Application of Blockchain Technology in Education in storing academic records

By

LUKEERA MICAHEL ELYWIN
S19B23/656

DEPARTMENT OF COMPUTING AND TECHNOLOGY
FACULTY OF COMPUTING AND TECHNOLOGY

Email Address: lukeeraelywin@gmail.com; Phone Number: +256778607862

A Project Proposal Submitted to the Faculty of Science and Technology for the Study Leading to a Project in Partial Fulfillment of the Requirements for the Award of the Degree of Bachelor of Science in Computer Science of Uganda

Christian University.

SUPERVISOR

Mr. SSEJJUKO RONALD

Email...............

Phone:...................

FEBRUARY 2022

DECLARATION

I declare that this Research Proposal is my original work. Where other people’s work has been used, I have correctly acknowledged it following the university standards.
I confirm that I have not used work previously produced by another student or any other person to hand in as my own.
I have not allowed and will not allow anyone to copy my work to pass it off as his or her work.

Signature......................................
LUKEERA MICHAEL ELYWIN

CHAPTER 1 INTRODUCTION

BACKGROUND OF STUDY

Blockchain is the core technology used to create the cryptocurrency, Bitcoin, through the maintenance of immutable distributed ledgers in thousands of nodes proposed by Satoshi Nakamoto in 2008 (Nakamoto 2008). It has been considered part of the fourth industrial revolution since the invention of the steam engine, electricity, and information technology (Chung and Kim 2016; Schwab 2017). It has the potential to transform the current Internet from “The Internet of Information Sharing” to “The Internet of Value Exchange.” Blockchain technology is expected to revolutionize the operating modes of commerce, industry, and education, as well as to promote the rapid development of a knowledge-based economy on a global scale. Due to its immutability, transparency, and trustworthiness for all transactions executed in a blockchain network, this innovative technology has many potential applications (Underwood 2016). During the initial stages of its appearance, blockchain technology was not able to draw a lot of attention. However, as Bitcoin continues to run safely and steadily over the years, society has since become aware of the enormous potential of the underlying technology of this invention in its application not only in cryptocurrency but also in many other areas (Collins 2016). Blockchain technology has become a hot topic for more and more countries, institutions, enterprises, and researchers. Presently, blockchain technology has been applied in various fields such as cryptocurrencies in the financial area, which includes Bitcoin, Ethereum, Zcash (Zerocash), etc. Bitcoin is the first peer-to-peer payment network of electronic cash based on blockchain technology. One of the crucial features of blockchain technology is how many nodes in a distributed blockchain network maintain consensus and the Bitcoin blockchain network adopts a hash-based Proof-of-Work (PoW) distributed consensus algorithm (Nakamoto 2008). Ethereum is an open-source, public, blockchain-based distributed computing platform featuring smart contract functionality using a proof-of-stake consensus algorithm (Beck et al. 2016). Zcash is a decentralized and open-source cryptocurrency like Bitcoin. However, it offers better privacy and selective transparency of transactions by using a proof-of-zero-knowledge consensus algorithm. Zcash payments are published on a public blockchain, but the sender, recipient, and amount of a transaction remain private (Peck 2016). Besides, some organizations and enterprises are also trying to develop decentralized platforms based on blockchain technology. For example, Arcade City, the so-called “Uber Killer,” is a ride-sharing company that has integrated its model into Ethereum, including identity and reputation systems (Zheng et al. 2017). Ubitquity is a digital property management company that offers secure recording and tracking records built on a blockchain platform.

Swan (2015) indicated that the development of blockchain applications could be divided into three stages; Blockchain 1.0, 2.0, and 3.0. Blockchain 1.0 is the deployment of cryptocurrencies as a peer-to-peer cash payment system. Blockchain 2.0 is a more extensive blockchain application than simple cash transactions, including stocks, bonds, loans, smart property, and smart contacts. Blockchain 3.0 is developing blockchain applications beyond currency, finance, and markets, such as in the areas of government, health, science, literacy, culture, and art. According to the previously mentioned principle, the current applications of blockchain is still in the 1.0 and 2.0 stages. Most people do not know about the term “blockchain,” not to mention the potential applications of using blockchain technology. Although researchers discussed the usage of blockchain in the commercial areas (Swan 2015), several studies focused on how blockchain technology can be applied in education (Devine 2015; Sharples and Domingue 2016).

PROBLEM STATEMENT

Academic records of a person, such as degrees, diplomas, are separated data, stored in the databases of various providers of education and students or graduates do not have the authority to manage their own information. Moreover, no other unofficial person (e.g. an employer) has access to modify or even view these official records, in the context of heightened internationalization of education and work with the increasing mobility of students and graduates, easy access to the personal degree record is paramount.

PURPOSE

This study examines the usability of blockchain technology in storing academic records of a person, such as degrees, diplomas, and any other certificates and ease of access.

Specific Objectives

Blockchain technology has limitless possibilities and could become an extensive part of education systems. Some benefits of adopting blockchain technology in the field of education are the following
(but are not limited to):

- Reliability: Make information unchanged, immutable, and distributed over time in that any system participant can verify the authenticity of data and be certain it has not been tampered with thus the records are secure.
- Availability: Allow users to control their data through private and public keys, allowing them to own it.

SIGNIFICANCE

This study is significant since blockchain gives students ownership of their personal records, allowing them to control their academic identity. This makes proving the accuracy of the credentials on their resumes much easier for graduates who are job hunting, for example, and gives them more control over what an employer can access.

SCOPE/LIMITATIONS

The area of study is based on Uganda Christian University and it is to impact the graduates, its limited to storing academic documents.

CHAPTER 2 LITERATURE REVIEW

INTRODUCTION

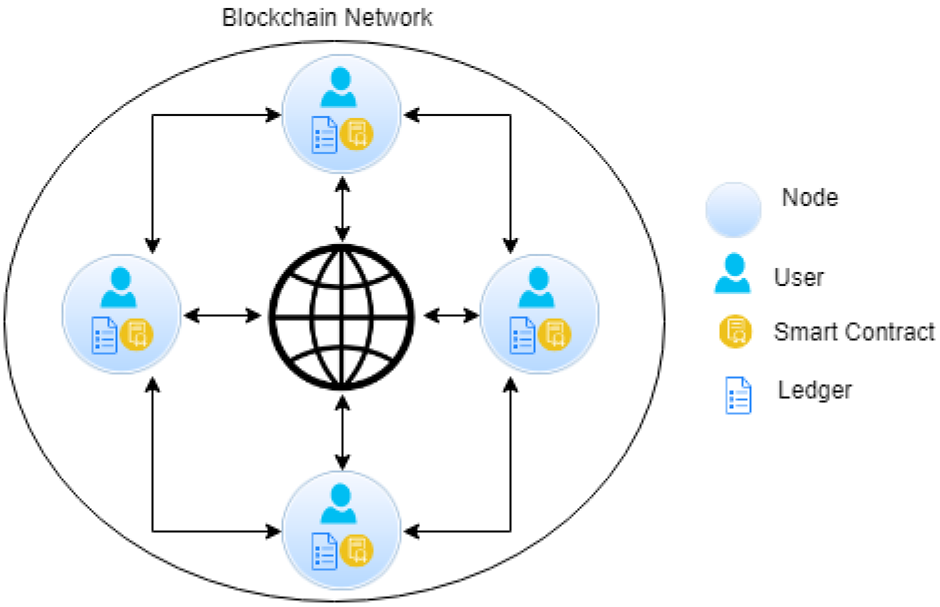
The certification procedures are part of our everyday life. A certificate is a verification of the existence or possession of declared characteristics or acquired competencies. In most cases, the certificate is issued by an institution and handed in paper form to the holder. These bureaucratic procedures are time-consuming, and expensive and leave plenty of opportunities to issue fake documents. The advancement of technology offers a plethora of tools to the scammers to falsify the paper certificates, hence having a technology that
offers protection against these malicious activities is quite beneficial. Blockchain technology shows great potential to avert the corruption of certifications. The characteristics of the blockchain technology, like, auditability, immutability, non-repudiation, transparency, verifiability, and irrevocability, make it a perfect candidate for enhancement of the traditional certification procedures. These characteristics make blockchain technology suitable for any type of application where certification is needed. This includes the certification of origin, possession, quality level, class, properties, measured parameters, some features, and location while tracing the movement, or similar. This proposal introduces one of the pioneering works in the field of blockchain usage as certificate storage. The proposed application shows the potential to overcome the long bureaucratic procedures and prevent fraudulent activities during the certification procedures. It uses blockchain technology, also known as Distributed Ledger Technology(DLT), which is transforming the activities in a trustless environment and still keeps a single truth in the whole system.

The implementation of blockchain technology for building an online certificate database will increase the commodity of living and ease up the administrative procedures to issue and verify the certificates. The problem with fake education diplomas is present in many countries. Especially it is tricky to overcome during the process of mutual recognition of foreign diplomas. In, Sayed points out the crucial characteristics of the blockchain technology to overcome the fake diploma problem and mentions a few projects related to the application of blockchain technology. Furthermore, the author analyzes the fraudulent activities regarding fake diplomas and proposes a structure for a concrete blockchain-based application to overcome the problems. Besides the potential to overcome fraudulent activities over the certification and validation process, the implementation of blockchain-based applications for certification will also have a financial impact. The financial impact and potential business model are analyzed in. Tariq et al. in are developing a blockchain-based accreditation and degree verification system by the use of Ethereum Blockchain. The uniqueness of the proposal is the implementation of the private version of the Ethereum Blockchain in order to keep the system under the Proof-of-Authority consensus mechanism. A similar approach to implementing a private type of blockchain is described in. They are using the Hyperledger Sawtooth enterprise blockchain in order to manage

the credentials and privileges in a system. In contrast to these approaches, the application presented here is implemented on a public blockchain. It
offers a complete decentralization of the database while keeping the robustness of the application and managing the credentials of the users. In addition to the use case of blockchain-based diploma certificate management, there are use-cases where the blockchain technology is used as a certificate management mechanism for a birth certification, certificate revocation lists, green certification in the energy sector, product compliance, and assurance in the construction industry, endorsement and forestry certification.

Blockchain Technology

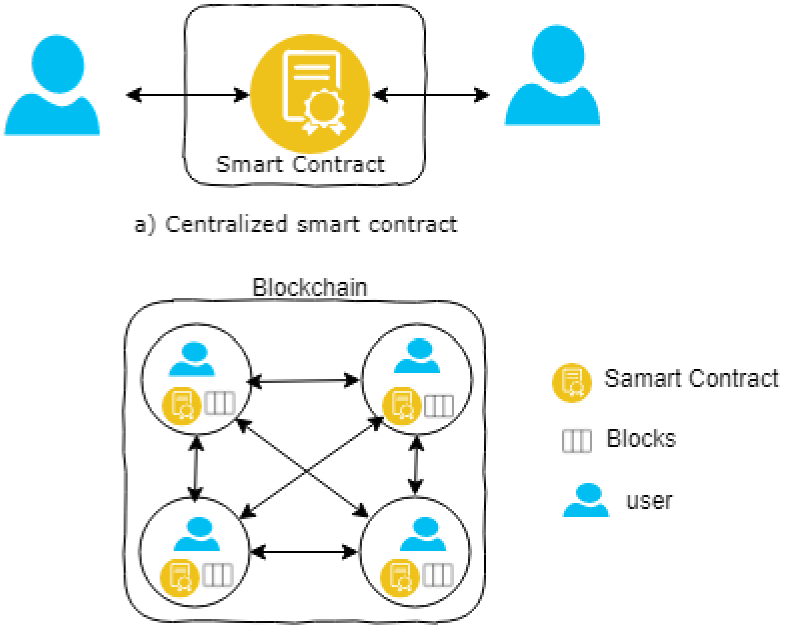
Blockchain is a distributed database that stores the transactions sent between the participants in a secure and immutable way. Blockchain is a P2P network that allows nodes (peers) to collaboratively maintain the network for block and transaction exchange Therefore, there is no need for a third trusted party since the participants can communicate and send transactions between each other directly. A cryptographic hash identifies the block, and each block references the previous one, which creates a chain of blocks (Figure 1). Each block contains several transactions, and the maximum size of each block varies according to the blockchain platform type, for example, 1 Mb in Bitcoin and between 20 to 30 kb in Ethereum. The blocks in the chain are immutable and cannot be changed, which prevents the double-spending problem.



The second generation of blockchain has emerged in the form of Ethereum, which allows for building and implementing distributed applications. The Ethereum blockchain allows smart contracts to be built on top of it, and this has opened the door for researchers to integrate blockchain into various fields. Blockchain has generally been divided into two main types: public and private blockchain. Public blockchain (such as Ethereum) allows anyone to join and participate in the network. In contrast, in a private blockchain (such as Ripple), only users with permissions can join and participate in the network.

Smart Contracts

A smart contract refers to an event–condition–action stateful computer program that is carried out between two or more parties who do not have implicit trust in one another. In other words, it is a self-executed code that is run to apply roles and conditions between two or more parties. By applying a smart contract using blockchain technology, there is not only a reduction in third-party costs within the transaction process but there is also improved transaction security. A smart contract can be either centralized or decentralized; it can be implemented to run off-chain in a centralized environment or to run on blockchain in a decentralized environment



a) Centralized smart contract

b) Decentralized smart contract

Blockchain and Smart Contract Applications within Education

In recent years, the role of blockchain applications in education has received increasing attention across several disciplines. Blockchain and smart contract technologies are increasingly involved in education in different means and forms. For example:

- Digital certificate applications: These applications are intended to provide greater control over the students' earned certificates and to decrease dependence on third-party intermediaries – including employers and universities – for storing, verifying, and validating credentials. Examples are Open Blockchain and the Blockcerts project.

BLOCKCHAIN-BASED CERTIFICATE STORAGE

Blockchain technology is a decentralized data storage structure, capable of operating in a trustless community, tracking, and recording modifications, and reducing the need for third parties. Moreover, the blockchain database structure, also known as the distributed ledger, offers liveness, immutability, redundancy, and non-repudiation of the records. The database structure model of the blockchain technology is presented in Fig. 2. The records in the blockchain database are organized in blocks, where the blocks are generated in predefined time intervals. All the information generated in one blockchain network is stored in every participating node, thus creating a complete copy of the common database of the system, in every participating node. This property makes the database structure redundant, reliable, and very robust.

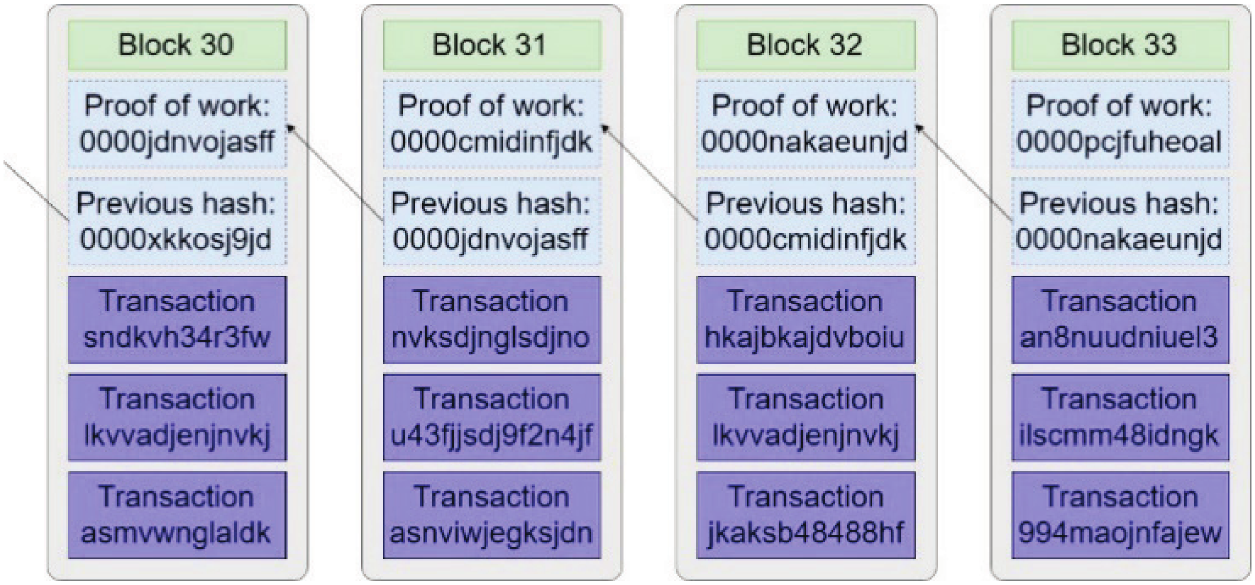

Block 30
Proof of work: 0000jdnvojasff
Previous hash: 0000xkkosj9jd
Transaction sndkvh34r3fw
Transaction lkvvadjenjnvkj
Transaction asmvwnglaldk
Block 31
Proof of work: 0000cmidinfjdk
Previous hash: 0000jdnvojasff
Transaction nvksdjnglsdjno
Transaction u43fjjsdj9f2n4jf
Transaction asnviwjegksjdn
Block 32
Proof of work: 0000nakaeunjd
Previous hash: 0000cmidinfjdk
Transaction hkajbkajdvboiu
Transaction lkvvadjenjnvkj
Transaction jkaksb48488hf
Block 33
Proof of work: 0000pcjfuheoal
Previous hash: 0000nakaeunjd
Transaction an8nuudniuel3
Transaction ilscmm48idngk
Transaction 994maojnfajew

Figure 2 The structure of the blockchain

As presented in Fig. 2, the blocks are connected in a single-chain formation. The connection between two consecutive blocks is through the common data field known as-block hash. The block hash is calculated by use of a cryptographic hash function, which is a one-way function that creates a fingerprint of the block of records, that is unique and irreversible. The block hash is calculated for the current data block and it is set in the header data of the next data block. The implementation of hashing function in the process of block creation and linking the data blocks in this way makes the record in the database tamper-proof. Practically even the smallest change in a data record will significantly change the block hash, which will represent an attempt for modification of the database. Regarding the type of hash functions, the Bitcoin network uses SHA-256 and RIPEMD-160 algorithms, while Ethereum uses the KECCAK-256 algorithm, which is not following exactly the FIPS 202 standard, also known as the SHA-3 algorithm. Besides the hash function, blockchain technology deploys encryption functions to provide security to the user wallet and digital signature for the transactions. The main encryption algorithm is the Elliptic-curve encryption algorithm, using the elliptic curve (EC)
y 2 = x 3 + ax + b over a finite Galois field (GF) defined with a prime number p. Encryption algorithms over the elliptic curve work in a way that an algebra over the elliptic curve plus a neutral point at infinity is defined. Using this algebra means that any sum of two different or two same points will give again a point on the same elliptic curve. Adding the point to itself, which is multiplying by two, will again give another point on the curve. Hence we can add the same point to itself multiple times, which defines the operation of multiplication as in classical arithmetic. Elliptic curve cryptography (ECC) algorithms start from a base point G and this point is
multiplied by a number that represents the private key k. Using the addition rules of the ECC algebra, one can get a point that is equal to the point
K = kG = G + G + ... + G. This will represent the public key K that corresponds to the private key k, using the given curve. Bitcoin and Ethereum use the Elliptic-curve Digital Signature Algorithm (ECDSA), with the elliptic curve secp256k1. This curve has the following parameters:

- p = 2 256 – 2 32 – 2 9 – 2 8 – 2 7 – 2 6 – 2 4 – 1
- a = 0, b = 7, making the curve y 2 = x 3 + 7 mod p
- The coordinate x of the base point G is G x = 02 79BE667E F9DCBBAC 55A06295 CE870B07 029BFCDB 2DCE28D9 59F2815B 16F81798
- The order of the base point G is n = FFFFFFFF FFFFFFFF FFFFFFFF FFFFFFFE BAAEDCE6 AF48A03B BFD25E8C D0364141

- The cofactor is h = 01.

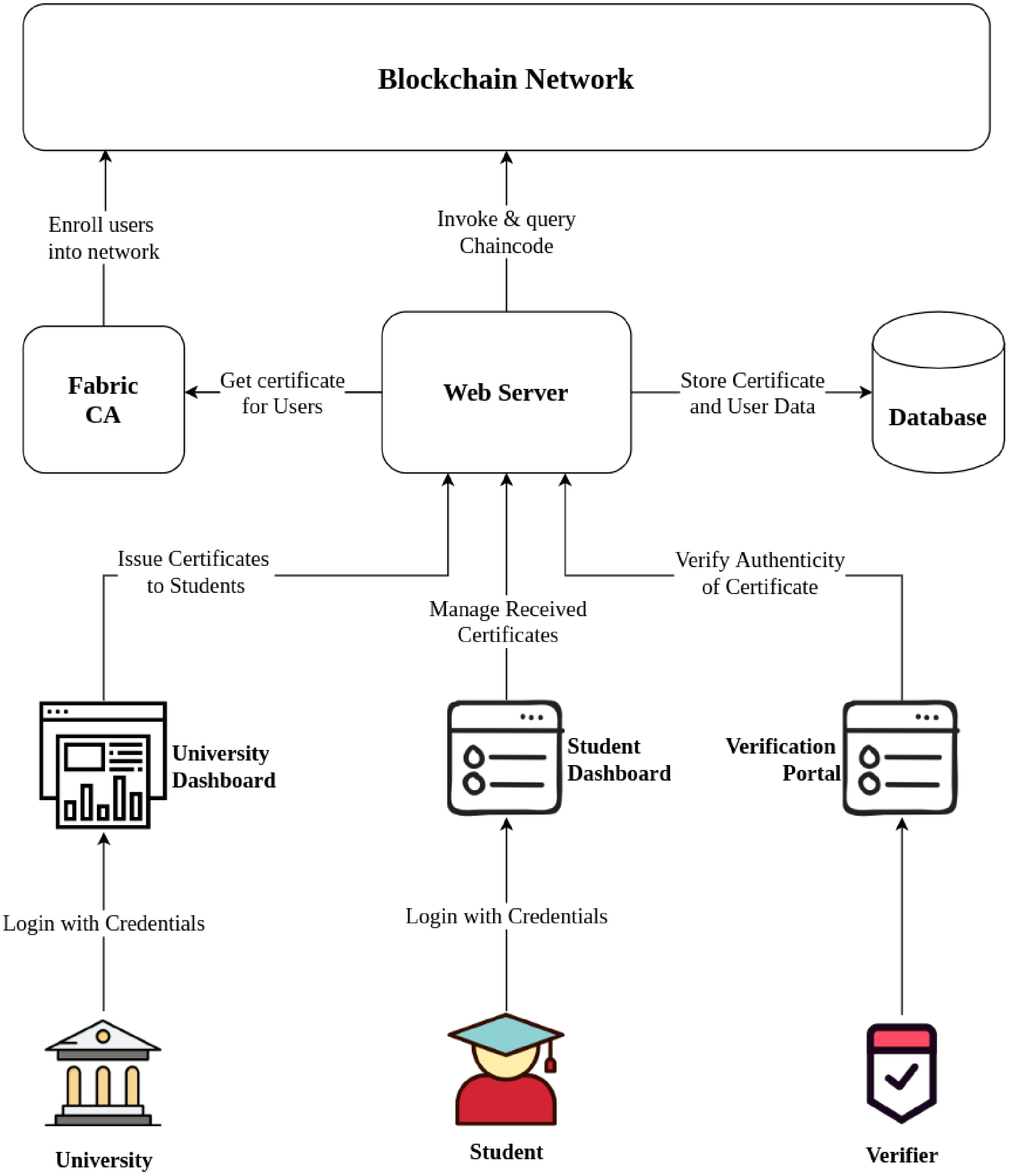
For protecting the data confidentiality in the digital wallet and transaction maintenance, Ethereum additionally uses the Advanced Encryption Standard (AES). The digital wallet is a file that stores user credentials, basically the private and public keys. The private key is used in the procedures to digitally sign user transactions and decrypt messages, while the public key is practically the wallet address of the user and it is used to encrypt messages sent to another user. Another important mechanism is the consensus algorithm which helps the network to coordinate the state of the common database. Due to the trust-less approach of building the network and possible malicious users in the network, the consensus mechanism offers procedures for decentralized synchronization of the databases owned by the network users. The three most common consensus algorithms are:

- Proof-of-Work (PoW) ,
- Proof-of-Stake (PoS) , and
- Practical Brzantine Fault Tolerance (PBFT) .

Every algorithm has its own advantages and disadvantages. PoW has the most reliable properties for anonymous usage of the network but it is the most energy inefficient algorithm due to heavy computational processes. PoS has less reliable properties but it is more energy-efficient than PoW because it implements moderate computational processes. PBFT is energy efficient but it is not feasible for pure public blockchain technologies because it is designed to work in closed networks.

With the deployment of the Ethereum Blockchain technology, the feature called smart contract was introduced. A smart contract is a self-executable and transparent code, stored in the immutable ledger of the Ethereum Blockchain. The last property makes the smart contract code impossible to be modified. This code, or more precisely functions from this code, can be invoked by those who have credentials. Often, smart contracts have properties to follow the terms of the regular (legal) paper contracts. In that way, it can often replicate and enforce the legal procedures into an automatic machine code. The implementation of smart contracts will provide unambiguous and automated procedures, transparent, reusable, and publicly accessible by everyone. By the development of smart contracts, that follows regular procedures, it is possible to store, check or revoke any information. A function in the smart contract will record the information on the blockchain, thus creating immutable evidence. Additionally, the smart contract can manage the credentials of the application users.

Architecture Overview



CHAPTER 3 METHODOLOGY

INTRODUCTION

This chapter covers the proposed methods of data collection and tools to be used in the development of the Students' Exit Management System. The first section of this chapter brings out the details of the data gathering techniques and it also highlights why they are preferred. The second sections bring out the development methodology and techniques and also the required technology to accomplish an effectively working system. This chapter ends with a conclusion giving a synopsis of what has been covered in the different sections.

DATA GATHERING METHODOLOGY

Refers to the device used to collect data, such as a paper questionnaire or computer-assisted interviewing system. Qualitative and quantitative methods of data collection are going to be used to collect data.

Qualitative research

Qualitative ('qual') research is often used for exploring. It helps researchers gain an understanding of underlying reasons, opinions, and motivations. It provides insights into the problem or helps to develop ideas or hypotheses for potential quantitative research. Qualitative data collection methods vary using unstructured or semi-structured techniques. Common methods include focus groups, individual interviews, observation or immersion, and diary studies. The sample size is typically small, and respondents are selected to fulfill a given quota.

Quantitative research

Quantitative ('quant') research is used to quantify the problem by way of generating numerical data that can be transformed into useable statistics. It is used to quantify attitudes, opinions, behaviors, and other defined variables, and generalize results from a larger sample population. Quantitative research uses measurable data to formulate facts and uncover patterns in research. Quantitative data collection methods are much more structured; they include various forms of surveys – online surveys, paper surveys, mobile surveys and kiosk surveys, face-to-face interviews, telephone interviews, longitudinal studies, website interceptors, online polls, and systematic observations. The methodologies that I used for this project on order to collect data from the organization are:

- Observation: Observation of students' behavior during the times of job seeking will be used to assess their reactions and attitude toward the current system.
- Interview: Several interviews will be conducted for both the students(graduates) and staff to find out their requirements for the System.
- Questionnaires and Online survey: Several online surveys and physical questionnaires are going to be used in order to collect data from both graduates and staff about the current system and their requirements for the new system.
- Online survey: Research from different and various researchers will be used to understand and get a comprehensive understanding of the technology and application.

DEVELOPMENT APPROACH

A software development approach helps us to structure, plan and control the process of developing software. Agile methodology: As an innovative approach, the agile methodology is used for articulating a well-organized project management procedure allowing for recurrent alterations. The agile methodology was selected because it has several invaluable advantages excluding the time wastage. This methodology is an adaptive approach that responds to changes favorably in
each phase from gathering to implementation. The agile methodology is found to be relevant for this project.

DESIGN AND DEVELOPMENT TOOLS

These are sets of technological equipment used to develop a system. This section covers the different tools, both software, and hardware that are required in order to develop the system.

Design Tools

i. Use Case Diagrams
ii. Sequence Diagrams

Programming Languages

The languages, frameworks, and libraries to be used in the development of the system include but are not limited to the following;

a). Backend

- Nodejs
- Solidity
- IPFS (Interplanetary File System
- Ganache
- Ethereum
- Ether
- Web3
- Smart-contract

b). Frontend

- ECMA Script 5
- ReactJs
- Metamask

Testing

- Trufflesuit

REFERENCES:

- Sayed, R. H. (2019). Potential of blockchain technology to solve fake diploma problem. University of Jyväskylä, JYX Digital Repository.
- Oliver, M., Moreno, J., Prieto, G., & Benitez, D. (2018). Using blockchain as a tool for tracking and verification of official degrees: business model.
- Tariq, A., Haq, H. B., & Ali, S. T. (2019). Cerberus: A blockchain-Based Accreditation and Degree Verification System. arXiv preprint arXiv:1912.06812.
- Buterin, V. et al. (2014). Ethereum white paper: A next-generation smart contract and decentralized application platform.
- http://blockchainlab.com/pdf/Ethereum_white_paper-a_next_generation_smart_contract_and_decentralized_application_platform-vitalik-buterin.pdf, 2014.
- Wegelid, F. (2019). Storing digital certificates using blockchain. Lund University.
- Olson, K., Bowman, M., Mitchell, J., Amundson, S., Middleton, D., & Montgomery, C. (2018). Sawtooth: An Introduction. The Linux Foundation.
- Shah, M. & Kumar, P. (2019). Tamper proof birth certificate using blockchain technology. Int. J. Recent Technol. Eng.(IJRTE), 7.
- Baldi, M., Chiaraluce, F., Frontoni, E., Gottardi, G., Sciarroni,D., & Spalazzi, L. (2017). Certificate Validation through Public Ledgers and blockchains. ITASEC, 156-165.
- Andoni, M., Robu, V., Flynn, D., Abram, S., Geach, D.,Jenkins, D., McCallum, P., & Peacock, A. (2019). Blockchain technology in the energy sector: A systematic review of
- challenges and opportunities. Renewable and Sustainable Energy Reviews, 100, 143-174.
- https://doi.org/10.1016/j.rser.2018.10.014
- Al Harthy, K., Al Shuhaimi, F., and Al Ismaily, K. K. J.2019. The upcoming blockchain adoption in higher-education: requirements and process. In 2019 4th MEC International Conference on Big Data and Smart City(ICBDSC) (2019), 1–5.
- Kanan, T., Obaidat, A. T., and Al-Lahham, M. 2019.SmartCert blockchain imperative for educational certificates. In 2019 IEEE Jordan International Joint Conference on Electrical Engineering and Information Technology (JEEIT) (2019), 629–633.
- Mori, K. and Miwa, H. 2019. Digital university admission application system with study documents using smart contracts on blockchain.