ACADEMIC DOCUMENT AUTHENTICITY VERIFICATION USING BLOCKCHAIN TECHNOLOGY

ELIUTHERIUS JUMA WANYONYI

ICT-4-2733-18

A RESEARCH PROJECT SUBMITTED TO THE SCHOOL OF COMPUTING AND INFORMATICS IN PARTIAL FULFILMENT OF THE REQUIREMENTS FOR THE AWARD OF THE DEGREE OF BACHELOR SCIENCE, COMPUTER SCIENCE.

NOVEMBER 2019

DECLARATION

This research proposal is my original work and has not been presented for a degree in any other University for academic purpose.

ELIUTHERIUS JUMA WANYONYI

ICT-4-2733-18

Signed: _____ Date: _____

Supervisor Approval

This research proposal has been submitted with my approval as the university supervisor

Name: CATHERINE MUKUNGA

Signed: _____ Date: _____

DEDICATION

I dedicate this project to God Almighty my creator, my strong pillar, my source of inspiration, wisdom, knowledge and understanding. He has been the source of my strength throughout this program and on His wings only have I soared. I also dedicate this work to my brother and sister who have encouraged me all the way and whose encouragement has made sure that I give it all it takes to see it through. To my parents Mr. & Mrs. Robert who have been affected in every way possible by this quest and my good friend Celline Nanjala. Thank you. My love for you all can never be quantified. God bless you.

ACKNOWLEDGEMENTS

I would like to acknowledge the assistance and guidance offered by my supervisor Madam Catherine. Also, deep appreciation to the entire school of Computing and Informatics for all the support they offered, not forgetting my colleagues with whom we have worked closely to make the entire research a success.

DECLARATION ii
DEDICATION iii
ACKNOWLEDGEMENTS iv
CHAPTER ONE: INTRODUCTION 1
1.1 Background of the Study 1
1.2 Statement of the Problem 1
1.3 Objectives of the Study 2
1.3.1 General Objective 2
1.3.2 Specific objective 2
1.4 Research Questions 2
1.5 Purpose of the Study 3
1.6 Justification of the Study 3
1.7 Scope of the Study 3
CHAPTER TWO: LITERATURE REVIEW 4
Introduction 4
2.1 Block chain Technology 4
2.1.1 Strengths of Blockchain technology 4
2.1.2 Weaknesses of Blockchain technology 4
2.2.1 Blockchain for Cryptocurrency 5
2.2.2 Blockchain for Digital Identity 5
2.2.3 Blockchain for Real Estate 5
2.3 Blockchain Technology for Document Verification 5
2.3.1 Conceptual Framework 6
2.3.3 Existing works 6
2.3.3.1 Bitcoin Network 6
2.3.3.2 Block-certs Project by Massachusetts Institute of Technology Media Lab: 6
2.3.3.3 Blockchain based Academic Certificate Authentication System Overview by 7
Rujia Li, Yifan Wu, IT Innovation Interns 7
2.4 Summary and Identified Gaps 8
2.4.1 Blockcerts 8
2.4.2 Blockchain based academic certificate authentication system 8
2.5 Recommendation and future work 9
CHAPTER THREE: RESEARCH DESIGN AND METHODOLOGY 10
3.1 Introduction 10

3.2 Research Design 10
3.3 Target Population 10
3.5 Data collection instruments 10
3.6 Data analysis methods 10
CHAPTER 4: FINDINGS AND DISCUSSION 11
4.1 Introduction 11
4.2 Findings overview 11
4.3 Interpretation and explanation of the study findings with respect to stated research questions or hypothesis 13
4.3.1 Interpretation: 13
4.4 Nature of the findings 14
5.1 Introduction 15
5.2 Summary of findings 15
5.3 Weakness 15
5.4 Recommendation and future work 16
REFERENCES 17
APPENDICES 18
Appendix A: Project Budget 18
Appendix B: Project Schedule 19

LIST OF TABLES AND FIGURES

Table 1 : Continents 11
Table 2 Distribution Chart 12
Table 3 : Block chain adaptation 12
Table 4 : Project Budget 18
Table 5 : Project Schedule 19

Figure 1 Conceptual Diagram 6
Figure 2: Block chain based academic certificate verification. 8
Figure 3 : Project Comparison Chart 13

CHAPTER ONE: INTRODUCTION

1.1 Background of the Study

With each day passing by technology will always advance in ways that try to make life more efficient and improve convenience. As the world's population keeps on increasing, resources become minimal and people have to work extra harder to meet their needs. Jobs as well have not been spared and in fact many governments around the globe are always on the quest of creating more jobs for their citizens.

As mentioned earlier, the world's population is on the rise and as people strive to survive, they might just find themselves on the wrong side of the law. Technology has enabled people to easily forge academic certificates that might go under the radar without being noticed as a fake. However, on the brighter side, the same technology can be used to put measures in place to check for fake academic certificates.

This has been made possible, thanks to Satoshi Nakamoto, an anonymous person who introduced blockchain to the world. In his paper, published in 2008, Satoshi Nakamonto proposed an electronic payment system that would work on the basis of smart contracts, without the intervention of third parties between peer-peer transactions. Later in 2009, Satoshi introduced the bitcoin cryptocurrency that has ever since, gained popularity and trust around the globe.

Different applications of the blockchain technology have then been innovated since the introduction of blockchain to date, including the use of the technology in document verification. This innovation comes in handy, as this research is intended to bring to light the works that already exist on academic document verification and how to improve on them.

1.2 Statement of the Problem

Many people get certified on annual basis. The academic institutions that they attend offer them certificates as proof that they have been certified for the stated course on their certificate. The certificates range from skills certificates to bachelor's degree certificates. Employers usually request for these certificates whenever they want to employ workers. Some of the job applicants usually try to cheat the system by presenting fake certificates during the job recruitment process or interview. Unsuspicious employer might not take time to verify these documents and end up with quacks in his/her labour team.

However, if they want to verify, they can contact the university that the candidate attended and make an inquiry if the certificate is genuine. This process is long and is dependent on the university that the inquiry is made. In case the candidate colludes with the university to lie about the certificate, it would be very hard to detect fake certificates.

This problem can however be solved through the implementation of Smart academic certificates that are based on the blockchain technology. These certificates are forge proof and easy to verify.

1.3 Objectives of the Study

1.3.1 General Objective

The general objective of this research is to have a scrutiny on bitcoin and blockchain technology, the applications of this technology and focus on how it can be implemented in academic document verification in order to get rid of fake certificates.

1.3.2 Specific objective

1. To find out the existing systems for document verification using blockchain.
2. To investigate the various applications of block chain technology
3. To find out the suitability of a sub-system that can counter the weaknesses of the existing systems for document authenticity verification.

1.4 Research Questions

1. What are the existing blockchain based document verification systems?
2. What are various applications of block chain technology?
3. What are the strengths and weaknesses of a document verification system?

1.5 Purpose of the Study

The research will focus on the existing platforms that are used for document verification using the blockchain technology. From the research, strengths and weaknesses of the existing platforms will be weighed and a recommendation will be proposed.

1.6 Justification of the Study

The biggest merit of this research is that it will assist in academic certificate verification. When people are employed with fake certificates, institutions and corporations are likely to face huge loses because of having quacks who don't understand the job. However, employing people with fake certificates can be significantly reduced by have an instant way of verifying certificates. This can be achieved by the help of using blockchain technology.

This research comes in handy in helping to understand the relationship between blockchain technology and bitcoin. The researcher will analyze the existing methods of document verification using blockchain by studying their weaknesses and strengths and then giving a recommendation on how to improve these systems.

1.7 Scope of the Study

The study will focus on document verification using blockchain technology. In this research, the researcher will take a look at the authenticity of the certificates issued over the bitcoin network and how to increase the authenticity of certificate issuer within the network instead of anyone being able to issue academic certificates.

CHAPTER TWO: LITERATURE REVIEW

Introduction

This chapter reviews the theories related to Blockchain technology, Document verification, conceptual framework of the research, related work and the gaps in literature.

2.1 Block chain Technology

A blockchain is a distributed database that records transactions or even digital events that have been executed or performed and shared among the participating parties. Each transaction can be verified by mode of consensus of a majority of the members in the system. And, recorded information in the chain can never be altered or erased. Each of the transactions made on the blockchain is certain and verifiable. To use a basic analogy, it is easy to steal a book from a secluded room that has no people than stealing the same book from a big hall containing many people observing you.

2.1.1 Strengths of Blockchain technology

Blockchain has a big advantage as it has a database that is directly shared without the need of a central administrator. Instead of a central application logic, blockchain transactions are validated and authorized on their own. Therefore, with the blockchain acting as a consensus mechanism, there is independence on verification and processing of transactions. Andoni. (2018).

2.1.2 Weaknesses of Blockchain technology

Verification of signature. This is necessary although their computation is complex and can cause bottleneck on the network. In comparison, centralized databases do verification only once and subsequent requests do not need more verification.

Consensus mechanisms. In the blockchain database, effort should be put in place to ensure a consensus is reached in the network. This may involve too much back-and-forth communication. Compared to centralized database, blockchain will involve too much communication since a consensus involves several members of the network.

Redundancy. Centralized database will always process transactions once or twice while in a blockchain, the same transaction is processed independently by every member of the network. This results to the need of more work to be done in quest for the same result.

2.2 Applications of Blockchain Technology

2.2.1 Blockchain for Cryptocurrency

Bitcoin is the first cryptocurrency that implemented the distributed ledger technology and was invented back in 2009. From there since it has gained popularity and traction by business owners who feel the need for a distributed trust model where they can perform their transactions.

2.2.2 Blockchain for Digital Identity

Using blockchain for identity recognition purpose can be the next big source of integrity when it comes to user identity. For companies this will mean they will not incur costs for storing user data in the database. This model will also benefit users since their identity data will be easily accessible and they will have more control over their personal data.

2.2.3 Blockchain for Real Estate

Real estate industry involves several parties. For efficiency, these parties need trust among themselves. Blockchain can introduce an element of trust among these individuals. The properties can be stored in the blockchain with their history and will provide all necessary information at its time of need: information such as history of the property ownership.

2.3 Blockchain Technology for Document Verification

Verification of documents is very important while dealing with counterfeit documents. With these documents in a shared environment, it becomes hard for anyone to alter their contents or come up with fake documents and present them as real. This will also make document verification fast and effective.

2.3.1 Conceptual Framework

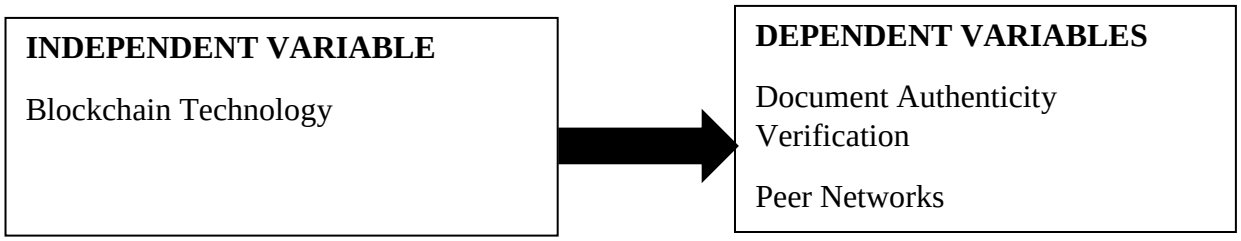


Figure 1 Conceptual Diagram

2.3.3 Existing works

2.3.3.1 Bitcoin Network

Back in 2008, a group writing under the name of Natoshi Nakamoto published a paper entitled “Bitcoin: A Peer-To-Peer Electronic Cash System”. The paper explained a peer-to-peer electronic cash system that would allow users to conduct online payment transactions directly from one person to another, eliminating the need for a third party as a bond of trust within the transaction. Basically, these third parties are the financial institutions. A cryptocurrency by the name Bitcoin was the first realization of this concept (peer-to-peer transactions). Up to date, Satoshi Nakamoto is anonymous, hence no one knows who really is the founder of this blockchain technology. A few months after publishing the Peer-to-peer electronic cash system, an open source program implementing the new protocol was released that began with the Genesis block of 50 coins. Anybody can install the Genesis Block and take part in the bitcoin network.

Bitcoin introduction journey:

2008

• **August 18 -** The Domain name "bitcoin.org" was registered

• **October 31 –** A paper describing the Bitcoin design was published

• **November 09** -Bitcoin project was registered at SourceForge.net

2009

• **January 3 -**Genesis block was established

• **January 9 -**Bitcoin v0.1 was released and then announced on the cryptography mailing list

• **January 12 -**First Bitcoin transaction, in block 170 from Satoshi to Hal Finney

2.3.3.2 Block-certs Project by Massachusetts Institute of Technology Media Lab: J. Philipp Schmidt, Juliana Nazare

This project, which was done by the Media Lab Learning Initiative and Learning Machine builds an environment that enables users to create, share and verify all educational certificates that are blockchain based. These digital certificates have to be registered on the Bitcoin blockchain and then cryptographically signed by members who participate in the blockchain network. The system is divided into three major parts:

1. Cert-schema: Cert-schema explains the entire process of making a digital certificate. This is done by the use of a JSON file which has all the necessary fields that are required for the cert issuer code to place it on the blockchain network. Needed for our cert-issuer code to place it on the blockchain.
2. Cert-issuer: This module takes the JSON certificates that have been made by the cert-schema and issue them via a transaction from the issuer to the recipient on the Bitcoin blockchain. At this stage, the certificate has a unique hash that represents it.
3. Cert-viewer: The Cert-viewer displays and verifies the certificates after they have been issued to the learners. It also provides for the learners to make their own bitcoin identity and also request for a certificate.

2.3.3.3 Blockchain based Academic Certificate Authentication System Overview by Rujia Li, Yifan Wu, IT Innovation Interns

This system was proposed as an improvement to the blockcert which was created by the MIT media lab. Among the short comings that they realized from the blockcerts based academic document verification included;

- utilizing a multi-signature scheme to ameliorate the authentication of certificates
- exerting a safe revocation mechanism to improve the reliability of certificates revocation
- establishing a secure federated identification to confirm the identity of the issuing institution.

The system (Rujia Li, Yifan Wu, IT Innovation Interns, 2016) is composed of four major components. These components are what make up the entire system and implement the bitcoin network for document verification. These components include:

- verification application which includes a federated identity,
- An issuing application that involves a multi-signature and Bitcoin-address based revocation system,
- Blockchain

- local Database (MongoDB)

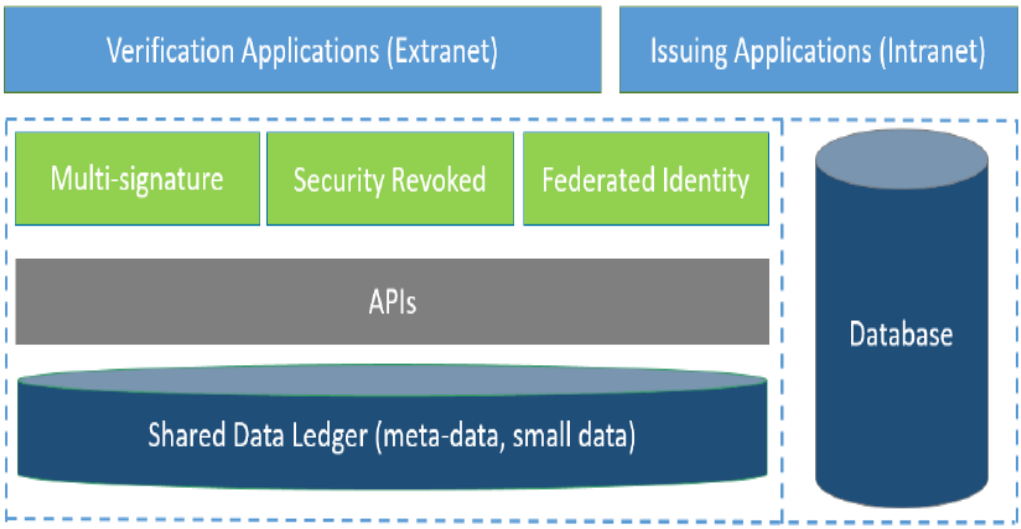


Figure 2: Block chain based academic certificate verification.

The issuing applications take charge of the heavy lifting duties which include: Application of the certificates, certificate examination, signing the certificate and issuing of the same. In addition, the issuing applications are the ones responsible for revocation of the certificates.
The verification application checks on the authenticity and integrity of all certificates issued.
The blockchain is the party of trust and also acts as the database(distributed) which saves the authentication data. The MongoDB was used as the database is friendly in working with JSON-based certificates and it also provides high availability and it is also highly scalable. Rujia Li, Yifan Wu, IT Innovation Interns. (2016)

2.4 Summary and Identified Gaps

2.4.1 Blockcerts

Blockcerts is a certificate verification system that was launched by MIT Media Lab in June 2016. Blockcerts makes use of the Bitcoin blockchain which acts as the infrastructure of trust and the database. This infrastructure removes the dependence on third parties and advocates for transparency in any network transactions.
Blockcerts is a nice system but it does not provide for the authenticity of issuing institutions. This turns out to be a major problem that anyone in the network can issue certificates.

2.4.2 Blockchain based academic certificate authentication system

Basically, this system works as follows:
Firstly, the student requests for a credential from his/her school of choice.

The school confirms the student's information and matches it with a bitcoin transaction once it has been approved.

After that, the other schools in the network sign the transaction with their own private keys.

The student then is issued with a JSON-based certificate.

When applying for a job, the student will present the certificate to the employer who will then check whether the certificate is a fake through the blockchain network.

This will be achieved by checking for the authentication code by comparing the one issued by the student and the one that is in the bitcoin network.

Although the system is self-sufficient, there needs to be an authoritative body that verifies the institutions joining the network. Leaving it open may lead to un-necessary population within the peer-peer BTC network.

2.5 Recommendation and future work

There need to be a third party that ensures only verified institutions are able to join the network and issue standard certificates. This can be done by introducing a moderating peer-node with the same privilege as the other peers but oversights all the peers(institutions) that offer certificates.

With this recommendation, less man-power will be required and it will see more efficiency in handling counterfeit certificates. However this system will not leave room for errors. Any errors in the system will stick there forever once it is added to the block chain. If the proposed sub-system can be built on top of the blockchain technology, changes can be affected before the data is committed to the blockchain. This is where the oversight will come in handy. This will enhance the regulation of institutions issuing certificates and ensure credibility of the certificates within the block chain network.

CHAPTER THREE: RESEARCH DESIGN AND METHODOLOGY

3.1 Introduction

This chapter presents the various methods or procedures which will be used in studying the research problem. The subsections under this chapter include; research design, target population, sample size, sample size and sampling procedures subject to research (sampling design), instruments of collecting data and data analysis methods.

3.2 Research Design

In this research the type of research design that will be used is descriptive research design using observational study and data collection from secondary sources. Most of the universities under review by the researcher which include: Princeton University | USA and Universidad Europa Madrid, have published information on their websites that will assist the researcher with data collection.

3.3 Target Population

The research study will target data published by Universities that offer block chain education such a University of Nicosia and those that offer block chain based document authenticity verification such as Barkley University. Also, the research will target the block cert project by Mat lab on block chain document verification using the bitcoin network.

3.5 Data collection instruments

The researcher will primarily collect data from recorded sources. The secondary data will be collected through analysis of secondary sources such as official university websites.

3.6 Data analysis methods

The data collected will be analysed using Atlas tool for qualitative data. Quantitative data collected from observation of the published data will be analysed using SPSS.

CHAPTER 4: FINDINGS AND DISCUSSION

4.1 Introduction

This chapter will cover the findings that the researcher found out. The researcher gives an overview of the findings and discusses the findings in details. The findings are based on the research objectives and intends to answer the research questions. Graphical presentation of data has been presented by the researcher for easier interpretation and understanding. In the findings, the researcher has provided both positive and negative arguments concerning the research.

4.2 Findings overview

In my research, I had a quest of finding out the number of institutions that are using blockchain-based verification of academic certificate authenticity.

First, I had to find some of the universities that are offering studies in Blockchain technology among them included:

University of Nicosia | Cyprus

Princeton University | USA

Universidad Europea Madrid

Duke University | USA

The University of California, Berkeley | USA

In my findings, it was evident that most of these universities are in Europe and the united states. These two continents share a 50/50 distribution of the universities as shown in the graph below:

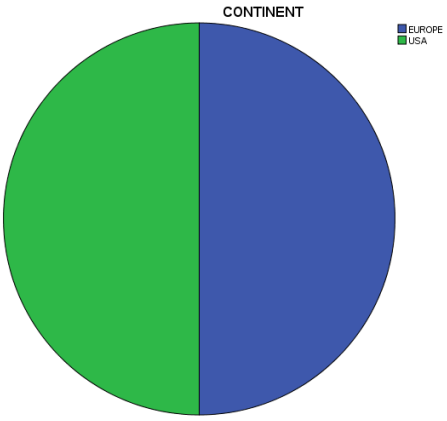
How are the universities spread out in continents?

Table 1 : Continents

CONTINENT

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	EUROPE	3	50.0	50.0	50.0
	USA	3	50.0	50.0	100.0
	Total	6	100.0	100.0	

Table 2 Distribution Chart



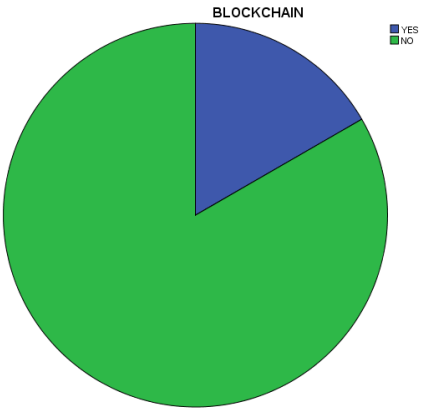
I also had a task of finding out how many universities offer their certificates through the blockchain network. Among the six universities, only one was offering their certificates through the blockchain network. This formed only 16% of the total population in my sample.

How many offer verifications using block chain?

Table 3 : Block chain adaptation

BLOCKCHAIN

		Frequency	Percent	Valid Percent	Cumulative Percent
Valid	YES	1	16.7	16.7	16.7
	NO	5	83.3	83.3	100.0
	Total	6	100.0	100.0	



4.3 Interpretation and explanation of the study findings with respect to stated research questions or hypothesis.

During the research, I had to formulate my units of measure. These were used to check the success of the systems used for document verification. The units included:

The success rate of the verification models themselves based on:

- Security
- Forgery
- Authenticity
- Longevity
- Time consumed for process completion
- Incurred costs

These units were used to compare the application of Blockchain between University of Nicosia, Block cert and our proposed project. The Multiple bar diagram below is a graphical representation of the findings.

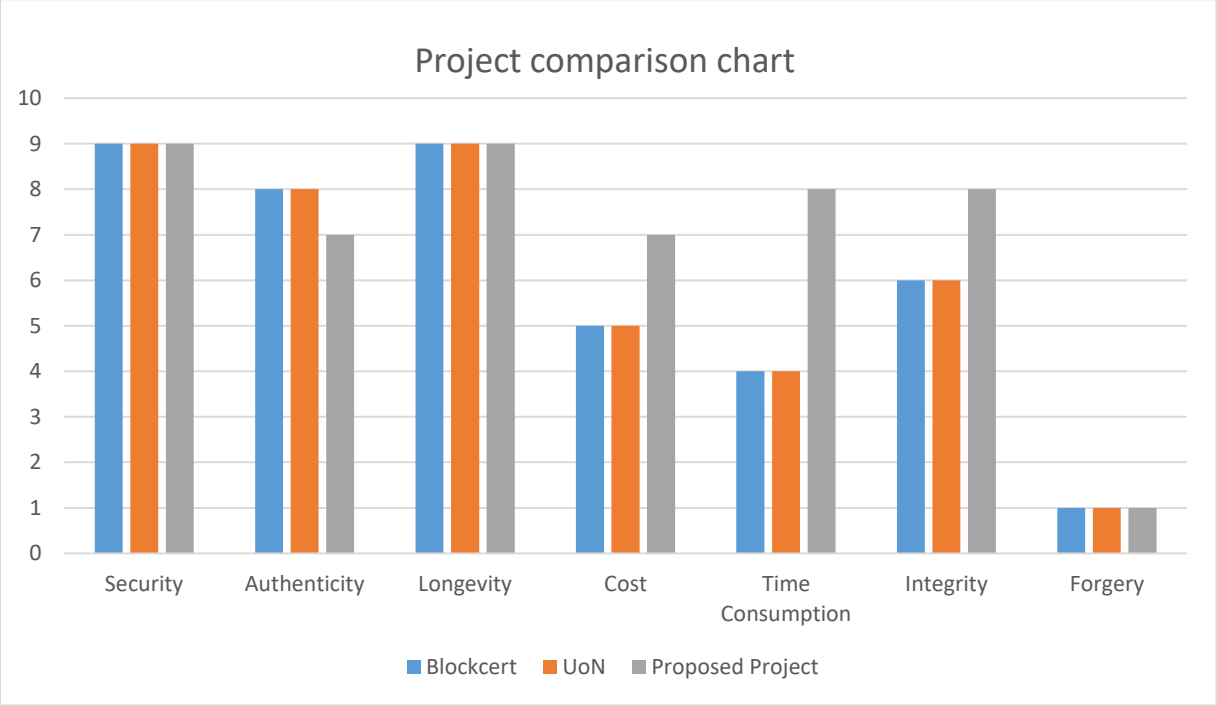


Figure 3 : Project Comparison Chart

4.3.1 Interpretation:

Security: On a scale of ten, they all scored 9. This is because all of the projects implemented the same security measures as the one used in bitcoin network.

Authenticity: By introducing a third party to the network, the authenticity of the documents might be compromised. The main aim of blockchain network is to get rid of the third party, which my research proposes to introduce.

Longevity: This means that the blockchain document will be in existence even if the institutions that offered these certificates are not in existence any more. These certificates will still be in the network and anyone who wishes can verify them.

Cost: The proposal will add additional mining costs for document authenticity checks when they are passed to the third party. This is the broadcasting fees that the university will be required to pay for miners to confirm the issued certificates on the block chain.

Time Consumption: A third party will mean the time consumed will be twice the time used between peer-peer document verification. The verification process will include two levels which will consume twice as much time as it were only one level. This means the proposed project will consume more time to verify the documents.

Integrity: Integrity of the documents will be protected by the third party whose responsibility is to ensure only certified institutions can offer certificates within the network. In this case, the proposed project scored higher in terms of integrity.

Forgery: Theoretically, it is impossible to introduce a fake certificate in a block chain network. In all the three projects, the same methods of peer confirmation are used and hence it is easy to detect fake certificates in all of them. This makes forgery a near impossible act.

4.4 Nature of the findings

In the findings, the researcher found out that most of the universities that offer their certificate via the blockchain network are distributed between Europe and USA. Africa and Asia did not have tertiary institutions that offer their certificates via blockchain network. However, the blockchain technology was implemented in other areas such as currency transactions. Also, blockchain studies are gaining momentum across all other continents.

In the reseachers findings, only one university was offering blockchain based certificates. However, other institutions such as university of California are in their testing phase of fully implementing the blockchain based certificates.

CHAPTER 5: SUMMARY, CONCLUSIONS AND RECOMMENDATIONS

5.1 Introduction

This chapter summarizes the research findings. It summarizes the findings on the viability of implementing the research findings and the implications it will have. This chapter is the conclusion of the research document and also has the recommendations drawn from the research findings.

5.2 Summary of findings

Existing blockchain based authenticity verification tools that were found by the researcher were the Blockcert by Matlab and University of Nicosia. They both implement the same technology and use the bitcoin blockchain to verify the authenticity of documents.

Apart from document authenticity verification, it has been discovered through the research, that blockchain technology has numerous other applications among them being: Cryptocurrency which is widely used blockchain application, Digital Identity, Real estate among other uses.

Also, the research has identified a weakness in introducing a third party to the blockchain network which has been elaborated in section 5.3 of this chapter.

5.3 Weakness

This research proposes a third-party verifier. However, this beats the logical purpose that blockchain intends to serve. Blockchain intends to get rid of the need for third party to verify authenticity of transactions. By introducing a third-party into the verification process, more resources will be consumed. First and foremost, blockchain transactions consume a lot of processing power and this will even worsen by the introduction of a third-party which will only make the process lengthy.

Additionally, this project will add additional mining costs for document authenticity checks when they are passed to the third party. This is the broadcasting fees that the university will be required to pay for miners to confirm the issued certificates on the block chain.

5.4 Recommendation and future work

There need to be a third party that ensures only verified institutions are able to join the network and issue standard certificates. This can be done by introducing a moderating peer-node with the same privilege as the other peers but oversights all the peers(institutions) that offer certificates.

With this recommendation, less man-power will be required and it will see more efficiency in handling counterfeit certificates. However, this system will not leave room for errors. Any errors in the system will stick there forever once it is added to the block chain. If the proposed sub-system can be built on top of the blockchain technology, changes can be affected before the data is committed to the blockchain. This is where the oversight will come in handy. This will enhance the regulation of institutions issuing certificates and ensure credibility of the certificates within the block chain network.

REFERENCES

Michael Crosby, Google. (2015). Sutardja Center for Entrepreneurship & Technology Technical Report. Berkley: University of California

Woochul Song. (2016). Blockchain Technology: Advantages and disadvantages of Blockchain Technology. Retrieved from BlockchainTechnologycom Website: https://blockchaintechnologycom.wordpress.com/2016/11/21/advantages-disadvantages/

Issam (Sam) Andoni. (2018). Forbes Technology Council: Blockchain as an application Platform. Retrieved from Forbes Website: https://www.forbes.com/sites/forbestechcouncil/2018/05/07/blockchain-as-an-application-platform/

University of Birmingham Rujia Li, Yifan Wu, IT Innovation Interns. (2016). Blockchain based Academic Certificate Authentication System Overview: Retrieved from UoB Website: https://intranet.birmingham.ac.uk/it/innovation/documents/public/Experiments/Blockchain-based-Academic-Certificate-Authentication-System-Overview.pdf

J. Philipp Schmidt, Juliana Nazare, Juliana Nazare.(2016). Digital Certificates Project. Retrieved from Media.mit website: http://certificates.media.mit.edu/

Bamford, A.; Wimmer, M. 2012. The Role of Arts Education in Enhancing School Attractiveness: a literature review. EENC Paper. http://www.interarts.net/descargas/interarts2548.pdf.

National Advisory Committee on Creative and Cultural Education (NACCCE). 1999. All Our Futures: Creativity, Culture and Education. London: Department for Education and Employment. Retrieved from: http://files.eric.ed.gov/full text/ED440037.pdf.

Yong Shi, Secure storage service of electronic ballot system based on block chain algorithm, Taiwan, R.O.C.:Department of Computer Science, Tsing Hua University, 2017

University of Nicosia (UNIC). (2017) Publication of Academic Certificates Retrieved from UNIC website: https://www.unic.ac.cy/iff/blockchain-certificates/

OSE-Lab Smart contracts whitepaper, (2015)Available: https://github.com/OSE-Lab/learning-blockchain/blob/master/ethereum/smart-contracts.md.

University of California Berkley USA. (2015) BlockChain Technology Beyond Bitcoin. Retrieved from the Berkley.edu website: https://scet.berkeley.edu/wp-content/uploads/BlockchainPaper.pdf

APPENDICES

Appendix A: Project Budget

Table 4 : Project Budget

	TASK	AMOUNT(Ksh)
1	Printing and Binding	**1,000.00**
2	Consultation	**5,000.00**
3	Laptop	**30,000.00**
4	Internet Connection	**5,000.00**
5	Data collection	**1,000.00**
TOTAL		**42,000.00**

Appendix B: Project Schedule

The project schedule has been summarized in the Gantt chart below.

Table 5 : Project Schedule

MONTH / PROCESS	SEP	OCT	NOV	DEC	JAN	FEB	MAR
Problem Definition and Research project Analysis							
Literature review preparation							
Proposal defence presentation							
Data collection							
Data analysis							
Documentation							
Research Project Review and Presentation							