blockchain users(Moore, 2009).in order to keep privacy, public keys are anonymously preserved. The usage of cryptographic techniques, as well as the creation of hash functions, is essential.

To guarantee that the certificate is not a forgery, the aforementioned themes must be addressed. Employers can look up a student's credentials on the blockchain and verify them.Table 6 summarizes this current research in terms of common security themes required for academic credential verification systems. Although the goals or expectations of these systems are similar in that they want to create a digital certificate platform or ecosystem to make the certificate system more safe and efficient, they have distinct methodologies and focus on the challenges they want to tackle. To give recipients more influence over the certificates they acquire, the MIT Media Lab employs Blockcerts to deliver digital certificates to groups of students. This effort's beneficiaries might not need to rely on a third-party mediator to store, verify, or validate credentials. According

to MIT's certification architecture, the issuer signs a digital certificate and stores its hash within a blockchain transaction.

The receiver is allocated to the output of this transaction. Because MIT needed to distribute certificates based on user-created key-pairs for their graduation and workshop participation certificates, there was a difficulty with ownership in this endeavor. This strategy also demands a great degree of confidence. Another important factor to consider is privacy, as data can be viewed by anybody and certificates are only useful if they belong to a single person. The issue here is that the recipient may be able to share the certificate with one company while being unable to keep it hidden from another, as is required. The hashing technique is used when an employer has to verify the legitimacy of a certificate while also releasing both the certificate and the hash of the certificate stored in the blockchain. In this situation, the notion of privacy isn't properly achieved. Blockcerts, an open standard, is being used to construct apps that certify blockchain-based academic credentials, professional certificates, and other credentials in a separate project. Blockcerts is built on the self-sovereign identification of all participants by allowing components to generate, issue, review, and validate certificates in the blockchain. Blockcerts lacks an independent verification mechanism to confirm the validity of certificates stored on the blockchain, although they are tamper-proof. As a result, it's possible to spoof the certificate. Furthermore, because the system has no registration process, any issuer can send certificates to recipients, who can then offer any bitcoin address, privacy and security problems persist. To establish ownership of a certificate, both the issuer and the recipient must provide public addresses. Blockcerts does not certify the mapping of public keys to individuals or organizations (Blockcerts). SmartCert is another blockchain-based digital credential verification solution. SmartCert is a blockchain-based solution for confirming the integrity of academic qualifications and combating certificate fraud. SmartCert uses digital signing of educational certificates to ensure transparency in the recruitment process. The student will give the hash to a potential employer to verify the certificate. . However, because the machine viewing the data could be attacked by an intruder, a genuine user may have difficulty obtaining access to a hash or digitally signed certificate. Another challenge with this application is that cryptography does not ensure privacy. Records Keeper is another blockchain-based option for certifying academic degrees. RecordsKeeper can be used by educational institutions to issue certificates and send the user a receipt that can be shared with a third party to validate the certificate's authenticity. Using the receipt obtained from the student, the third party will authenticate the certificate's authenticity in the Records Keeper ledger. This method has minimal flaws, but parties that want to

read a certificate on the Record Keeper blockchain must possess it. This is essentially a transfer of ownership to a third party that could be tampered with. This could be useful for encrypting data on a private blockchain. Table 6 summarizes current approaches and highlights their major shortcomings and security themes addressed by each study.

Table 6: Summary of practices on Blockchain based Document Fraud Detection and verification

Study	Among the features were	Shortcomings	Essential Security Themes addressed
Blockcerts	Platform with an Open Standard	There is no separate verification service available. Spoofing attacks are possible.	No Security theme addressed
Smartcert	Fake Certificates are no longer an issue. An employer receives hash from a student.	Attacks are a possibility. Basic information security precautions are required. There is no apparent way to verify the parties' validity.	Authorization, Ownership
Records Keeper	In the certificate, there is proof of authenticity. The entire verification process is built around the concept of ownership.	Vulnerability to certificate manipulation After establishing ownership, participants can verify.	Authentication, Ownership
MIT Media Lab	Students have more control. Digital keys are used.	There is a lack of trust. Everyone has access to the certificate. There is no apparent technique for verifying the authenticity of parties.	Authorization, Ownership, Privacy
UNIC	Resolve the issue of phony certificates Integrity, privacy, and ownership are all positive attributes.	Requirements for a company to verify a certificate are insufficient.	Ownership, Privacy

CHAPTER THREE

ACADEMIC DOCUMENT ISSUES VALIDATION AND REQUIREMENTS ELICITATION

3.1. Overview

Expert opinions in an area can be extremely useful for research in order to make significant contributions to that field. Interviewing students and experts (for example, registrar officials) in a formal setting would be the best method to validate the issues raised in the Academic Document. Because expert knowledge was still required, it was decided that a survey and interview would be a more efficient way to acquire opinions and results.

Prioritizing degree fraud issues and updating the underlying systems is one way to approach them. The blockchain distributed architecture, which allows for the immutable and secure storing of academic credentials, appears to be a suitable solution. This could be a useful technique to obtain document traceability, possibly leading to the verification becoming totally digital and automated. The goal of this study is to determine the scope of academic document difficulties in Ethiopia and whether blockchain technology may help solve them. As a result, the premise is that blockchain systems could be a good fit for Ethiopian Academic Document Verification. A survey and interview were done to validate the concerns with academic documents and elicit requirements for a document verification system. It was able to propose and develop a prototype implementation of a blockchain architectural solution utilizing these criteria, with the goal of determining whether the gathered needs are practical to achieve.

This chapter examines the survey and interview's purpose, methods, and results.The survey and analysis performed here also formed the basis for the requirements used to create a proof of concept prototype.However, due to time limitation and budget only three universities were used for the survey and interview: Adama Science and Technology University, RiftValley University, and Admas University.since all problems related to paper certificate are common to all students found in Ethiopia,we believe that survey and interview conducted in those three mentioned universities can be used to identify problems and elicit requiremements of academic document verification system.

3.2. Survey

The survey was disseminated to graduate and undergraduate students at three universities: Adama Science and Technology University, RiftValley University, and Admas University.The surveys were delivered to graduate and undergraduate students. The questions were broken into two parts when the participants agreed to take part in the questionnaire. The first section consisted of generic questions about issues participants may have had with their certificates/diplomas after graduation. The second portion focused on the participants' level of understanding of Blockchain technology and their opinions on using it to issue and manage certificates and diplomas. We discovered the issues that students may experience after receiving their certificates/diplomas as a result of this study. We asked the participants a set of questions to see whether they had any adverse experiences with their certificates/diplomas being lost or damaged. We also calculated the percentage of participants who would have preferred an electronic version of their certificates or diplomas.

3.2.1. Purpose and Target

The purpose of conducting survey in this study was to investigate into the issues that arise when students graduate with paper certificates and diplomas. A number of accurate and valid scales were used in the survey. The survey was sent to three Ethiopian university students, and 4325 people of diverse ages, genders, educational levels, and majors agreed to take part in the study. The table below details the demographics of the participants.

Table 7: Demographic Information

		Number of Participants	**Percent**
Gender	Male	2356	54.8
	Female	1969	45.2
University	Adama Science and Technology University	521	12.0
	RiftValley University	2815	65.1
	Admas University	989	22.9
Degree Level	Graduate Students	1280	29.6
	Undergraduate Students	3045	70.4
Field of Study	Computer Science	703	16.3
	Accounting and Finance	318	7.4
	Business Administration	356	8.2
	Mechanical Engineering	228	5.3
	Public Health	178	4.1
	Clinical Nursing	224	5.2
	Information Systems	578	13.4
	Software Engineering	636	14.7
	Psychology	335	7.7
	Surveying Engineering	769	17.8

Age	16-24 years old	2035	47
	25-36 years old	1790	41.4
	36-50 years old	422	9.8
	Above 50 old	78	1.8
Year of Graduation	Before 1-5 years ago	3235	74.8
	Before 6-10 years ago	651	15
	Before 10 year ago	439	10.2

The survey's questions can be generally divided into three categories. Each group contains a set of questions that are similar but serve a different goal.

- **Question Group 1:A Focus on Four Paper Weaknesses**

In this survey Question group, we looked at four scenarios that students can encounter after graduation: loss, damage, late issuance and duplication. Participants' replies to questions about their credentials and diplomas were analyzed using descriptive statistics. in the first scenario,18.7 percent of participants said yes, while 81.3 percent said no to lose their diploma as shown in figure 9.

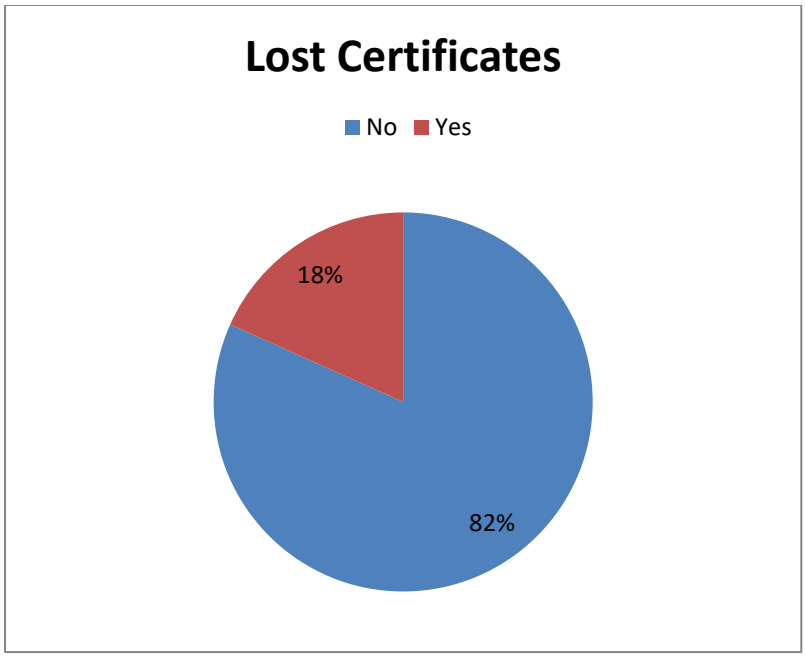

Figure 9: Lost Certificates

In the second Sceanrio,the findings revealed that 32.3% of participants said their paper certificates/diplomas were damaged, whereas the majority (67.7%) said their certificates/diplomas were not undamaged as shown in figure 11.

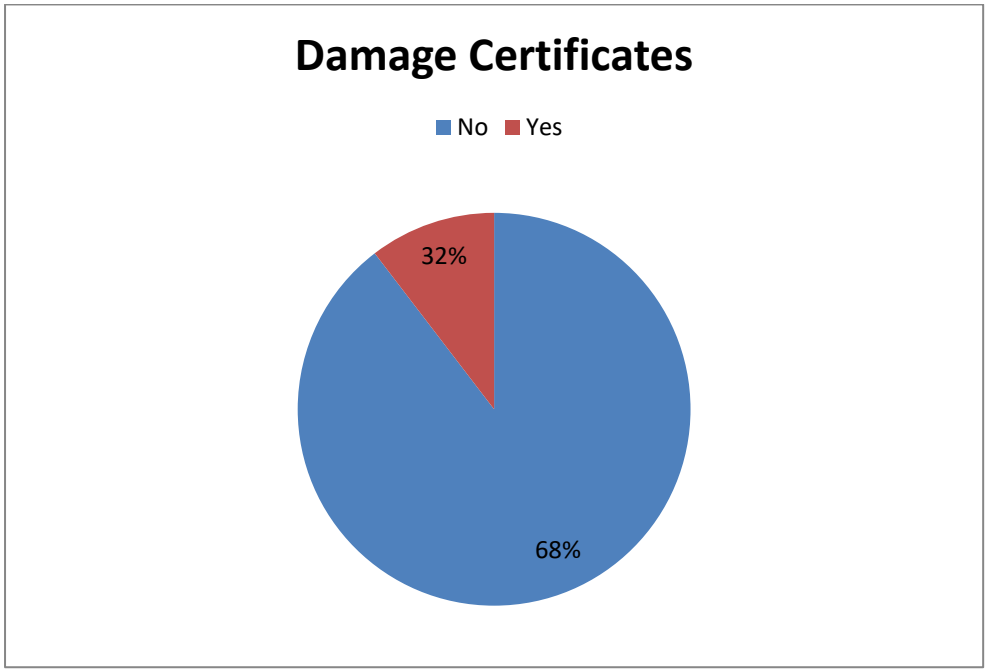

Figure 10: Damage Certificates

In terms of late certificate/diploma issuance, 64 percent of participants said they had problems getting their certificates/diplomas, while 36 percent said they didn't have any problems getting their certificates/diplomas.

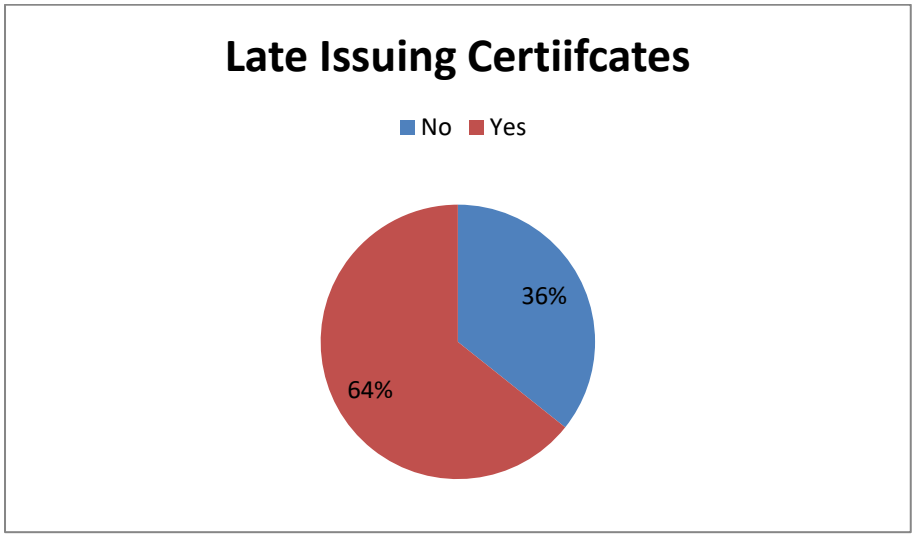

Figure 11: Late Issuing Certificates

15.8 percent of participants said they had issues obtaining duplicate certificates/diplomas if the original copy was lost, while 84.2 percent said they didn't.

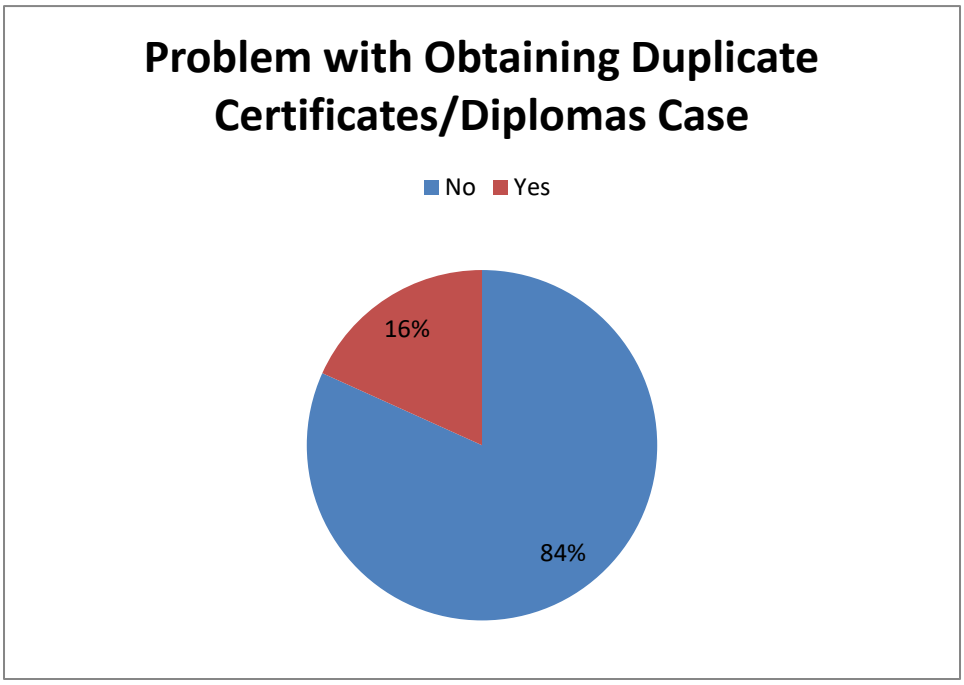

Figure 12: Problem with Duplicate Certificate

- **Conclusions from Question Group 1**

We found that the students had issues with their certificates/diplomas when they are based on paper in all four scenarios. As a result, up to 36% of the participants in each case were given negative responses.

- **Question Group 2: Academic Document Storage Related**

Participants are asked how many paper certificates or diplomas they had received. The majority of participants (61.3%) have one paper certificate/diploma, 25.9% have two paper certificates/diplomas, and 12.8% have multiple paper certificates/diplomas, according to the findings. The participants were then asked where they generally stored their paper certificates/diplomas; the majority (83%) said they kept them at home, 17% said they kept them somewhere else. These findings can be seen in the pie chart below.

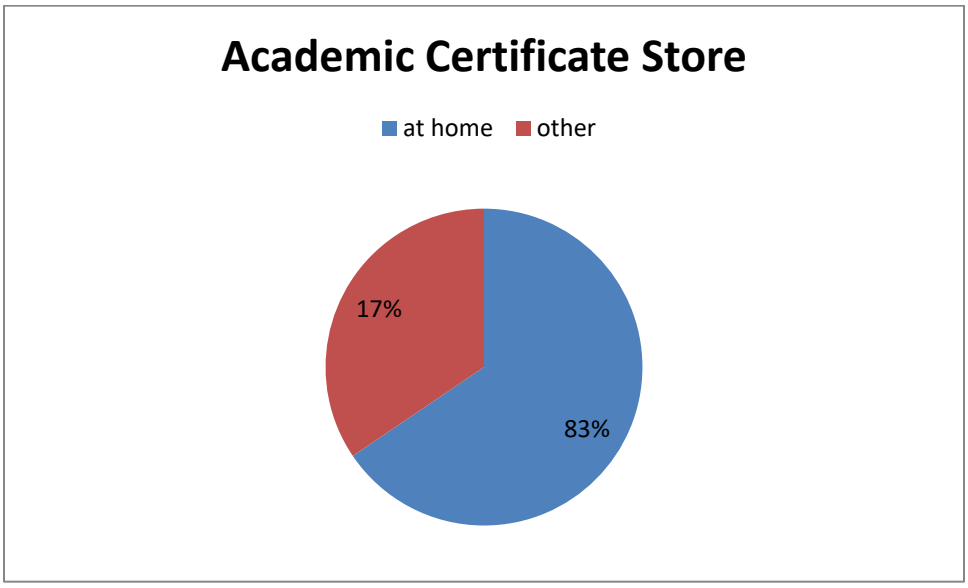

Figure 13: Academic Certificate Keeping location by Participants

The second question is to determine preferences for certificates/diplomas, participants were asked two questions: do you prefer electronic certificates/diplomas or paper certificates/diplomas? According to the study, 14 percent of participants prefer electronic certificates/diplomas, while 12 percent prefer paper certificates. The majority of participants (74%) preferred both electronic and print certificates and diplomas. The second question is raised for those respondents which prefer electronic certificate. Do you prefer blockchain technology to keep certificate or the current centralized system? 62 percent of respondents do not know blockchain technology and 10 percent respondents prefer blockchain technology for electronic document and the remaining 28 percent of respondents prefer the current centralized database for their electronic certificate.

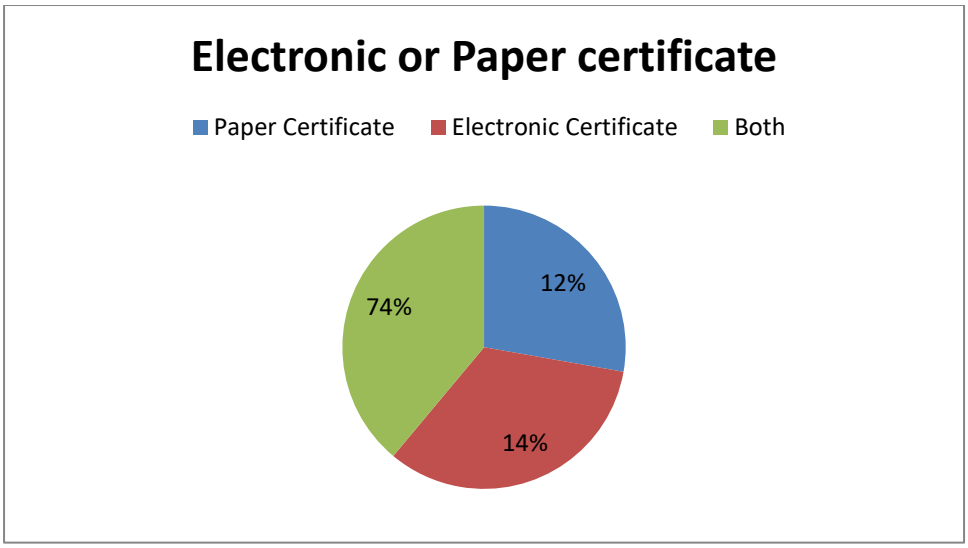

Figure 14: Electronic or Paper Certificates/Diplomas

- **Conclusions from Question Group 2**

The Majority of the participants indicated they keep their documents at home, and claimed issue electronic document makes easy accessibility than paper certificates. Furthermore, 10% of the participants believe that Blockchain technology is better for maintaining paper documents.

- **Question Group 3: Opinions and Knowledge about Blockchain Technology**

This section includes some questions about the respondent's understanding of blockchain.the first questions is Blockchain Technology Knowledge by Degree Level. The frequency results indicated that 302 undergraduates and 120 graduate students are familiar with Blockchain technology, whereas 2290 undergraduates and 1160 graduate students are not. The chi-square test revealed that there is a statistically significant link between level of comprehension of Blockchain technology and degree level; the Chi-Square test p-value was $0.03 < 0.05$.

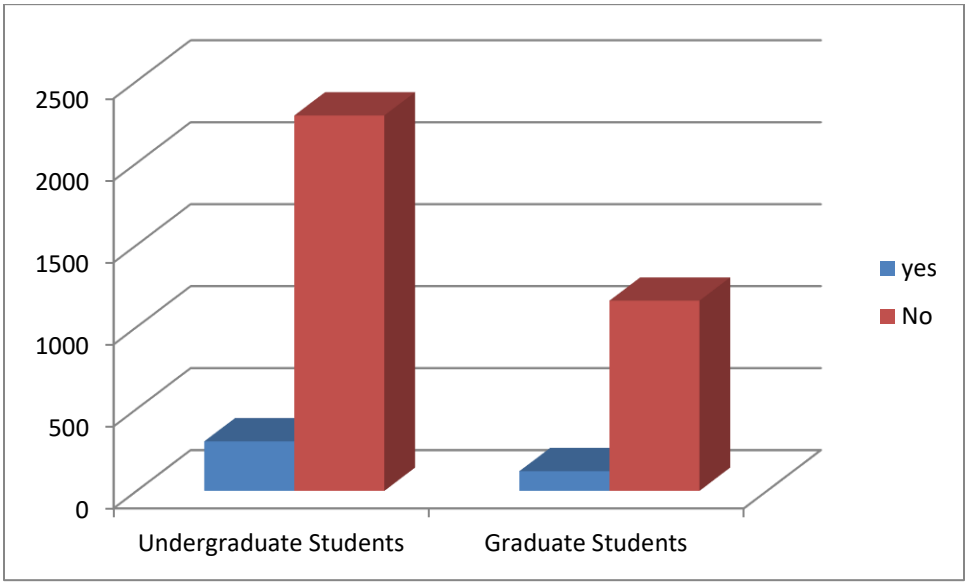

Figure 15: Level of Understanding of Blockchain (Degree level)

The second question is Blockchain Technology Knowledge by Age level. The frequency result shows that 200 participants between the ages of 16 and 24 indicated that they had some understanding of Blockchain technology, while 100 others in the same age group indicated that they have no comprehension of Blockchain technology. Furthermore, 300 people between the ages of 25 and 36 indicated some level of understanding of Blockchain technology, whereas 200 participants in the same age range reported no level of awareness. Furthermore, 263 individuals

between the ages of 37 and 49 said they understand Blockchain technology to some extent, while 150 others in the same age group stated they do not even know it at all. 13 individuals aged 50 and up stated that they understand Blockchain technology, while 24 others stated that they have a basic understanding of the technology. Whether there was a link between participants' ages and their level of comprehension of Blockchain technology, a Chi-square test was utilized. The Chi-square test revealed that there is a statistically significant link between participants' age and their knowledge of Blockchain technology; the Chi-Square test's p-value was 0.001< 0.05 in figure below

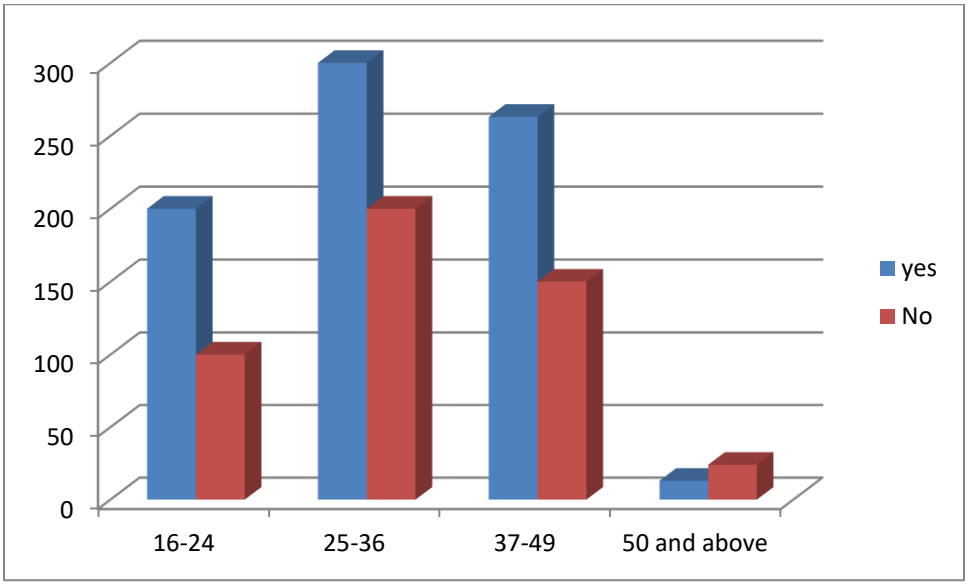

Figure 16: Level of Understanding of Blochchain Technology by age range

The third question is Blockchain Technology Knowledge by Field of Study. A Chi-square test was done to see if there was a statistically significant relationship between the participants' level of understanding of Blockchain technology and Field of Study. The Chi-square test results indicate that there is no statistically significant association between the participants' degree of understanding of Blockchain technology and their Field of Study; the Chi-square test shows p-values of 0.152 > (0.05).See the table 8.

Table 8: The Chi-Square Test

Factor	The Chi-square Test Result
Field of Study	0.152

- **Conclusions from Question Group 3**

Based on two factors, age and degree level, the Chi-square test found a statistically significant relationship between participants' level of comprehension of Blockchain technology and their demographic data. However, no statistically significant association between participants' level of awareness of Blockchain technology and field of study has been established.

To better understand the relationship between participants' opinions about Blockchain technology security for certificates/diplomas and their degree level, participants were asked: do you believe that Blockchain technology can offer increased security for your certificates/diplomas in the future? To see if there is a link between participants' degree level and their opinions of Blockchain technology security for their certificates/diplomas, a Chi-square test is utilized.

- **Degree Level**

According to the frequency results, 1454 undergraduate and 403 Graduate Students have a positive perception of Blockchain technology security, whereas 400 Undergraduate and 98 Graduate Students have a negative perception. Because the p-value of the Chi-Square test was (0.327)>0.05, the result of the chi-square test indicates that there is no statistically significant relationship between perceptions of Blockchain technology security for certificates/diplomas and their degree level.

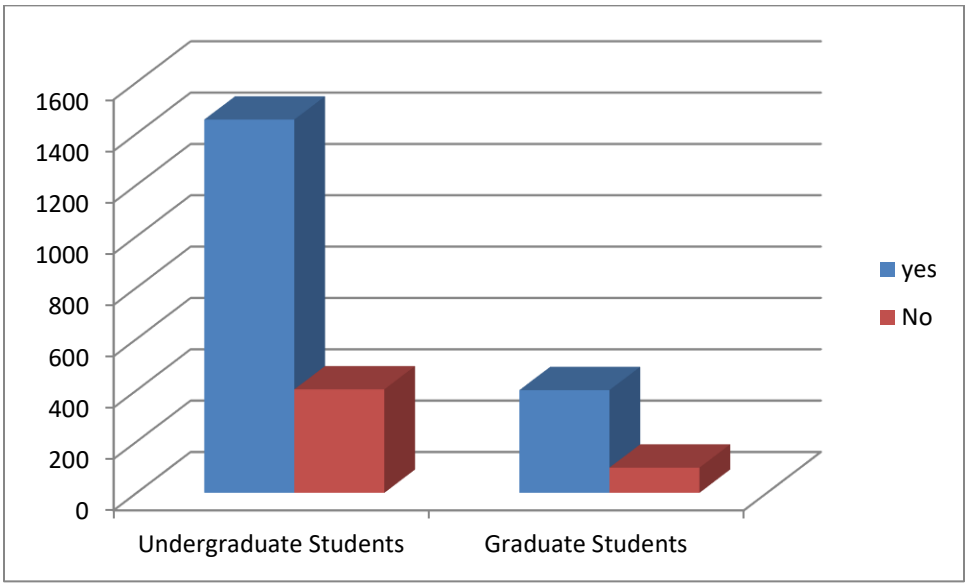

Figure 17: Security in Blockchain Technology with Degree Level

- **Field of Study**

The majority of participants who knew how Blockchain technology is used to maintain certificates/diplomas were from computer-related majors, according to the frequency result. Eight students from the Computer Science major, six from the Information Systems major, and three from the Software Engineering major said they were familiar with how Blockchain technology is utilized to manage certifications and degrees. The Chi-square test, on the other hand, found no statistically significant association between participants' awareness of how Blockchain technology is utilized to maintain certificates/diplomas and their major. Since the p-value of Chi-Square test (0.217)>0.05.,see the Figure 15

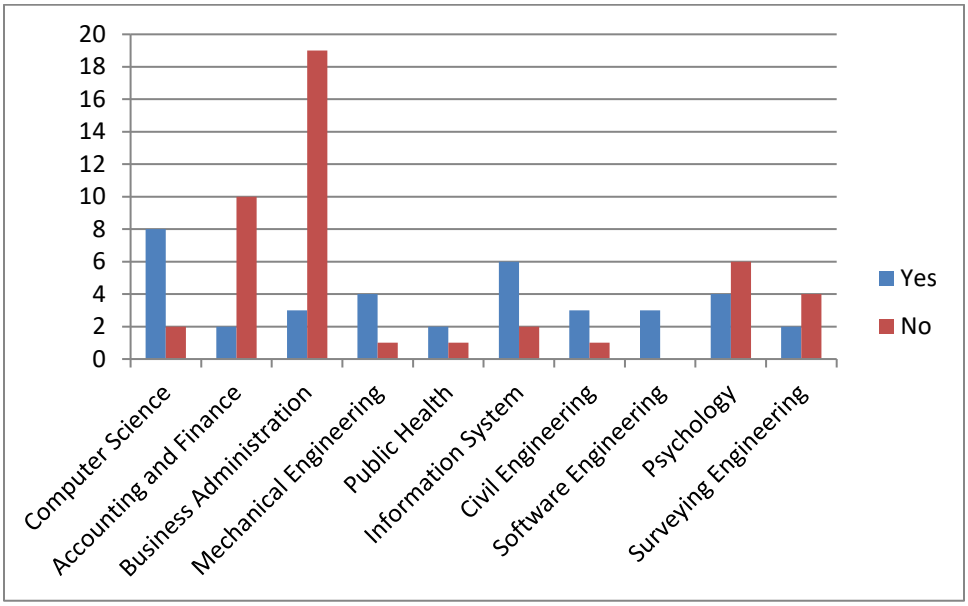

Figure 18: How to Manage Diplomas/Certificates (Field of Study)

In general, the Chi-Square test p-values are (0.327, 0.217) < 0.05. As a result, there is no statistically significant relationship between participants' opinions of Blockchain technology security and their Field of Study and degree level.

3.2.2. Conclusion from Survey Result

Data from participants was evaluated using descriptive statistics and the Chi-square test to get at these conclusions. Participants who may have difficulty with their paper certificates/diplomas after graduation were recognized as problem cases. We found that the students had issues with their certificates/diplomas when they are based on paper in all four scenarios. As a result, up to 36% of the participants in each case were given negative responses.

The majority of participants had insufficient awareness of Blockchain technology and could not understand how it was utilized to administer and issue their certificates/diplomas, according to the results. According to the Chi-Square testing, approximately 85.4% of participants still want Blockchain technology to be utilized to manage, issue, verify and safeguard their certificates/diplomas.

3.3. Interviews

Interviews with two university officials, Admas University and RiftValley University, employees who are responsible for creating, managing, and viewing students' degrees, and those who have the authority to hire and verify the applicant academic document.Employees from the registrar and human resources (HR) departments of those universities made up the interview sample. The audio-recorder was used to get direct feedback from the participants during each interview, which lasted 10 to 15 minutes. Both departments were given codes, R for the registrar and HR for human resource.

- **Question 1**

The purpose of the first question was to determine the participants' level of knowledge of Blockchain technology. Are you familiar with the notion of Blockchain technology for R and HR?
The following are the responses to this question:
R: “I'm familiar with Blockchain technology; my understanding is that it permits a code to be connected with a document to verify its authenticity.”
HR: “I am not familiar with Blockchain technology”.
The sentiment analysis method was used to classify the replies, which were divided into three categories: negative, positive, and neutral.
As a result,
R: Positive-65%.
HR: Negative-33%.

- **Question 2**

Do you think that maintaining academic data on Blockchain technology will be more technically challenging for staff? This question was asked of both R and HR.
The following are the solutions to this question:

R: “I'm not sure if blockchain technology is beneficial or not.”

HR: “I'm not sure if Blockchain technology will be beneficial or not because I'm not familiar with how we now keep academic records.” The sentiment analysis method was used to classify the replies, which included negative, positive, and neutral categories.

As a result,

R: Negative-12%.

HR: Negative-7%.

- **Question 3**

Do you think that maintaining academic data on Blockchain technology can be useful to control Degree Fraud?

This question was asked of both R and HR.

The following are the solutions to this question:

R: “I'm not sure if blockchain technology can prevent degree fraud.”

HR: “Blockchain may or may not overcome degree fraud problem.” The sentiment analysis method was used to classify the replies, which included negative, positive, and neutral categories.

As a result,

R: Negative-38%.

HR: Neutral-78%.

- **Question 4**

R and HR were asked the following question: Do you believe that implementing Blockchain technology will increase security risks? If so, why do you think that is? The following is the response to this question:

R: “I believe that while blockchain for diplomas has low risk because diplomas are merely a formality, blockchain for transcripts poses a greater risk because transcripts are sought after to be faked. Universities face a slew of problems as a result of falsified transcripts.”

HR: "I'm not sure what HR does." The sentiment analysis method was used to classify the replies, which included negative, positive, and neutral categories.

The result:

R: Negative - 15%

HR: Negative- 32%

- **Question 5**

R was asked the following question: What are your opinions on the benefits of implementing Blockchain technology for certificates/diplomas? The following is the response to this question:
R: “I believe Blockchain technology can improve in the verification of diploma authenticity. The sentiment analysis method was used to classify the replies, which included negative, positive, and neutral categories. As a result, we have:
R: 66 % positive

- **Question 6**

R was asked the following question: Do you believe Blockchain technology can minimize the financial cost of managing student records for students? The following is the response to this question:
R: Because student records include more than just their transcript and diploma, there will always be a cost associated with storing them. The result was divided into three categories using the sentiment analysis method: Negative, Positive, Neutral.
The result is:
R: Positive - 88%

- **Question 7**

R was asked the following question: Do you think Blockchain technology would make it easier for students to communicate their degrees? The following is the response to this question:
R: “I believe Blockchain technology can help secure student records by enabling students to access their records with minimal interference.” The result was divided into three categories using the sentiment analysis method: Negative, Positive, Neutral.
The result is:
R: Positive - 63%

- **Question 8**

R was asked the following question: how do you manage transfer issues? The following is the response to this question:
R: “when there is transfer case,the student must contact his home university to send official transcripts to us.the process takes upto six months.” The result was divided into three categories using the sentiment analysis method: Negative, Positive, Neutral.
The result is:
R: Positive - 56%

- **Question 9**

R was asked the following question: Would you support your university's adoption of Blockchain technology? The following is the response to this question:

“Why not?” says R. The sentiment analysis method was used to classify the replies, which included negative, positive, and neutral categories.

The result is:

R: Positive-52%.

- **Question 10**

HR was asked the following question: What is the method that Human Resources uses to validate an employee's degree or certificate? The following is the response to this question:

HR: “There is no mechanism or verification process in place to authenticate applicant degrees.”

The result was divided into three categories using the sentiment analysis method: Negative, Positive, and Neutral.

HR: Neutral-46%.

3.3.1. Discussion on Results Found from Interviews

In the previous questions, we aimed to learn more about Blockchain technology from the registrar and HR departments at Admas University and Riftvalley University, as well as their personal views on using it to issue, administer, and validate certificates/diplomas. We discovered that the registration department replied to all of our questions, with the majority of them being positive, indicating that they were in favor of using Blockchain technology to issue and maintain certificates and degrees. Otherwise, the HR department did not respond to the majority of the questions, and those that were responded to were negative. We noticed that HR was concerned about implementing the new technology.

3.4. Summary of Results from Survey and Interviews

The study confirms that for recently graduated students, paper certificates and diplomas are a severe problem; these certificates and diplomas may be lost, damaged, or otherwise corrupted. Despite their lack of experience with Blockchain technology, almost 85% of the students in this study stated a readiness to use it to award certificates and diplomas. The Chi-Square test resulted in a p-value of less than (0.05). As a consequence, a statistically significant association was found between participants' self-reported level of comprehension of Blockchain technology and their

demographic data based on two criteria: age and degree level. However, no statistically significant link was observed between participants' knowledge of Blockchain technology and the major results. The Chi-Square test yielded a p-value of more than one (0.05). As a consequence, no statistically significant link was discovered between demographic data(major) and participants' perceptions of Blockchain technology security. Furthermore, the Chi-Square test's p-value was greater than (0.05). As a consequence, no statistically significant link was discovered between demographic data and self-reported knowledge of how Blockchain technology is used to keep certificates/diplomas up to date. The registrar and HR at those universities were also interviewed, and the registrar approved of the notion of using Blockchain technology to issue and maintain certificates and degrees, despite the HR's concerns about adopting new technology. After analyzing all of the groups of questions from the survey and interview, the first research question of the thesis, as stated in the problem statement, should now be able to be answered: What challenges can students face after graduation as a result of paper certificates in Ethiopia? according to the results of the survey and interviews, the majority of graduate students confront issues such as late certificate issuance, preserving academic records, and degree fraud.

The majority of the survey and interview conclusions were summed up in the analysis of each question group. The most essential aspects of the Document Verifications, points of improvement, blockchain characteristics, and information system functionalities important to the design were all covered in these conclusions.

Table 9: Requirements were gathered and organized by improvement area of focus.

Area	Requirements
Security	Security in line with the most recent specifications
	Users' access is restricted.
	Data storage that is safe
Traceability	Detection of Document Fraud
	Regulatory monitoring
Enforcing Transactions	Contracts that can be enforced (smart contract functionality)

According to the survey and interviews, there is a considerable need for blockchain technology to be used to issue, manage, and maintain academic records, which will help employers detect degree

fraud and authenticate documents. In addition, based on this study, we designed a blockchain-based Academic Degree Fraud Detection, Verification and Locker Model for Ethiopia. requirements listed in table 9 are the main focus of the design in the following chapter.

CHAPTER FOUR

DESIGN OF ACADEMIC DOCUMENT FRAUD DETECTION, VERIFICATION AND LOCKER

4.1. Overview

Ethiopia's higher education ecosystem has grown and diversified greatly over the previous few decades, and it is predicted to continue to grow exponentially in the years ahead, due to factors including population growth, growing income levels, and increased upper-secondary enrollments. However, in Ethiopia, the majority of higher education institutions use a manual system to keep and organize student records. It's now time to answer the final two questions, which were generated from the previous chapter's conclusions and needs. The first question, "What is the most appropriate Blockchain tool or framework for developing an architecture that can satisfy these requirements?" necessitates a review of the frameworks. The second question is, "Can such a tool be used to create a workable architectural design that meets all of these requirements?" demands the collection of elicited requirements into a list, as well as the creation and implementation of an architectural design utilizing the specified framework. This chapter comprises to a step-by-step explanation of these activities. The first segment examines which frameworks best meet the requirements before making a decision. The second section presents the proposed Architecture of Academic Degree Fraud Detection, verification and locker.

4.2. Framework Comparison and Choice

After Conducting survey and interview the previous chapter, it's time to address the second question from the issue statement: What Blockchain tool or framework is best for developing an architecture that meets these requirements?

A mixed analysis that focuses on the most significant functionalities that a document verification system should contain is required in order to make a smart choice for the framework. The framework analysis from Chapter 2.6 should be considered in addition to the requirements from the previous chapter.

4.2.1. Framework Choice

So, what can be concluded from the survey and interview? To begin with, a private blockchain framework appears to be more appropriate due to the numerous security control methods that are required. Second, the architecture should support highly customized networks, encompassing not only asset management but also identity management, with unique rights granted to blockchain participants.

Finally, APIs must be supported by the framework.

We can examine the applicability of each framework by combining these needs with the capabilities of the frameworks provided in the previous chapters:

• Ethereum - Ethereum is a public framework with a built-in cryptocurrency and significant Education capabilities. It does, however, cost money to run code. Having many of the essential functions on Ethereum would be much more expensive than maintaining a private network with only a few nodes. At the same time, it lacks the necessary identity management, authentication, and authorization tools out of the box. It has great financial and traceability features, but security and cost scaling are lacking.

R3 Corda - It's a private network that's less expensive to operate and can meet most privacy requirements. It also places a strong emphasis on financial transactions, which was a popular demand. However, it falls short in the administration of data such as assets and entities, resulting in poor traceability.

• Hyperledger Fabric - It provides the necessary methods for authentication and authorization, as well as smart contract capacity, like the other frameworks. It's highly customisable, with all of the data and identity management features you'll need. It also has easy-to-deploy rest servers, which is vital for synchronization. It does, however, have a drawback: while it is customisable, it lacks a native cryptocurrency, thus financial transactions are only possible if they are designed from the ground up to be emulated by the network. If we assume that Document related Transactions can be simulated within the network, Hyperledger meets almost all of the requirements from a requirements standpoint.

R3 Corda has the disadvantages of asset management and traceability, while Ethereum has the disadvantages of cost and security.A performance comparison should also be employed to make the framework decision final. Hyperledger has lower latency, execution time, and throughput than Ethereum, according to previously published experiments stated in section 2.6.All of this while being less expensive to maintain and meeting more requirements than any of the other frameworks examined.

Finally, the question "What Blockchain tool or framework is best for developing an architecture that can meet these requirements?" may be addressed. Hyperledger Fabric appears to be the tool that meets the most requirements while also having higher performance and cheaper costs, making it the most appropriate of the evaluated technologies for the creation of a Document Verification and Locker architecture.

In general,the following are the main reason for selecting Hyperledger Fabric framework as implementation tool in this study:

- Hyperledger is a private blockchain hence records are not in public domain
- Access levels can be customized as per requirement as it is a role based blockchain
- It requires less computation power while performing transactions, because the participants are known and limited
- Nodes are known and trusted and faults can be quickly fixed by manual intervention
- It allows participants to create channels
- It does not use coins or transaction is not required unlike Ethereum.

4.3. Proposed Design

As shown in figure 19, the proposed model can be used to solve all problems identified during investigation done through survey and interview that are related to Academic degree fraud detection and verification and have advantages for countries like Ethiopia by providing a decentralized, shared, transparent, secured and easily accessible academic record repository.
The proposed model consists of two main Layers, Front End (Web Application Layer) and Backend (Blockchain Application Layer).

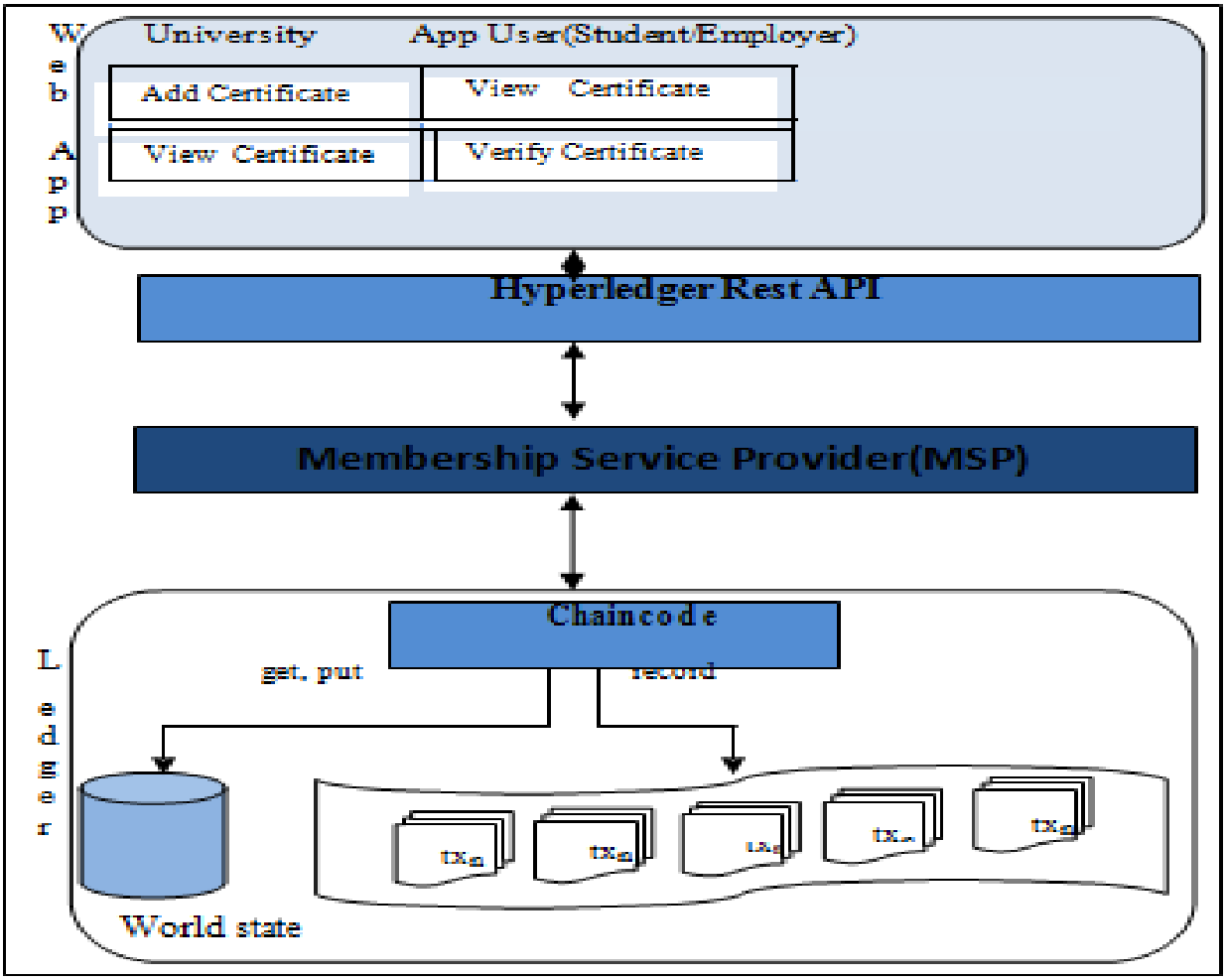

Figure 19: Design of Academic degree Fraud detection and verification model

- **Web Application Layer**

The Web Application provides an interface for Issuer (E.g University or Academic Institutions) and Employer to perform functions such as accessing a document, transcript exchange, requesting a transcript to be sent, uploading and hashing a certificate, and verifying a certificate. Users can perform functions through the web application by interfacing with the Hyperledger REST APIs to perform the functions. A database of the students, universities, transcripts, and transcript requests was used by the web application and corresponds to the contents of the Hyperledger ledger.

- **Blockchain Application Layer**

The Blockchain Application Layer on the other hand is comprised of Membership Service Provider, chaincode and Ledger(World State and Transaction Log).

- **Membership Service Provider (MSP)**

Membership Service Provider (MSP) is used to manage identities on the blockchain network. In proposed system, this provider is used to authenticate System Admin user,issuer or university, and employer who wants to join the blockchain network. This is mainly important to allow only trusted university and employer to access and perform user level functions.

- **Design of Chaincode**

The most crucial operations for a degree fraud detection and document verification system are designing proper smart contracts for storing information like Academic certificate data and user information in blockchain and executing duties like authentication, issuing document, and validating document. The smart contract will carry out the tasks or transactions based on the data and criteria specified in the smart contract. In hyperledger fabric, the smart contract runs on the peers and creates transactions. More broadly, it enables users to create transactions in the Hyperledger Fabric network's shared ledger and update the world state of the assets.
We have included two smart contracts in the proposed system, as indicated in the table 10 that can handle the most common and basic use cases that the Degree fraud detection system has.

Table 10: design of smart contracts used in proposed model

Smart Contracts	Description
Academic Certificate	University or academic institutions can keep track of information about degrees they've been issued.
Identity Management	Used for authorizing users of the blockchain system

These smart contracts will not store vast amounts of data or long textual descriptions, such as Issuer or Date of Issuance, but simply the information necessary to carry out the tasks or transactions under the smart contract. Participants in smart contracts are recognized with their own blockchain address, just like in other smart contracts. The Academic Certificate contract will provide information on the degree awarded by the issuer university, such as the issuer's name, document type, document id, and issuance date. The Identity Management smart contract would register system users and delegate who has the authority to execute other smart contracts and modify data on the blockchain.

- **Ledger**

Ledger in proposed architecture provides a verifiable history of all valid document transactions and invalid document transactions occurring during the operation of the system. World state stores the current values of a set of ledger states. On the other hand, a blockchain in ledger records all the changes that have resulted in the current the world state.couchdb was used to maintain academic documents in world state

CHAPTER FIVE

IMPLEMENTATION AND PERFORMANCE ANALYSIS

5.1. Overview

We provide a prototype implementation of the proposed architecture as proof of concept. This research is being done as a proof of concept to see if establishing a blockchain-based document verification system utilizing Hyperledger Fabric is feasible for developing countries like Ethiopia. It does not depict how a fully completed System might behave or seem. According to the results of the survey and interview, the goal is to demonstrate a product concept that can improve the discipline of Document verification by making data more easily accessible, reducing synchronization time, improving integration and security, and providing a tool that assists in ensuring end-to-end traceability. The proposed architecture is implemented using Hyperledger Fabric as a framework. Golang is used to create chaincode.

5.2. A prototype Implementation of Proposed Model

The proposed system's has two main users : Issuer and Employer.

- Issuer(University or Academic Institutions) - A university is a sort of user who can add and store store academic certificates on the blockchain ledger.
- Employer: This user has access to certifications issued by the institution or issuer.

Login page is depicted in the figure 20 below.

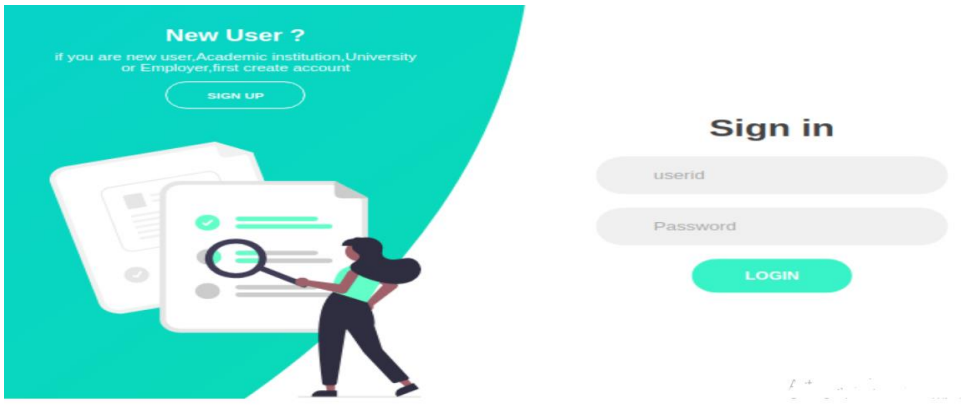

Figure 20: User Login Page

Figure 21 displays homepage of the issuer or academic institution. As shown in figure, all documents id issued by the issuer will be displayed. For example, in this case only one document is issued by Adama Science and Technology University.

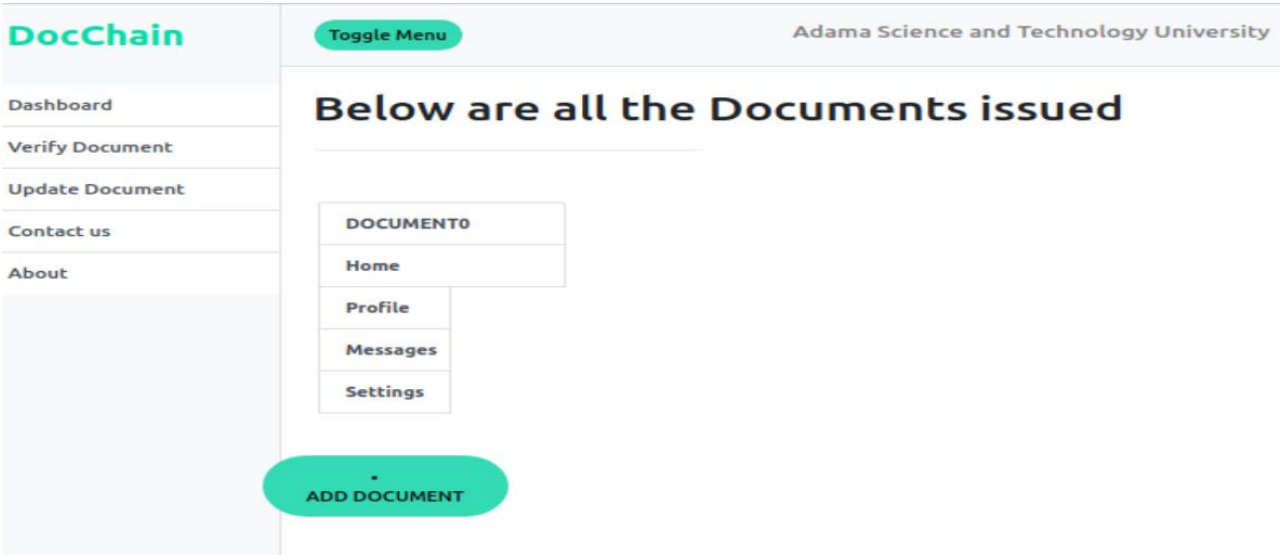

Figure 21 : Issuer (University or Academic Institution) Page

Figure 22 presents details of issued and stored document on block chain ledger .as shown in figure, when there is a document stored on block chain ledger, the user can easily search and retrieve directly from the ledger.

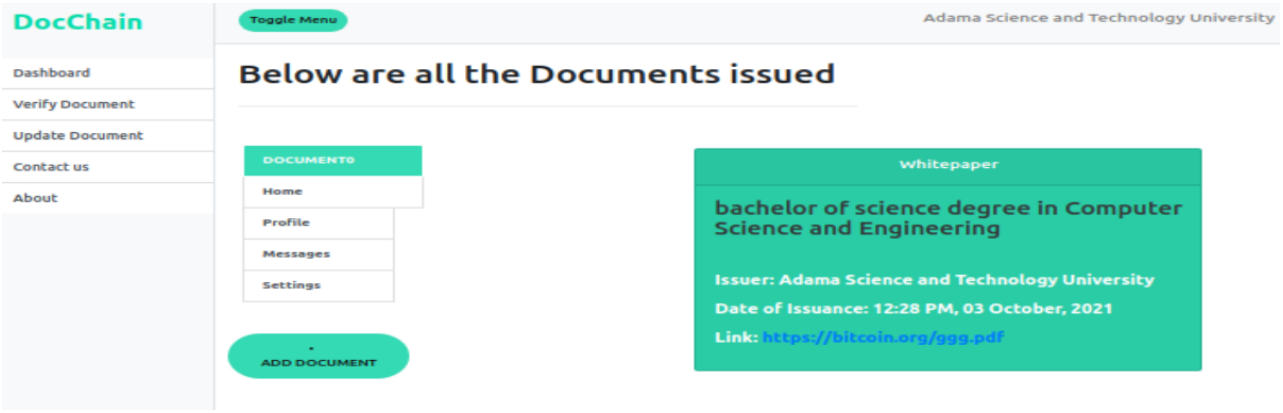

Figure 22 :View Document Page

Figure 23 displayed academic document search form. The user can easily search an academic document stored on a ledger simply by inserting Document Id.

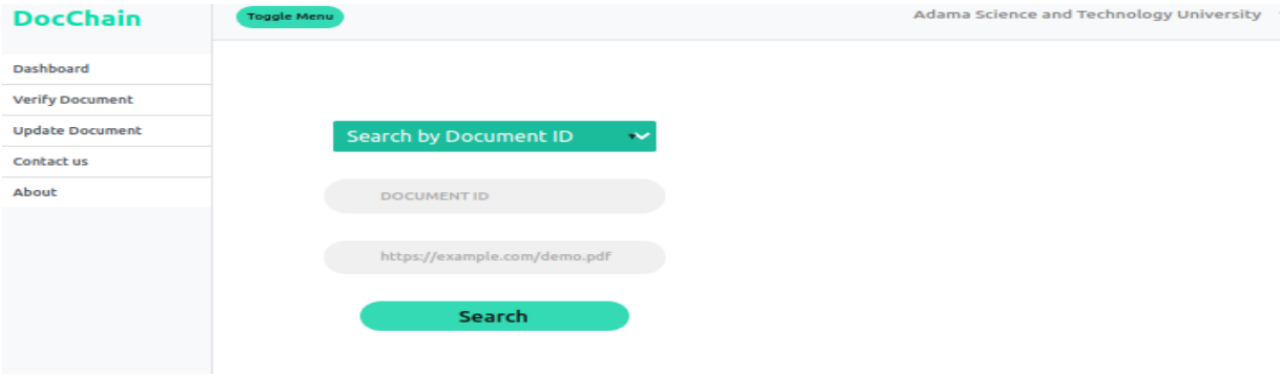

Figure 23 :Verify Document Page

Figure 24 displays a message when the searched document is not found on the Blockchain ledger. As indicated in figure, when there is no document stored on the ledger with searched document id, the system displays no document message for the user(employer).this can be helpful in detecting degree frauds during recruitment.

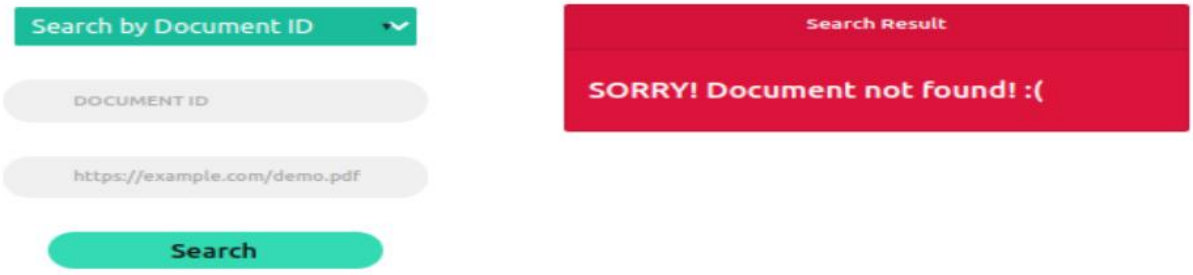

Figure 24: No Document Found Message

- **Smart Contract for Create user Account**

```
func (s *SmartContract) CreateUser(ctx contractapi.TransactionContextInterface, userName
string, name string,

email string, password string) error {

        user := User{

                UserName: userName,

                Name:     name,

                Email:    email,

                Password: password,

                DocType:  "USER",

        }

  userAsBytes, _ := json.Marshal(user)

        userCount++

        return ctx.GetStub().PutState("USER"+strconv.Itoa(userCount), userAsBytes)

}
```

Figure 25 :Smart contract for create Account

Smart Contract to Issue Academic Certificate

```
func (s *SmartContract) CreateDocument(ctx contractapi.TransactionContextInterface, name string, url string, issuedBy string, hashedDoc string, docType string) error {

	loc, err := time.LoadLocation("Ethiopia/Addis Abeba")

	if err != nil {

		return fmt.Errorf("Failed to load location. %s", err.Error())

	}

	document := Document{

		Name:          name,

		Url:           url,

		IssuedBy:      issuedBy,

		DateOfIssuance: time.Now().In(loc).Format(timeFormat),

		HashedDoc:     hashedDoc,

		DocType:       docType,

	}

	documentAsBytes, _ := json.Marshal(document)

	docCount++

	return ctx.GetStub().PutState("DOCUMENT"+strconv.Itoa(docCount), documentAsBytes)

}
```

Figure 26: Issue Certificate Smart Contract

Smart Contract Verify Document

```
func (s *SmartContract) QueryDocumentByHash(ctx
contractapi.TransactionContextInterface, hashedDoc string) ([]DocumentQueryResult,
error) {

    var queryString = "{\"selector\": { \"hashedDoc\" : \"" + hashedDoc + "\"}}"

    results, err := getDocumentQueryResultForQueryString(ctx, queryString)

    if err != nil {
        return nil, err
    }
```

Figure 27: Verify Documents smart contract

4.3. Performance Analysis of Proposed Model

There is no clear methodology for evaluating and assessing the various blockchain solutions in terms of their various aspects, such as performance, security, and scalability, despite the fact that there are many blockchain-based solutions. The performance of the proposed model in terms of execution time, latency, and throughput is evaluated in this section by varying the workload in each platform up to 1000 transactions due to the limitation of type of computer used for performance testing. We also look at the scalability of the proposed model by changing the number of nodes from one to ten.

We used a modified version of Hyperledger caliper v0.4.1 to analyze the performance of the Proposed model, which is a performance benchmark tool for multiple blockchain-based solutions that uses a running blockchain network as the target platform.

This tool will generate html reports that include some performance metrics like resource usage and transactions per second (TPS). To calculate the transaction execution time, we updated

Hyperledger caliper.The performance analysis layer, the adapter layer, the interface layer, and the blockchain framework are the four key layers that make up the architecture for analyzing the performance of a blockchain platform.

The caliper architecture's major component is the adaptability layer. This layer's primary function is to integrate various blockchain implementations into the evaluation system.The adaptor is responsible for translating between the blockchain protocol and the caliper north bound interfaces for each blockchain platform to be tested.The interface layer is in charge of providing a number of blockchain north bound interfaces for deploying, invoking, and querying smart contracts.This layer also includes functions for monitoring memory and CPU usage.

The performance evaluation layer's job is to run stress tests on the blockchain platform that has been developed, with the blockchain network data and test settings being provided as input for each test.

Since the performance of blockchain based document verification is also dependent on type computer used, the system was tasted using the following computer.

Table 11:Personal Computer Specification used for Performance Testing

Operating System Used	Ubuntu 18.04 installed on Virtual Box
Processor Type	Intel Corei5
Processor Speed	2.5 GHZ
Installed Ram	8GB
Storage	1terabyte

We tested the proposed model's by using three common performance used for evaluating blockchain based use cases namely, Execution time, Average latency and Throughput with single peer.We examined the execution time of the proposed model by altering the number of transactions and assessing the execution time for different functions. The results of the Caliper test demonstrated that as the number of transactions grows, so do the execution times. When it comes to the invoke function, it's important to note that as the number of transactions gro ws, so does the average latency. The proposed model's throughput decreases as the number of transactions increases. Figure 30 depicts Caliper Test report generated for performance analysis.

Caliper report

Summary of performance metrics

Name	Succ	Fail	Send Rate (TPS)	Max Latency (s)	Min Latency (s)	Avg Latency (s)	Throughput (TPS)
open	400	0	40.1	7.24	0.74	5.53	26.7

Performance metrics for open

Name	Succ	Fail	Send Rate (TPS)	Max Latency (s)	Min Latency (s)	Avg Latency (s)	Throughput (TPS)
open	400	0	40.1	7.24	0.74	5.53	26.7

Figure 28: Performance test Report Generated by Hyperledger Caliper Tool

CHAPTER SIX

CONCULISON AND RECOMMENDATIONS

6.1. Conclusions

Blockchain technology has already been proposed by previous researchers as an effort to assist and benefit the educational environment. It apart from the issues associated with falsifying paper certificates and diplomas, there are other issues that students may face after graduation as a result of paper certificates. The goal of this study is to identify some of the issues with paper certificates as well as to evaluate the potential of alternative Blockchain-based solutions for paper certificates and diplomas. When it comes to issuing, managing, and authenticating certificates and diplomas, Blockchain technology comes in handy. The study's goal is to learn about the use of Blockchain technology to issue, administer, and validate certificates and diplomas from three university students. To determine the necessity and demand for Blockchain technology, it is critical to evaluate and understand the perspectives of persons who are responsible for producing and managing students' academic records.

In recent years, blockchain technology has showed promise in combating counterfeit academic credentials. A blockchain database can store a student or trainee certificate, similar to grades. Rather than requesting verification of the applicant's degree from their local university, companies can instantly access a digital certificate stored in a blockchain database. As a result, this technology has the potential to eliminate the current educational system's fraudulent behaviors. Furthermore, this technology can generate authentic credentials, which eliminates the need for students, teachers, and university officials to rely on academic certificates.

All of Ethiopia's academic document forgery difficulties might be addressed with the proposed blockchain-based academic certificate verification approach. The proposed system architecture is built on the hyperledger fabric framework, and it allows academic institutions or universities to issue records and share academic certificates and transcripts with students, possible employers, and other universities. Potential employers can use the blockchain database to check papers submitted by applicants.

6.2. Recommendation

Blockchain is an emerging technology in the world of education, with a lot of revolution and research just getting started in this distributed technology. Following are some recommendations based on the current publications covered in this study:

- In this study, we proposed a model for academic Degree Fraud detection, verification and locker that addresses several security concerns. More research is needed to include other security requirements such as ownership and confidentiality.
- This study was limited to the verification of academic certificates. Further study, particularly in nations like Ethiopia, is required, including the verification of passports, house blueprints, bank statements, and birth certificates.
- Due to the immutability attribute of Blockchain Technology, one of the key limitations of using Blockchain for document verification is certificate revocation. To overcome this obstacle, more research is required.
- Most of Certificate verification systems only focused on verifying Academic information. Especially for countries like Ethiopia, further studies needs to be conducted that include verification of Passport, house blueprint, bank statements and birth certificate.
- In this thesis, we tried to study application of Blockchain Technology for Academic Certificate Verification. The future study can include developing an exam or assignment evaluation system by combining blockchain technology with artificial intelligence instead of depending on human intervention to make the evaluation activities trust-free.

REFERENCES

New Business Ethiopia. (2019). *Study finds 3,200 civil servants with forged credentials in Ethiopia – New Business Ethiopia*. https://newbusinessethiopia.com/crime/study-finds-3200-civil-servants-with-forged-credentials-in-ethiopia/

Raynor de Best. (2019). *Bitcoin blockchain size 2009-2021 | Statista*. https://www.statista.com/statistics/647523/worldwide-bitcoin-blockchain-size/

Yonas Abiye. (2019). *MoE partners INSA to root out employees with fake documents | The Reporter Ethiopia English*. https://www.thereporterethiopia.com/article/moe-partners-insa-root-out-employees-fake-documents

Alpár, G., & Jacobs, B. (2013). Credential Design in Attribute-Based Identity Management. *Bridging Distances in Technology and Regulation*, *10522*.

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). https://doi.org/10.1016/j.rssm.2010.12.004

Awaji, B., Solaiman, E., & Marshall, L. (2020a). Blockchain-based trusted achievement record system design. *PervasiveHealth: Pervasive Computing Technologies for Healthcare*. https://doi.org/10.1145/3411681.3411689

Awaji, B., Solaiman, E., & Marshall, L. (2020b). Investigating the requirements for

building a blockchain-based achievement record system. *PervasiveHealth: Pervasive Computing Technologies for Healthcare*. https://doi.org/10.1145/3411681.3411691

Badr, A., Rafferty, L., Mahmoud, Q., Elgazzar, K., & Hung, P. (2019). *A Permissioned Blockchain-Based System for Verification of Academic Records*. https://doi.org/10.1109/NTMS.2019.8763831

Baum, S. (2014). Higher Education Earning Premium Value , Variation , and Trends. *Urban Institute*, *February*.

Castro, M., & Liskov, B. (1999). *Practical Byzantine Fault Tolerance*.

Cheng, J. C., Lee, N. Y., Chi, C., & Chen, Y. H. (2018). Blockchain and smart contract for digital certificate. *Proceedings of 4th IEEE International Conference on Applied System Innovation 2018, ICASI 2018*. https://doi.org/10.1109/ICASI.2018.8394455

Cohen, E. B., & Winch, R. (2011). *Diploma and Accreditation Mills: New Trends in Credential Abuse*. http://www.accredibase.com

Curmi, A., & Inguanez, F. (2019). Blockchain based certificate verification platform. *Lecture Notes in Business Information Processing*, *339*. https://doi.org/10.1007/978-3-030-04849-5_18

Eckstein, M. A. (2019). *Combating academic fraud: towards a culture of integrity | IIEP-UNESCO*. http://www.iiep.unesco.org/en/publication/combating-academic-fraud-towards-culture-integrity

Garwe, E. (2015). Qualification, Award and Recognition Fraud in Higher Education in Zimbabwe. *Critical Studies in Education*, *5*, 119–135. https://doi.org/10.5296/jse.v5i2.7456

Gavofyork, . (2019). *GitHub - ethereum/serpent*. https://github.com/ethereum/serpent

Ge, Z., & Hu, Y. (2021). Application Research of the New Mode of "Blockchain + Higher Education." *Advances in Intelligent Systems and Computing*, *1233 AISC*. https://doi.org/10.1007/978-3-030-51431-0_61

Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Čapkun, S. (2016). On the security and performance of Proof of Work blockchains. *Proceedings of the ACM Conference on Computer and Communications Security*, *24-28-October-2016*. https://doi.org/10.1145/2976749.2978341

Ghandour, A. G., Elhoseny, M., & Hassanien, A. E. (2019). *Blockchains for Smart Cities: A Survey*. https://doi.org/10.1007/978-3-030-01560-2_9

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*. https://doi.org/10.1007/978-3-030-04849-5_16

Han, M., Wu, D., Li, Z., Xie, Y., He, J. S., & Baba, A. (2018). A novel blockchain-based education records verification solution. *SIGITE 2018 - Proceedings of the 19th Annual SIG Conference on Information Technology Education*. https://doi.org/10.1145/3241815.3241870

HOLCOMB, Z. C. (2020). *FUNDAMENTALS OF DESCRIPTIVE STATISTICS*.

Innovation, C. for E. R. and. (2001). The Well-being of Nations The Role of Human and Social Capital (Complete Edition - ISBN 9264185895). *SourceOECD Education & Skills*, *2001*(5).

Juricic, V., Radoševic, M., & Fuzul, E. (2019). Creating student's profile using

blockchain technology. *2019 42nd International Convention on Information and Communication Technology, Electronics and Microelectronics, MIPRO 2019 - Proceedings*. https://doi.org/10.23919/MIPRO.2019.8756687

Koenig Edward., A. M. D. (2017.). *FIGHTING Domestic and International FRAUD in the - ProQuest*. https://www.proquest.com/docview/1239088196

KUrton, M. (2020.). *Blockchain Platforms - List of the Top 10 in 2020 | EM360*. https://em360tech.com/top-10/top-10-blockchain-platforms-explore-2020

Liu, B. (2012). Sentiment Analysis and Opinion Mining. *Http://Dx.Doi.Org/10.2200/S00416ED1V01Y201204HLT016 , 5*(1), 1–184. https://doi.org/10.2200/S00416ED1V01Y201204HLT016

Liyuan, L., Meng, H., Yiyun, Z., & Reza, P. (2019). E2C-Chain: A two-stage incentive education employment and skill certification blockchain. *Proceedings - 2019 2nd IEEE International Conference on Blockchain, Blockchain 2019*, 140–147. https://doi.org/10.1109/BLOCKCHAIN.2019.00027

Lu, Y. (2019). The blockchain: State-of-the-art and research challenges. In *Journal of Industrial Information Integration* (Vol. 15). https://doi.org/10.1016/j.jii.2019.04.002

McHugh, M. L. (2013). The Chi-square test of independence. *Biochemia Medica*, *23*(2), 143. https://doi.org/10.11613/BM.2013.018

Mikroyannidis, A., Domingue, J., Bachler, M., & Quick, K. (2019). Smart Blockchain Badges for Data Science Education. *Proceedings - Frontiers in Education Conference, FIE, 2018-October*. https://doi.org/10.1109/FIE.2018.8659012

Mohanta, B. K., Jena, D., Panda, S. S., & Sobhanayak, S. (2019). Blockchain

technology: A survey on applications and security privacy Challenges. In *Internet of Things (Netherlands)* (Vol. 8). https://doi.org/10.1016/j.iot.2019.100107

Moore, M. G. (2009). A sad reminder that diploma mills are still with us. In *International Journal of Phytoremediation* (Vol. 21, Issue 1). https://doi.org/10.1080/08923640903356129

Naumova, O. A., Svetkina, I. A., & Naumov, D. V. (2019). The main limitations of applying blockchain technology in the field of education. *2019 International Science and Technology Conference "EastConf", EastConf 2019*. https://doi.org/10.1109/Eastonf.2019.8725411

Poorni, R., Lakshmanan, M., & Bhuvaneswari, S. (2019). DIGICERT: A Secured Digital Certificate Application using Blockchain through Smart Contracts. *Proceedings of the 4th International Conference on Communication and Electronics Systems, ICCES 2019*. https://doi.org/10.1109/ICCES45898.2019.9002576

Saleh, O., Ghazali, O., & Rana, M. E. (2020). Blockchain Based Framework for Educational Certificates Verification. *Journal of Critical Reviews*, *7*, 79–84. https://doi.org/10.31838/jcr.07.03.13

Sayed, R. H. (2019). Potential of Blockchain Technology to Solve Fake Diploma Problem. *University of Jyväskylä Department of Computer Science and Information Systems*.

Selimi, M., Kabbinale, A. R., Ali, A., Navarro, L., & Sathiaseelan, A. (2018). Towards blockchain-enabled wireless mesh networks. *CRYBLOCK 2018 - Proceedings of the 1st Workshop on Cryptocurrencies and Blockchains for Distributed Systems, Part of MobiSys 2018*.

https://doi.org/10.1145/3211933.3211936

Shah, M., & Kumar, P. (2019). Tamper proof birth certificate using blockchain technology. *International Journal of Recent Technology and Engineering*, *7*(5).

Shahid, M. R., Mahmood, S., Hafeez, S., Zahid, B., Jabbar, S., & Ashraf, R. (2019). Blockchain based share economy trust point: Case study based validation. *PervasiveHealth: Pervasive Computing Technologies for Healthcare*. https://doi.org/10.1145/3341325.3342026

Share, E., Memorable, M., & They, L. (2014). *Fifty-eight Percent of Employers Have Caught a Lie on a Resume* (Vol. 2014). https://www.careerbuilder.ca/share/aboutus/pressreleasesdetail.aspx?sd=8%2F7%2F2014&id=pr837&ed=12%2F31%2F2014

Sharma, D., & Negasa, W. (2020). *A Blockchain-Enabled Digital Document Locker and Verification Model for Ethiopia*.

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*. https://doi.org/10.1109/IAC3T.2018.8674023

Trines, S. (2019.). *Academic Fraud, Corruption, and Implications for Credential Assessment*. https://wenr.wes.org/2017/12/academic-fraud-corruption-and-implications-for-credential-assessment

Turkanović, M., Hölbl, M., Košič, K., Heričko, M., & Kamišalić, A. (2018). EduCTX: A blockchain-based higher education credit platform. *IEEE Access*, *6*. https://doi.org/10.1109/ACCESS.2018.2789929

Vasin, P., & Co, B. (2019). *BlackCoin's Proof-of-Stake Protocol v2*. http://www.blackcoin.co

Yumna, H., Khan, M. M., Ikram, M., & Ilyas, S. (2019). Use of Blockchain in Education: A Systematic Literature Review. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, *11432 LNAI*. https://doi.org/10.1007/978-3-030-14802-7_17

Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International Journal of Web and Grid Services*, *14*(4). https://doi.org/10.1504/IJWGS.2018.095647

APPENDIX

Sample Smart Contract Code

```
// CreateDocument adds a new document to the world state with given details

func (s *SmartContract) CreateDocument(ctx contractapi.TransactionContextInterface, name string,

url string, issuedBy string, hashedDoc string, docType string) error {


	loc, err := time.LoadLocation("Ethiopia/Addis Abeba")


	if err != nil {

		return fmt.Errorf("Failed to load location. %s", err.Error())

	}


	document := Document{

		Name:          name,

		Url:           url,

		IssuedBy:      issuedBy,

		DateOfIssuance: time.Now().In(loc).Format(timeFormat),

		HashedDoc:     hashedDoc,

		DocType:       docType,

	}


	documentAsBytes, _ := json.Marshal(document)

	docCount++

	return ctx.GetStub().PutState("DOCUMENT"+strconv.Itoa(docCount), documentAsBytes)
```

```
}

//smart contract to create user account

func (s *SmartContract) CreateUser(ctx contractapi.TransactionContextInterface, userName
string, name string,

email string, password string) error {

	user := User{

		UserName: userName,

		Name:     name,

		Email:    email,

		Password: password,

		DocType:  "USER",

	}


	userAsBytes, _ := json.Marshal(user)


	userCount++

	return ctx.GetStub().PutState("USER"+strconv.Itoa(userCount), userAsBytes)

}


// QueryDocument returns the document stored in the world state with given id

func (s *SmartContract) QueryDocument(ctx contractapi.TransactionContextInterface,
documentNumber string) (*Document, error) {

	documentAsBytes, err := ctx.GetStub().GetState(documentNumber)


	if err != nil {
```

```
		return nil, fmt.Errorf("Failed to read from world state. %s", err.Error())
	}

	if documentAsBytes == nil {
		return nil, fmt.Errorf("%s does not exist", documentNumber)
	}

	document := new(Document)
	_ = json.Unmarshal(documentAsBytes, document)

	return document, nil
}

// QueryAllRecords returns all records found in world state
func (s *SmartContract) QueryAllRecords(ctx contractapi.TransactionContextInterface)
([]DocumentQueryResult, error) {
	startKey := ""
	endKey := ""

	resultsIterator, err := ctx.GetStub().GetStateByRange(startKey, endKey)

	if err != nil {
		return nil, err
	}
	defer resultsIterator.Close()
```

```
	results := []DocumentQueryResult{}

	for resultsIterator.HasNext() {
		queryResponse, err := resultsIterator.Next()

		if err != nil {
			return nil, err
		}

		document := new(Document)
		err = json.Unmarshal(queryResponse.Value, document)

		if err != nil {
			continue
		}

		documentQueryResult := DocumentQueryResult{Key: queryResponse.Key, Record:
document}
		results = append(results, documentQueryResult)
	}

	return results, nil
}

func getDocumentQueryResultForQueryString(ctx contractapi.TransactionContextInterface, queryString
string) ([]DocumentQueryResult, error) {
```

```
	fmt.Printf("- getDocumentQueryResultForQueryString queryString:\n%s\n", queryString)

	resultsIterator, err := ctx.GetStub().GetQueryResult(queryString)
	if err != nil {
		return nil, err
	}

	defer resultsIterator.Close()

	results := []DocumentQueryResult{}

	for resultsIterator.HasNext() {
		queryResponse, err := resultsIterator.Next()

		if err != nil {
			return nil, err
		}

		document := new(Document)
		_ = json.Unmarshal(queryResponse.Value, document)

		documentQueryResult := DocumentQueryResult{Key: queryResponse.Key, Record:
document}
		results = append(results, documentQueryResult)
	}
```

```
	return results, nil


	// // buffer is a JSON array containing QueryRecord
	// var buffer bytes.Buffer
	// buffer.WriteString("[")

}

//Intermediary function to be used by other functions when needed (will never be invoked from outside of the chaincode body)
func getUserQueryResultForQueryString(ctx contractapi.TransactionContextInterface, queryString string) ([]UserQueryResult, error) {

	fmt.Printf("- getDocumentQueryResultForQueryString queryString:\n%s\n", queryString)

	resultsIterator, err := ctx.GetStub().GetQueryResult(queryString)
	if err != nil {
		return nil, err
	}

	defer resultsIterator.Close()

	results := []UserQueryResult{}

	for resultsIterator.HasNext() {
		queryResponse, err := resultsIterator.Next()
```

```
		if err != nil {
			return nil, err
		}

		user := new(User)
		_ = json.Unmarshal(queryResponse.Value, user)

		userQueryResult := UserQueryResult{Key: queryResponse.Key, Record: user}
		results = append(results, userQueryResult)
	}

	return results, nil
}

func (s *SmartContract) QueryDocumentByHash(ctx contractapi.TransactionContextInterface, hashedDoc string) ([]DocumentQueryResult, error) {

	var queryString = "{\"selector\": { \"hashedDoc\" : \"" + hashedDoc + "\"}}"

	results, err := getDocumentQueryResultForQueryString(ctx, queryString)

	if err != nil {
		return nil, err
	}
```

```
	return results, nil
}

func (s *SmartContract) QueryDocumentByUrl(ctx contractapi.TransactionContextInterface, url string)
([]DocumentQueryResult, error) {

	var queryString = "{\"selector\": { \"url\" : \"" + url + "\"}}"

	results, err := getDocumentQueryResultForQueryString(ctx, queryString)

	if err != nil {
		return nil, err
	}

	return results, nil
}

func (s *SmartContract) QueryDocumentByUserName(ctx contractapi.TransactionContextInterface,
userName string) ([]DocumentQueryResult, error) {

	var queryString = "{\"selector\": { \"issuedBy\" : \"" + userName + "\"}}"

	results, err := getDocumentQueryResultForQueryString(ctx, queryString)

	if err != nil || results == nil || len(results) == 0 {
		return nil, err
	}
```

```
	return results, nil
}

func (s *SmartContract) ChangePassword(ctx contractapi.TransactionContextInterface, userName string, newPassword string) error {

	queryString := "{\"selector\": { \"userName\" : \"" + userName + "\"}}"

	results, err := getUserQueryResultForQueryString(ctx, queryString)

	if err != nil {
		return err
	}

	user := results[0].Record

	user.Password = newPassword

	userAsBytes, _ := json.Marshal(user)

	return ctx.GetStub().PutState(results[0].Key, userAsBytes)
}
```