TUDocChain-Securing Academic Certificate Digitally on Blockchain

Thesis submitted in partial fulfillment of the requirements for the award of degree of

Master of Engineering
in
Software Engineering

Submitted By
Sugandha
(Roll No. 801731012)

Under the supervision of:
Dr. Rinkle Rani
(Associate Professor)

COMPUTER SCIENCE AND ENGINEERING DEPARTMENT
THAPAR INSTITUTE OF ENGINEERING AND TECHNOLOGY
PATIALA – 147004

July 2019

CERTIFICATE

I hereby certify that the work which is being presented in the thesis entitled, "*TUDocChain-Securing Academic Certificate Digitally on Blockchain*", in partial fulfillment of the requirements for the award of degree of Master of Engineering in *Software Engineering* submitted in Computer Science and Engineering Department of Thapar Institute of Engineering and Technology, Patiala, is an authentic record of my own work carried out under the supervision of *Dr. Rinkle Rani* and refers other researcher's work which are duly listed in the reference section.

The matter presented in the thesis has not been submitted for award of any other degree of this or any other University.

Sugandha
(801731012)

This is to certify that the above statement made by the candidate is correct and true to the best of my knowledge.

Dr. Rinkle Rani
(Associate Professor, CSED)

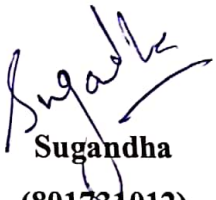
Acknowledgement

First of all, I would like to thank God for blessing me with all the strength and resources required to complete this task. I would like to express my deepest gratitude towards my respected supervisor **Dr. Rinkle Rani**, Associate Professor, Computer Science and engineering Department for guiding and encouraging me to accomplish this task successfully. I am thankful to my supervisor for her valuable times, patience and sharing experiences as well as knowledge with me which has made this journey rewardable and enjoyable.

I am also very thankful to **Dr. Maninder Singh,** Professor and Head of Computer Science and Engineering Department, for the motivation and inspiration for the completion of thesis.

I am also thankful to the entire faculty team and staff member of computer Science and Engineering Department for their assistance and cooperation.

Last but not the least, I would like to thank my family and friends for their wonderful support and encouragement without none of this would have been accomplished.



Sugandha

(801731012)

ABSTRACT

Blockchain is an integral distributed public ledger technology, which uses the consensus algorithm and cryptography techniques to devise the characteristics of decentralization, traceability, immutability and tamper-proof ledger. Blockchain is the main technology behind the cryptocurrency. Now it is applied in many fields including education, IOT and Risk management. Blockchain allows digital information has been distributed on different nodes that increase the transparency and security of documents.

Digital Documents become a part of organization, institution and educational field whether public or private. Digital Documents not only authorize the transition of information but also maintain the data in digital form. Academic Certificates approve the procurement of learning outcome. Certificates become necessary for people's professional careers. It is essential to save these certificates in long-term available and tamper proof ledgers. A Blockchain stores transaction in a confirmable and persistent way, therefore it is appropriate to save certificate or learning certification. Blockchain divulge fraud of certificates and it substructure learning records. This is accomplished by keeping digital crypto-hashes of learning certificates and controlling authorization integrity through the development of smart contract on Blockchain. TUDocChain is the platform that entitle authorize the academic certificates on public ledger in a reliable and sustainable format. TuDocChain is implemented on Ethereum Blockchain. All the academic certificates managed by the Interplanetary File System (IPFS) in an address form. Blockchain does not store the records in original form it secures the data using hash value. Blockchain maintains the privacy of documents as well as the privacy of individual identities. In TuDocChain system issuer secure the document on Blockchain using distributed web i.e. IPFS. Students as a receptor view their documents on framework. It provides additional feature of verification of documents. The third party or authority wants to verified the student's documents, they verified using the address of certificates. TUDocChain is a platform provide the transparency and privacy feature using Blockchain technology.

Table of Content

List of Figures

List of Tables

CHAPTER 1

INTRODUCTION

1.1 Overview

Blockchain is a peer to peer distributed ledger created by consensus; integrate with the system for smart contract. Blockchain is the backbone of digital crypto-currency. Blockchain is a prominent technology, with almost daily declaration on its applicability to everyday life [1]. Blockchain technology has been implemented in different areas such as crypto-currency in financial area, education field for securing the data in the digital form, in healthcare sector securing the patient data. Because of its decentralized and immutable properties, it is used in various sectors. Blockchain developing the current internet from "The internet of information sharing" to "The internet of Value Exchange" [2] .

Academic Certificate plays an important role in education and development in companies. Students complete their degree or courses in different universities and educational institute. After completion of their courses universities and educational institutes award their student with degree or issue certificate. Students receive the certificate as a paper document. Certificates include many statements, most important are: Registration number, name of student, Certifier Signature, Address of organization, date of examination and other supplementary information.

Students receive a paper document that represents the certificate. Students can easily store paper documents or show them to any organization and person for any specific purpose. For entrance in organization or educational institute the authorities demand the previous qualified certificates as a proof even for recruitment company authority verify the credential of employee. They store the student document and maintain the certificate for a long period of time.

The substitute method to paper documents are digital certificates that are cryptographically signed. Comparatively management of digital certificate is easier than

the paper document but it required a lot of registry efforts. Third party easily verifies the students or employee documents with the help of crypto hash of certificate.

In frame of reference of education and certification, Blockchain technology provides forged preservation of certificate. Third party easily verifies the documents with the help of Blockchain features without the involvement of organization authority. In digital certificate process mainly three main steps are identified. Firstly, identity of certification authority has been created and maintained. Secondly certification authority awarded certificate to students and third step is the authenticate certificate by the recruiter or other organization authority. These three steps followed by a Blockchain based framework and adding additional feature of sharing certificate by students [3]. Blockchain education framework provide security as well as assured access and stable management of certificates according to the requirement of students, organization or educational institutions authority.

1.2 Introduction to Blockchain

Blockchain is the main technology behind bitcoin. Blockchain is first proposed in 2008 by Santoshi Nakamoto and implemented in 2009[4]. Blockchain is "an open distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way"[5]. A Blockchain is a time-stamped sequence of immutable records of data that is run by cluster of computers not maintained by any individual entity. Every individual block of data is secured and bound to each other using crypto-hash value. There is no central authority in Blockchain network. The information is open for anyone due to its shared and immutable ledger. Hence anything builds using Blockchain is transparent in nature and participation of individual is accountable for their action.

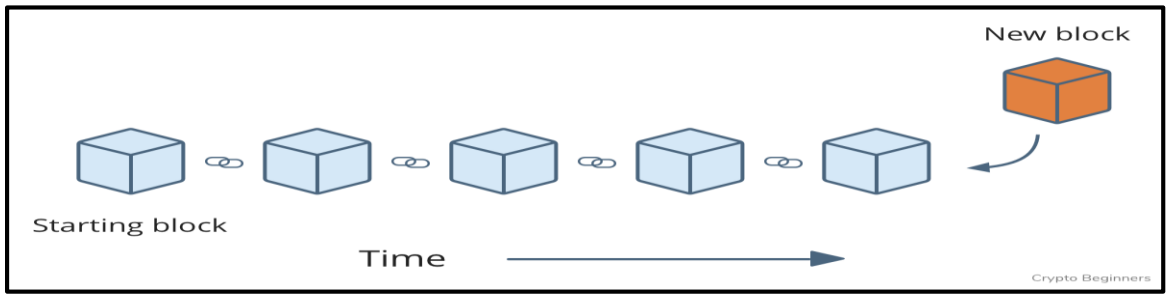


Figure 1: Example of Blockchain

1.2.1 Blockchain Architecture

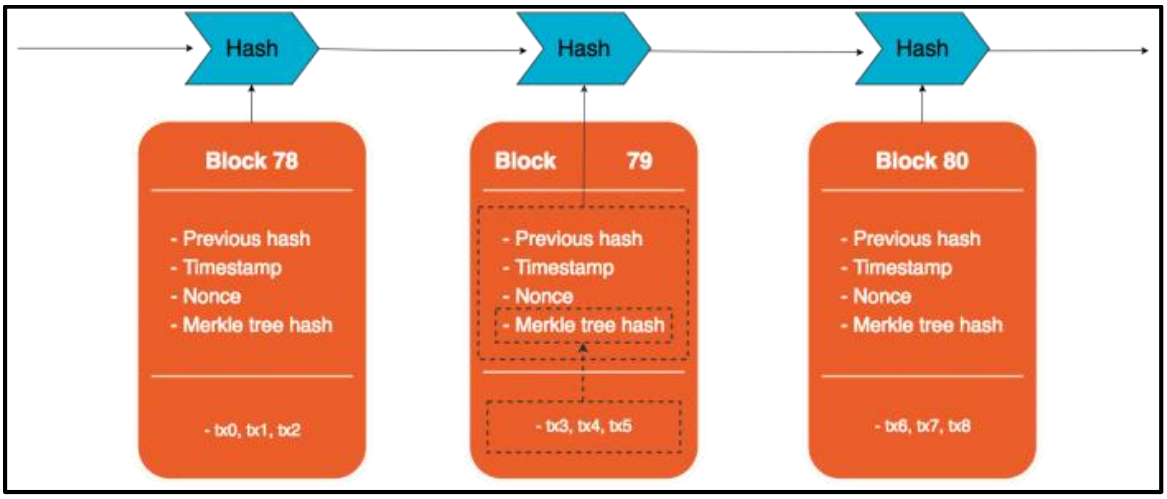


Figure 2: An Example of Blockchain which consist of Continuous sequence of Blocks

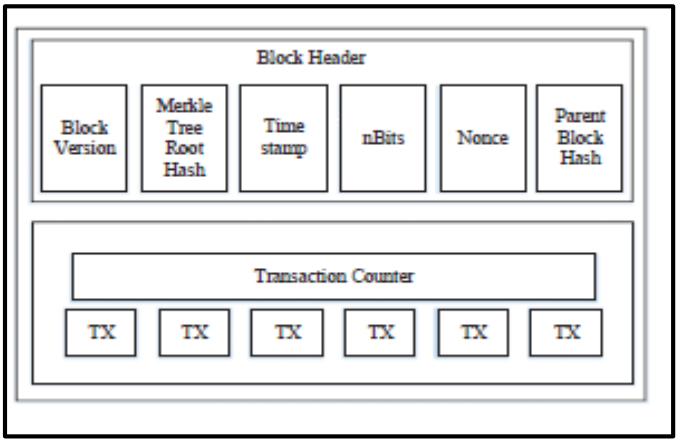


Figure 3: Block Structure

Blockchain is the chain of growing records(blocks). Blocks are linked together or form a chain with the help of hash value of previous block as shown in Figure 2. Linked list is implemented as a data structure to form a blocks whose main purpose is to bind the transactions together and distribute the transactions to nodes in the network. The first block is known as **Genesis Block** which has no parent block. Block internal structure is as follows:

Block: -Block contains a block header and block framework as shown in Figure 3. Block header includes hash value, version of block, time-stamp value, nonce value, nbits, parent hash value, Merkle Tree.

a. Block Version: - set of validation role followed by individual.
b. Merkle Tree Root Hash Value: - in the binary tree form it contain the hash value of all transactions as shown in Figure 4.
c. Timestamp: - Current time according to universal time.
d. nbits: - valid block hash threshold target.
e. Nonce: - 4-bits value, used in verification of adding new block into the chain through the process mining. For mining number of consensus algorithm are used.
f. Parent hash Value; - a 256-bit hash value that pointed previous block hash.

Blockchain framework contains the transaction counter and number of transactions. The number of transactions stored by block depends upon the size of block and size of each transaction. Asymmetric cryptography is used in the Blockchain. For asymmetric cryptography digital signature is used for the verification of transaction [6].

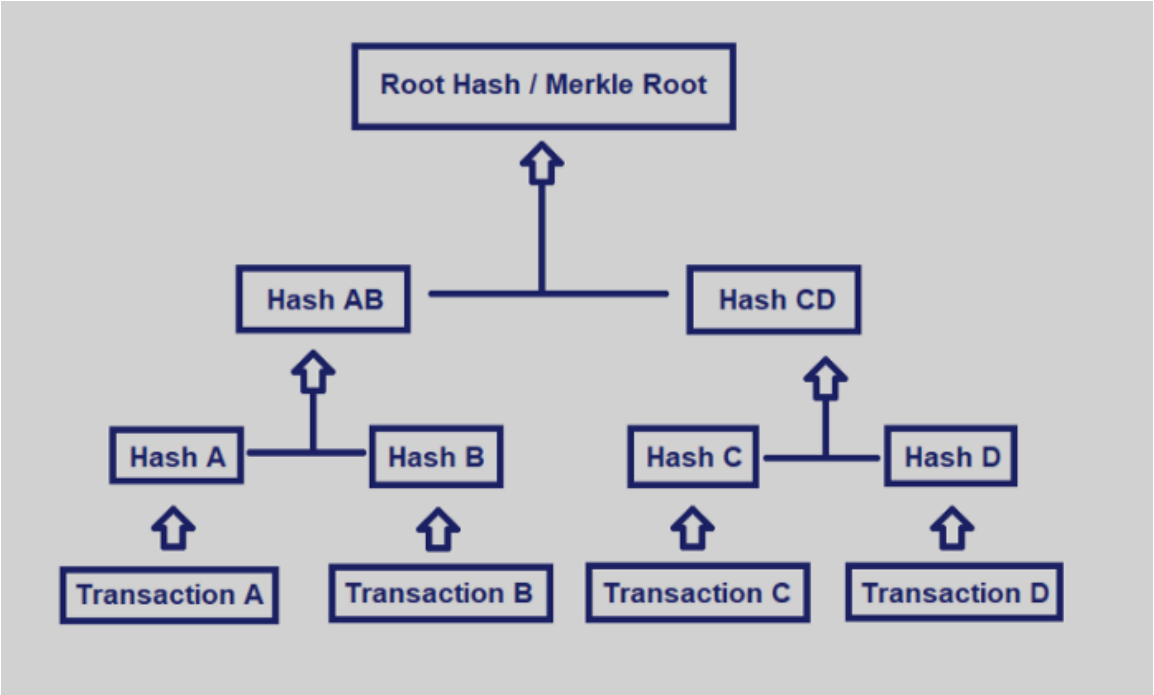


Figure 4: Merkle Tree

1.2.2 Digital Signature

As the signature provides validation and authentication to any transaction same principle digital signature works. Digital signature is the main feature of Blockchain that provide the security and integrity of the data that are stored in the Blockchain. Digital signature

work on the principle of asymmetric cryptography meaning information is shared with the help of public key.

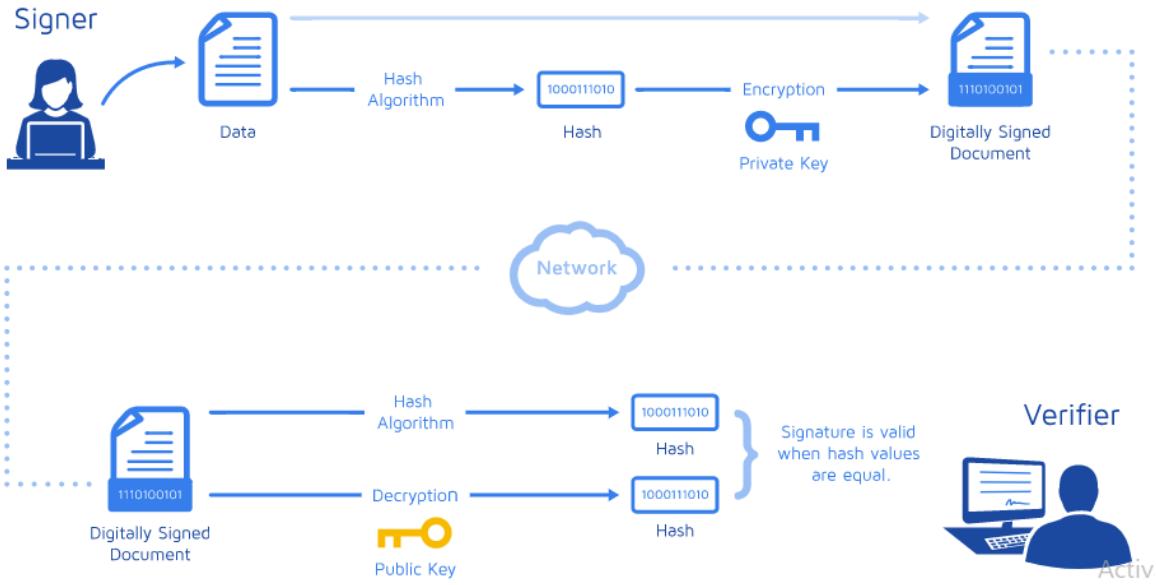


Figure 5:Working of Digital Signature

Digital Signature also known as Pubic Key Infrastructure (PKI). As shown in Figure 5 [1] a digital signature is made up of 4 components.

- A SHA-256 hash, it is a hash algorithm to generate a unique value.
- A Public Key
- A Private Key
- A time stamped when the document was issued.

Firstly, hash of document is generated by using the algorithm. Combining both hash value and the private key together generate a signature. Hash value of signed document is different from unsigned document. If any changed occurred after signing document its hash value changed automatically. For the verification of document sender send the signed document and the public key, and then the document is decrypted if the hash value is same as before the document is authenticated otherwise it is other's document. The combination of both private and public key secures the document.

1.2.3 Key Characteristics of Blockchain Technology

Blockchain tackle the issue of manipulation. In the realm of present day innovation numerous individuals have trust issues with Facebook, Google and bank. There are numerous things that the Blockchain is going to change. It is conceivable that Blockchain can genuinely disturb different ventures and make the procedures progressively just, secure, straightforward, and productive. Characteristics of Blockchain technology as follows: Decentralization, Immutability, Security, Trust.

1.2.4 Consensus Algorithm

Validation and security of new block is ensured by the consensus algorithm. When new block entered into the Blockchain block is validated by the miner. The process is known as mining. For the mining process some consensus algorithm is used. According to different platforms of Blockchain different algorithms are used. For bitcoin and Ethereum platform Proof of Work consensus algorithm is used. Improving the features of proof of work Proof of stack algorithm is used. Proof of work requires more amount of energy. Explain the work of these consensus algorithm as follows:

- **Proof of Work**

  In order to add a new block into the existing block correct proof are generating with the process known as mining. The individual who takes participation in this process is known as miner. The complex cryptographic puzzle is solved by the miners. The miner who solved puzzle early and correctly rewarded with the bitcoin. In the complex puzzle 4-bit value (known as nonce) added with the original hash value of the previous block. If the solution of puzzle is greater or equal to the crypto hash value, then the block is added into the chain otherwise it is rejected.

- **Proof of Stack**

  The individuals participating in the process of generating a new block in proof of stack algorithm are known as validators. Validator is chosen on the basis of economic stake in the network. The one who kept large number of coins for long time period is chosen for generating a new block. This algorithm is more relevant

and energy efficient than the Proof of Work, because lesser number of resources are used for choosing the validators.

For different crypto-currency number of consensus algorithm are used. Table 1 shows the comparison among different consensus algorithm [4], [6].

Table 1**:**Consensus Algorithm Comparison

Property	**Pow**	**PoS**	**PBFT**	**DPOS**	**Ripple**	**Tindermint**
Node Identity Management	Open	Open	Permissioned	Open	Open	Permissioned
Energy saving	No	Partial	Yes	Partial	Yes	Yes
Tolerated power of adversary	<25% computing power	<51% stake	<33.3% faulty replicas	<51% validators	<20% faulty nodes in UNL	<33.3% byzantine voting power
Example	Bitcoin	Peercoin	Hyperledger Fabric	Bitshares	Ripple	Tendermint

1.2.5 Types of Blockchain

Blockchain has been categorized into three types depending on the requirement of application. Comparison is shown in table 2.

i. **Public Blockchain**: Public Blockchain is permission less Blockchain. Anyone publically access the transaction easily. Public Blockchain provide maximum immutability, decentralization and transparency [1] . For storing transactions, it requires large cost and high electricity usage but the transaction speed is low. Bitcoin is one of the examples of public Blockchain that's why it takes 10 minutes for mining of new block. Other examples are Ethereum and Litecoin.

ii. **Private Blockchain:** Private organizations like bank perceive that they use the idea of Blockchain as a Distributed Ledger Technology and generate a restricted Blockchain. Write operation has been presented on central database and read operations have been presented on distributed network or say public network.

Private Blockchain increases the speed of transaction. Private Blockchain decrease the energy cost. Example MONAX and Multichain [7].

iii. **Consortium Blockchain:** In the Blockchain network some node manages the consensus mechanism and some other nodes run the transactions. It is the hybrid of public and private Blockchain. Multiple organizations share the network so it acts as a public Blockchain, access on nodes is restricted so it acts as a private Blockchain.

Table 2: Types of Blockchain

	Public Blockchain	**Private Blockchain**	**Federated/Consortium Blockchain**
Access	Anyone	Single Organization	Multiple selected organizations
Participants	Permission less, Anonymous	Permissioned, Known Identities	Permissioned, Known identities
Security	Consensus Mechanism- Proof of work/ Proof of Stake	Pre–approved participants, Voting/multi-party consensus	Pre-approved participants, Voting/multi-party consensus
Transaction Speed	Slow	Lighter and Faster	Lighter and faster
Example	Bitcoin, Ethereum, Litecoin	Multichain, MONAX	Hyperledger, B3i(Insurance), R3(Banks)

1.2.6 Type of records stored in Blockchain

Blockchain is used to store different type of transactions in the form of records, currency and contracts.

i. **Asset Transactions:** Bitcoin is the main currency implemented using Blockchain Technology. Different crypto-currency has been implemented since 2008. Every crypto-currency has its own value. Crypto-currency is the digital money excluded the involvement of third party and provides transparency in the transaction. Table:3 in Chapter 2 describes the existing crypto-currency. The value of one

crypto-currency is converted into another crypto-currency. For example, Bitcoin value is changed into Ethereum coin value.

ii. **Smart Contracts:** Smart contracts are a piece of code that serves as a programmed conceptual agreement between two parties. Contract contains some conditions which need to be fulfilled in order for some transactions to occur. Data Owner and Data consumer contracts are written in the language of solidity. After deploying the contracts agreement is established between two parties.

iii. **Certificates and Digital Signature:** The academic certificates, any records and personal documents in the form of transaction have been stored in Blockchain network on distributes network. The hash value is generated by using the hashing algorithm. If the records are directly stored into the Blockchain it occupies large amount of memory and space that increase the cost of storing records. Hash value stored with the digital signature stored into the Blockchain. Digital signature is generated using asymmetric cryptography. In asymmetric cryptography both private and public key has been used for encryption.

1.2.7 Applications of Blockchain

Blockchain technology has various applications in different fields. Blockchain is the main technology behind the crypto-currency. Blockchain is the backbone of bitcoin. As the part of fourth industrial revolution[2] since the innovation of steam engine, electricity and information technology [2]. Blockchain has been implemented in different sectors like in finance, internet of things, educational field, judiciary and commerce[2]. Figure: 6 gives the overview of application of Blockchain [4]. In finance sector crypto-currency has been used as a digital currency. It removes the involvement of third party and bank central data. Recently Facebook wants to launch his crypto-currency name Libra. The vouchers have been generating using the concept of Blockchain. PayPal coupon system works on the principle of Blockchain technology. Blockchain works on the IOT based platform. Literature Review in chapter 2 explains all the work performed using the Blockchain in educational framework. Blockchain provides the immutable and transparency feature its application works on the security and risk management platform. All the institutes' functionality has been implemented on the Blockchain platform.

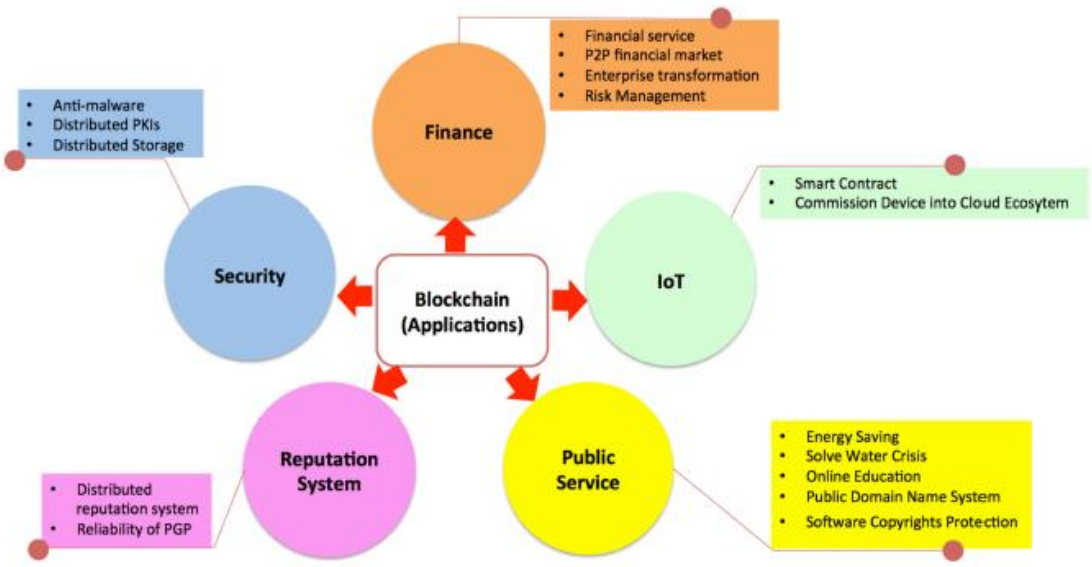


Figure 6: Application of Blockchain [4]

1.2.8 Characteristics of Blockchain Technology

Mainly Blockchain technology characterized four features. Decentralized, Traceability, Immutability and currency Properties[2]. Figure 7 explain the characteristics of Blockchain technology.

i. **Decentralization:** The transactions managed and secured on Blockchain are distributed on different networks. Securing and verification of transaction depend on distributed system architecture. With the help of mathematical algorithms and smart contracts trust factor has been maintained between the networks.

ii. **Traceability:** Transaction on Blockchain managed in chronological order. All blocks are linked with the encrypted hash value. Every transaction stored on Blockchain with the timestamped manner. Every transaction is easily traceable using the hash value. The hash value is stored in binary tree form known as merkle tree. The root of merkle tree is the hash value of that block which becomes the previous hash value of the new block. With the help of hash value all blocks are linked together.

iii. **Immutability:** Transaction shared on distributes network and all blocks are linked together with the help of hash value, these two properties make the Blockchain immutable. If someone wants to change the transaction content its hash value changes accordingly and with the change of hash value everybody knows about the change in hash value. It is impossible to change the content of transaction. The transaction stored on public ledger on different nodes provides the transparency property in Blockchain technology.

iv. **Currency Property:** Blockchain technology is trustable. Transactions are shared without the involvement of third party. Digital currency is used for securing the transaction on the Blockchain. In education platform on Blockchain for securing the academic certificates crypto-currency is used. Money is transferred from one individual to another individual with the involvement of third party like bank. Blockchain build a trustable network with the help of public ledger and consensus algorithm.

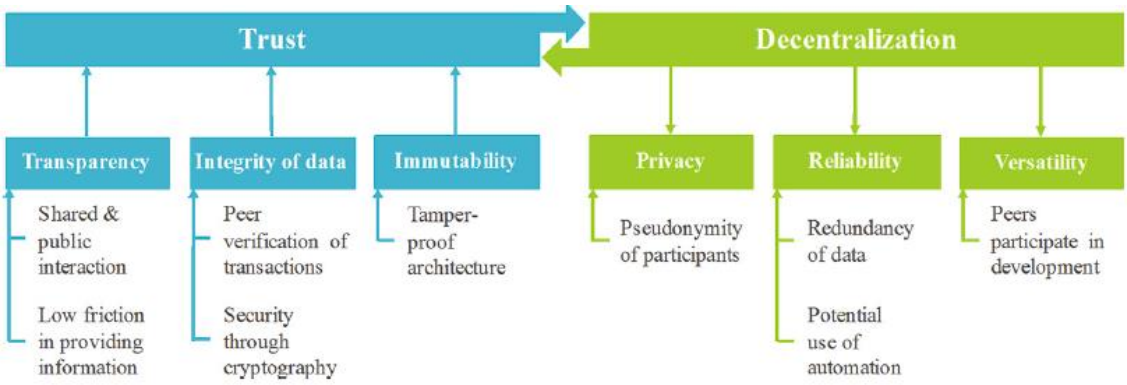


Figure 7: Characteristics of Blockchain Technology

Chapter 2

Literature Survey

Blockchain has been implemented in different sectors to entitle decentralization approach such as health[8], finance [7] crypto-currency (NAKAMOTO 2008), IOT [8], [9], risk management.

2.1 Blockchain in Education Field

Educational organizations and institutions use the Blockchain technology for verification and sharing of Documents, Transcripts and Personal Documents. Table 2 compares the existing applications of Blockchain in educational field.

2.1.1 Blockchain to permanently secure Certificates

In the United State around 200,000 forgery certificated are vend each year by a fraud diploma mills. Some degree sold at a rate of $100 dollars and the price go up to $50,000[10]. The verification, securing and sharing of documents is a manual process which is very messy and time consuming. To stop this forgery, Learning Machine collaborated with MTI Media Lab to the implementation of Blockcert for issuing, Storing, and verification of document using Bitcoin platform in Blockchain Technology[3],[10],[11]. University of Nicosia has issued Blockchain based certificate for DFIN-511 : Introduction to Digital Currencies[10].

Arenas et al. (2018) proposed a Blockchain based system named credence Ledger for the verification of academic documents [11]. System verified the credentials without the transaction of crypto-currency. Credence Ledger is implemented using permissioned Blockchain in which multichain is created by using multisignature. System require less resources for the verification and sharing of digital documents.

Ocheja et al. (2019) implemented a platform named Blockchain of Learning Logs (BOLL) [3]. BOLL platform manages digital hashes of learning records and managing access rights by using smart contracts on Ethereum Blockchain. BOLL is used for issuing, sharing and verification of learning records. Identities of issuer, receptor and verifier are stored into the Blockchain. The identity of issuer combined with the hash

value of the document stored into the Blockchain. Smart Contracts are created between the issuer and verifier of different organization. Learning Record Storage (LRS) is used to store the learning records of different institutions collectively. Students are doing studies in different institutes. LRS control all of the transcript and studying facts of that particular pupil from all institutes. Student records are collected into the Secure Box and the Secure box directly connect with the Blockchain.

In the field of education Sony Global Education developed a framework on IBM Blockchain which is delivered via the IBM Cloud and powered by Hyper Ledger Fabric 1.0, a Blockchain framework and one of the Hyper ledger projects hosted by The Linux Foundation. SGE platform is used by any institution for the securing and verification of credentials [15], [16].

Harthy et al. proposed a platform which is utilizing Blockchain to meet all the transaction of college i.e. college chain [17]. Chain include money transaction, certificate transaction, securing the profile of students, staff and third party (stakeholders), online library access and managing published research paper. Chain proposed using Ethereum Platform. Smart Contracts are constructed according to requirements and changes include in the college.

Bin Wu et al. proposed an application on Blockchain as a digital education system evaluate the competition skill grades of students [18]. An application has been framed as the academic certificate and other certificates achieved by the students are secured on one platform. The grade of individual student has been calculated through the certificate and performance of the student. Both teacher and students act as a client on Blockchain network. Both interact with the help of web. Teacher uploaded the data on Blockchain network through database. Competition question has been solved by the students and result is evaluated by the Blockchain network. Blockchain keeps the transparency between the students and teachers.

Table 3: Existing Applications of Blockchain on Education

Application	Blockchain Table	Record Type	Actual Data Stored	Verification	Access to Records
BlockCerts [10]	Bitcoin	Certificates	Hash of Certificate	Open	Off-Blockchain authorization
UNIC[10]	Bitcoin	Certificates on MOOC	Grouped hash of certificates	Open	Off-Blockchain authorization
Sony Global Education [11]	Hyper ledger	Academic Records	N/A	N/A	N/A
Grade base [12]	Bitcoin	Imperial College Certificates	Hash of certificate, online profile and CV	Open	Off-Blockchain authorization
Stampery [11][13]	Bitcoin and Ethereum	Certificates	Hash of data &transactions	Open	N/A
Credence Ledger[11]	Permissioned Blockchain (crypto-currency is not required)	School Records	Hash of Records	Open	N/A
TrueRec [14]	Ethereum	Documents like passport, certificates	Hash of documents (multichain with multi-signature)	Open	Off-Blockchain authorization
Open Certificate [11]	Ethereum	Certificate Insurance	IPFS generate the crypto hash value	Open	N/A
Blockchain of Learning Logs (BOLL)	Ethereum	Different institute's transcripts	Smart contracts	Open	N/A

2.1.2 Parallel Education Blockchain

Gong et al. implemented a smart education system using parallel education [19]. Parallel education Blockchain has been described the data distribution schema and data transfer on different layer. Figure:8 described the comparison between the education system and the smart education system on different layers. Parallel smart education work on three layers.

Data Layer provided a double securing mechanism named as distributed and central. Storage schema, storing achievements credits and rewards have been performed using distributed network. Data is divided into two parts formal and informal. The educational data such as records, academic certificates and rewards of certification act as a formal data. The data in the form of video act as an informal data. Informal data stored on the central network. Original data has been secured in central network and address of transaction or formal data stored on distributed network. The individual identities address stored on distributed network provide the transparency and privacy of data.

Logical Layer uses the consensus and non-consensus algorithm. Formal and informal data both uses the non-consensus mechanism. Evaluation of certificate , certificate recognition and grade certification [19] has been presented on logical layer. Formal data uses the non-consensus mechanism for mining where informal data uses the consensus mechanism.

Application Layer executed the smart contracts for different transaction on formal and informal such as creativity transferring, credit transferring and grade transferring. Once smart contract set up then the transactions are globally distributed on different network like on different organization, school, institution. Globally data has been validated through the smart contracts.

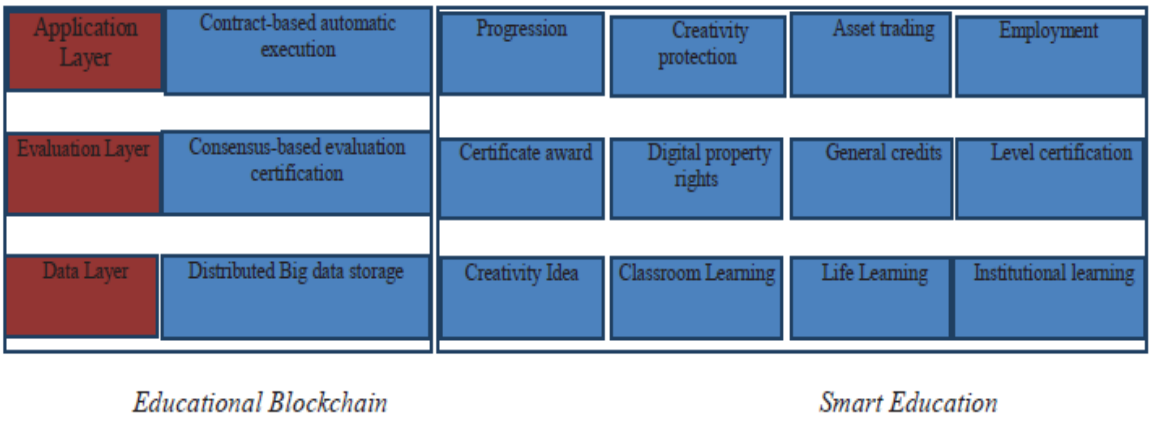


Figure 8: Education System on Parallel Blockchain

2.2 Blockchain securing personal data

Goswami et al. presented an architecture name Public Key Infrastructure (PKI) used for securing documents as e-document using Signing tools [20]. Digital Signature is used for securing the e-documents. Digital signature uses asymmetric key cryptography. Digital Signature is generated with hash value of the document. Hash value is encrypted using private key of the issuer. Certificate Revocation List (CRL) or online certificate status protocol (OCSP) act as a central server has been used for validation of documents.

Chowdhury et al. proposed a consortium based Blockchain application named personal data store(PDS) [21]. PDS has been provided a service to manage, store and deploy the personal data like medical records and academic records. A student goes for the interview and the interviewer asked for the academic records of that individual. Instead of validate all the records manually the students provide his/her access of PDS. Interviewer or organization easily validate the individual records from Blockchain platform PDS. Although PDS stores the personal data so the consortium Blockchain network is used for storing the records.

Giang Do introduced a system named BlockDS provides a secure distributed storage using distributed hash table (DHT) with keyword search service additionally [22]. The data owner uploads their data in encrypted form then data has been distributed on the distributed cloud storage nodes and data consumer validates the availability of data.

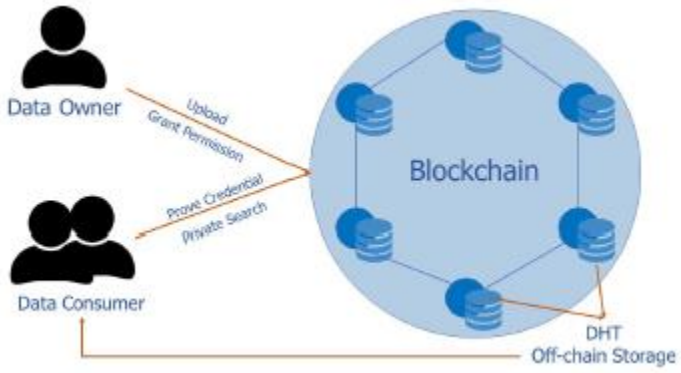


Figure 9: BlockDS System Model [22]

BlockDS system has been implemented using Hyperledger fabric using composer to handle the validation networks and assents for access to an off-chain method that is easily adaptable and uncertain- providing unchangeable assurance of reliability and clarity.

Wang et al. proposed a system on Blockchain. Framework has been divided into two parts [23]. One chain has been used for storing data and second chain used for storing transactions. Double chain has been implemented in this framework. Original data is stored in the DBC (Data Blockchain) and the records generated by the data transaction were stored in TBC (transaction Blockchain). PBFT consensus algorithm is used in double chain network. Double chain upgrade the performance of the Blockchain network and decrease the communication pressure[23] of the single chain Blockchain network. The architecture of this framework is as below in Figure:8.

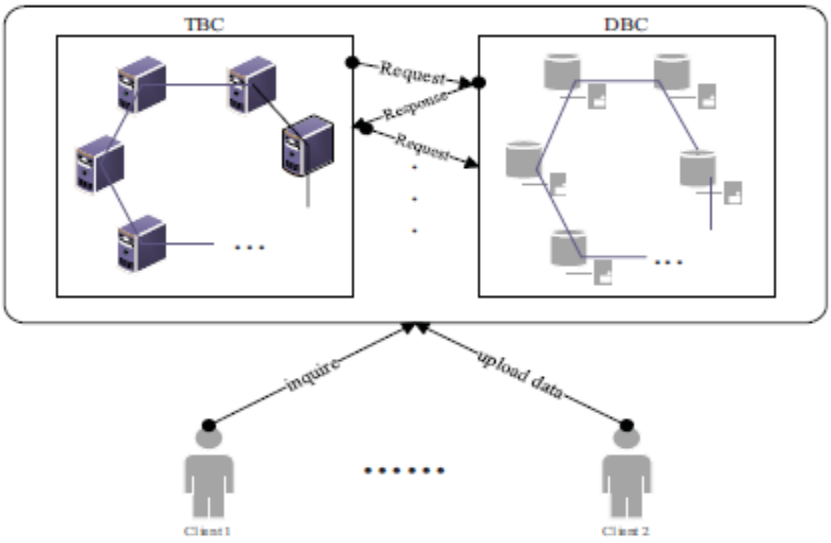


Figure 10:Double chain Blockchain[23]

2.3 Blockchain in Crypto-currency

Blockchain primary application is crypto-currency. Blockchain technology is used for generation of crypto-currency. For storing the data and documents on the Blockchain for transaction as an assets purpose crypto-currency is used.

Table 4: Comparison Between the Crypto-currencies

Crypto-currency	Year	Hash Function	Mining Method
Bitcoin	2008	SHA-256	Find all possible nonce value by computing proof of work and other users agree and verify the proof.
Litecoin	2011	Scrypt	Similar to Bitcoin(proof of Work)
Peercoin	2012	SHA-256d	Proof of work and proof of stake
Primecoin	2013	Cunningham Chain	Proof of work
Ripple	2014	EC digital Signature	Consensus System
Ethereum	2014	Ethash	Proof of work
Permacoin	2014	Floating digital signature	Proof of retrievability
Blackcoin	2014	Scrypt	Proof of stake
Auroracoin	2014	Scrypt	Proof of work
DarkCoin	2014	X11	Proof of work
Namecoin	2015	SHA-256d	Proof of work
Zcash	2016	Equihash	Proof of work
Cardano	2017	Ethash	Proof of Stake
EOS	2018	Ethash	Cloud Mining
Libra	2020(upcoming)	NA	Proof of stake

2.4 Ensuring Data Integrity

Zikratov et al. proposed a schema on data integrity and provide guarantee to data owner for securing the data [24]. Data integrity has been checked by TPA (third party auditor). This schema handled by the data owner. Data owner view all the changes and modifications done by the third party. Data owner assured the security of data. PDP

(provable data possession) schema has been used to explore statically the authentication of data uploaded to distributed cloud storage without restoring the data.

Augot et al. proposed a solution for user to achieve authenticated identities based on face-to-face proofing that can be assured against a record on Blockchain network [25]. Zero knowledge proofing has been used for identity. Framework has been implemented on bitcoin Blockchain network and grouping commitments using Merkle tree and decreasing bitcoin transaction and increasing the bandwidth of the network.

Methetwa et al. recommended a Blockchain based solution to authorize the assurance of hardcopy documents [26]. Validation of hardcopy documents has been done by combination of 2D barcodes, OCR (optical Character Recognition) and cryptographic hashing.

Chapter 3

Research Problem

3.1 Problem Statement

Certificates assure the competence of degree through a computation of knowledge and skills. Student once completed their study in the school and colleges, they receive a certificate or detail mark sheet. These certificates play a significant role in the learner's life. School, Colleges provide physical copy of the certificate and degree. Individual submit their hardcopies in organization for further studies then organization manually verify the documents of the student. Even in the career profession if individual apply for job, company demand for submit all the academic documents for verification purpose. Manually authorization of documents is time consuming and it increases the forgery cases. Some people without perusing certification courses receive the hardcopy or physical document from fraud institutes and organization. In the United State around 200,000 forgery certificated are vend each year by a fraud diploma mills. Some degree sold at a rate of $100 dollars and the price go up to $50,000[10]. Forgery of documents suspended in South Africa [26]. To decrease the forgery rate in the certificate and try to provide transparency in the certification process we proposed a system which generate the digital certificate by using Blockchain technology.

Blockchain technology provide the feature of trust, transparency, immutable and tamper-proof records. We proposed a system named as TUDocChain that provides a Blockchain platform in education. This can be used for issuing, securing and verification of academic documents. Blockchain Technology removes the involvement of third party. All the certificate and records of students stored on the Blockchain. All certificates manage by the certificate authority. Verifier publically authorizes the documents of students. On one platform all the student documents have been verified and secured. The personal documents have been secured using this platform.

Issuer issues the certificate digitally using digital signature with hash value of the particular certificate. Digital signature is generated using asymmetric key cryptography.

In asymmetric key cryptography public and private key is used for encryption. Verifier verifies the documents on distributed public ledger using public key of the issuer. Documents are easily authorized using Blockchain technology. All the documents shared on public ledger as a distributed network decrease the forgery. If anyone operate some changes in the documents its hash value changes immediately that why changes identify easily on the distributed shared network.

3.2 Research Gaps

Blockchain Technology has been implemented in different fields. A lot of work has been implemented in the crypto-currency. Even Blockchain technology has been implemented in the educational field. All the existing Blockchain based platform on education based on Bitcoin platform. Bitcoin works on proof of work consensus algorithm. For transaction it requires large amount of cost and energy. Transaction speed on the bitcoin platform is slow. Miners mined the new transaction into the block takes 10 minutes. To increase the throughput of the transaction Ethereum platform has been used for securing documents on Blockchain. Limitations in pervious study and research work are described below:

1. Multi-institution's certificate disconnected from one another. There is not a single platform which secures the entire learners certificate securely.
2. For transaction of document Bitcoin platform has been used. A Bitcoin transaction fee is very expensive. Certificates are managed on different platform which require excess of computational energy.
3. Transactions run on Ethereum platform which takes Ether for every transaction. The cost of ether purchase paid by the certifier who issues the certificate on Blockchain platform.
4. Lack of security and authority access of individual information by the certifier.
5. Disconnection of massive open online courses (MOOC) certification used as a proof of skill and knowledge with academic certificates. If online certificates and degree certificates both connected on platform will make the authorization process for the verifier easy.

6. Some application uses Hyperledger fabric for securing documents on Blockchain on permissioned Blockchain. Hyperledger fabric implementation is complexed.

3.3 Research Objectives

In the light of above discussed research gaps following objectives have been formulated.

1. To study various tools and techniques available for the implementation of Blockchain Technology.

2. Securing Certificates on distributed network to provide transparency among the students, institutions and third party stakeholders.

3. To manage and authorize Smart contracts on Blockchain.

4. To generate the content address using IPFS to provide privacy feature of personal profile.

5. To store Academic certificate using crypto hash value generated by the IPFS.

6. To use MongoDB NoSQL database for securing the documents.

3.4 Research Methodology

In the schema of our proposed system, we first are going through the literature review on existing application of Blockchain on education. Especially, we understand the concept of MIT Media Lab system named Blockcerts [27]. Blockcert implemented on bitcoin platform and uses the Open Badges for managing the records and encrypted the data using digital signature. Credence Ledger [11] architecture and Blockcert gives direction how the system worked on Blockchain. We discussed with the teachers, students and third party stakeholder that our proposed system feasible and useful for them. Exploring hands on practice on tools worked on Blockchain environment. Postman and flask has been used for implementing to generate the private Blockchain.

NodeJS, IPFS, Ganache, Metamask and truffle are used for implementation of proposed system. Ethereum Virtual Environment has been generated on the system. Smart Contracts has been deployed on Ethereum platform using truffle. Smart Contract access

the identity of issuer and student. Documents and records managed and stored using IPFS. Privacy of documents and identity managed using content address. Ether is generated from myether wallet for paying the transaction fees.

Our purposed system validated by uploading the college student's academic certificate on our system. Certificates and individual's identity successfully secured on Blockchain. Features of our proposed system can be executed successfully.

Chapter 4

Design of Proposed System TUDocChain

In this section the design and detailed implementation procedure of the proposed Blockchain on education TUDocChain has been described. It discusses tools and technique used in implementation and includes architecture, work flow diagram of the proposed system.

4.1 Brief Introduction on Ethereum

Ethereum is the crypto-currency released on 30 July 2015 by Vitalik Buterin[28]. Ethereum is an open source, public Blockchain established distributed computing framework and provide the functionality of smart contract[28]. It is an upgrade version of bitcoin i.e. changed from Nakamoto consensus via transaction based state machine. The ethereum Blockchain is an imperative a Transaction Based State Machine[29]. State transaction means when input is executed on system according to output transaction state has been changed. Transaction from one account to another has been performed using the ether value as a token. Go, C++ and Rust language is used for ethereum Blockchain. Proof of consensus algorithm has been used for mining the new transaction and block.

Figure 11: Ethereum[30]

During the mining process as discussed in chapter 1 nonce value is added between the hash value to increase the complexity of solving the equation by the miners. This

complex mathematical problem is known as block difficulty. The relation between the nonce and block difficulty has been shown mathematically as below [29].

$$N \leq \frac{2^{256}}{H_d} [29]$$

Where, N is the nonce value. H_d is the block difficulty. As the complexity of block difficulty increases it becomes harder for miner to find the nonce value.

4.1.1 Solidity

Solidity is an Object-oriented, high level language for executing Smart Contract[31].Smart Contracts are piece of code that command the nature of accounts within the Ethereum transition State. Smart Contract govern on Ethereum Virtual Machine. We have been implemented Smart Contract using ^5.0.0. Smart Contracts code effected from C++, Python and JavaScript programming language. Example of Smart Contract of storing data on the Contracts has been described in figure 17.

```
pragma solidity >=0.4.0 <0.7.0;

contract SimpleStorage {
    uint storedData;

    function set(uint x) public {
        storedData = x;
    }

    function get() public view returns (uint) {
        return storedData;
    }
}
```

Figure 12: Solidity Storage Program

4.1.2 Account

In Ethereum two types of accounts has been secured mapping 256-bit words to 256-bits words which shares the same address space; External Account consist of key pairs i.e. public and private key. Address is determined using the public key. Internal Account created by the execution of smart contract. Each account contains a balance in Ether (“wei” to be exact 1 ether is 10*18wei) [31]. Transactions have been done using Ether.

Every transaction is charged with amount of Gas, pay for the execution of transaction. Gas Price is a value generated by the transaction.

Price = gas price * gas required for transaction. [31]

4.2 Proposed Solution

We proposed a Blockchain based TUDocChain of academic certificates that provide issuing, securing and verification of transcripts in immutable and secure ledger. TUDocChain supports Ethereum, open source and public ledger. The IPFS generate the content address of academic certificate. Consortium Blockchain is used in securing and verification because the certificate management system is centralized system component and verification is done by the third party or other institutes. It consists of smart contracts, holding the information of issuer and receptor with document in the public ledger.

4.2.1 System Overview

TuDocChain is the platform of Blockchain in Education used to secure the academic certificate. Issuer with the hash value of the document and its private key generated from the myetherwallet upload the academic certificate on Blockchain. Students and passed out student authorized with a unique identification number. Through this ID they make request on platform after granting the request TUDocChain send a JSON RPC as response. Students want to apply in different institute through the certificate address. Verifier authorizes the student's records from the public distributed Blockchain. Figure 13 presents the overview of proposed system.

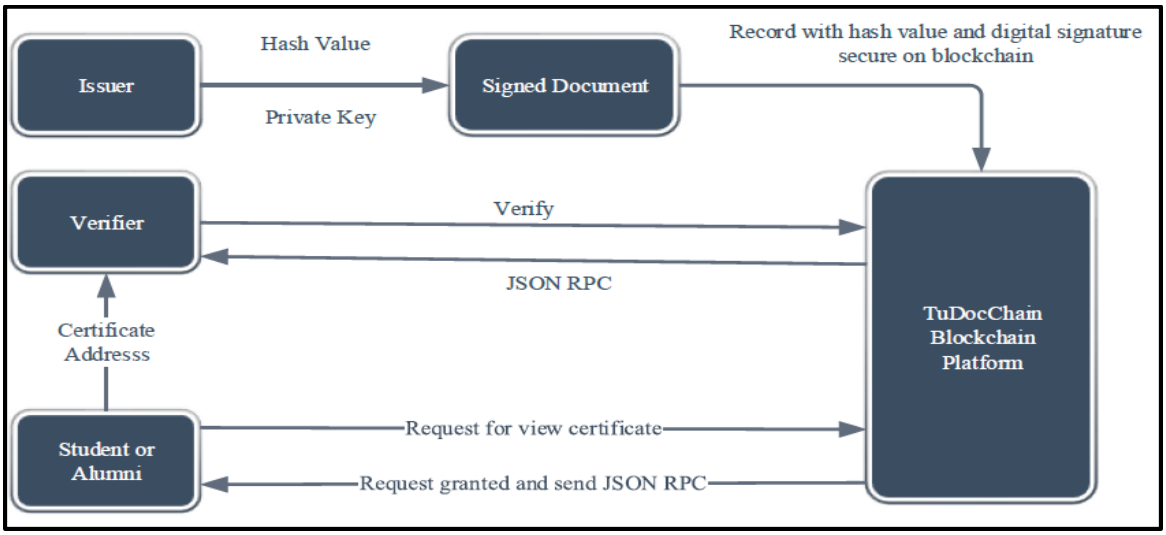


Figure 13: Overview of TUDocChain

4.3 Architecture of Proposed system

The Architecture of Proposed system describes the implementation of TUDocChain in Figure 14. It consists of Blockchain comprises Smart Contract, a distributed public ledger securing the identities of users and certification authority. A document management system i.e. IPFS interplanetary File System manages the academic certificates in the form of hash value where IPFS is a distributed web[32]. Documents have been controlled by using centralized NoSQL database MongoDB.

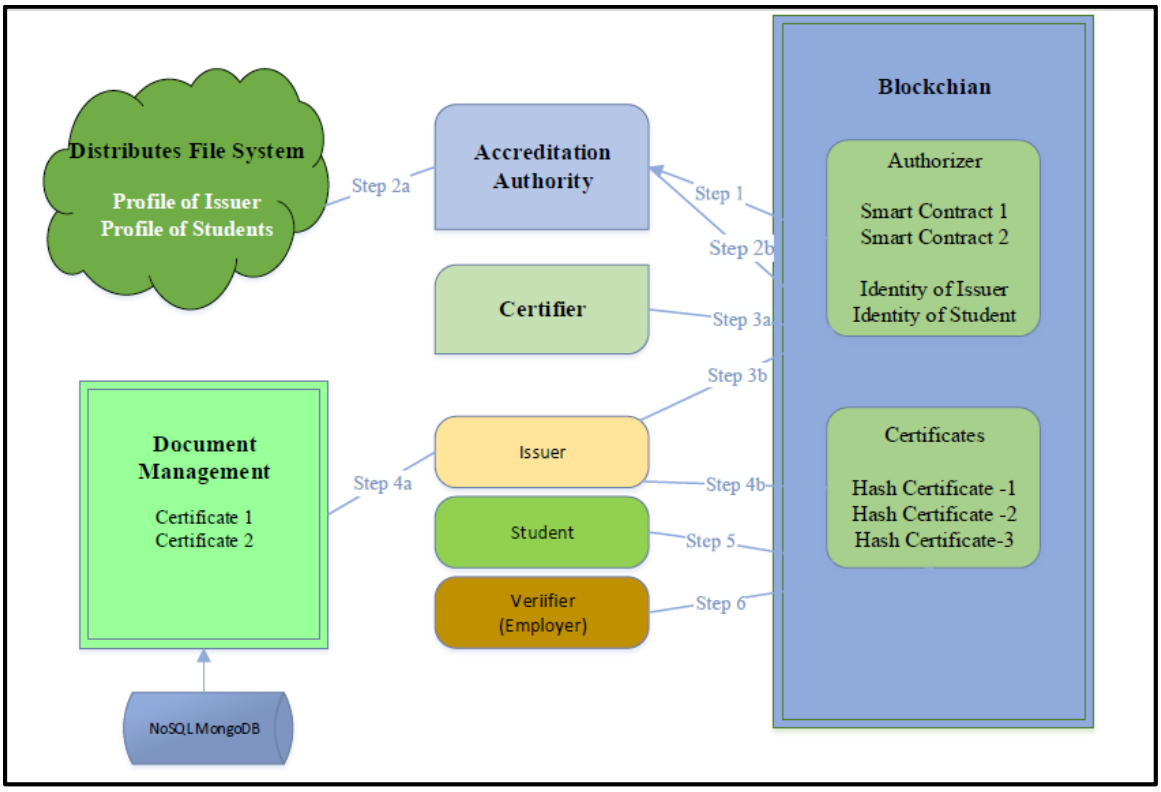


Figure 14: Architecture of TUDocChain

Initially smart contracts are secured on Blockchain by the authorizer in step 1. The first Contract (UserContract) manages the identities on Blockchain TuDocChain for Education framework and second one (CertificatemgmtContract) maintain the academic certificates issued by the issuer through the Document management use the NoSQL database query (Step 4a). MongoDB contain the details of Document in JSON and XML file. JSON file has been converted into PDF document. Document Management secures

the academic certificates in PDF Form. Issuer Access the Academic certificate on a centralized schema that increase the privacy of documents and personal information.

When Smart contract deployed (step 2a) then its certification authority's responsibility to add the address i.e. public key of issuer and authorizer on distributed file system (Step 2b). The records stored on Blockchain as a Public Blockchain is read only.

It maintains the identities as long term and tamper-proof. It maintains the name, country of issuer and students. Certification authority adds a public key address of issuer on Authorizer in Blockchain framework (Step 3b) and give him right to access the certificates. The authorized individual from the certification authority who kept the private key secures the certificate content as an address on Blockchain (Step 4b). Students receive and manage their academic documents from Blockchain (Step 5). Verifier easily verifies the records from the Blockchain directly without the involvement of authority and students not submit the physical documents to verifier. Verifier authorize the documents from the Blockchain by examine the crypto hash value of the certificate (Step 6).

4.3.1 IPFS as a distributed Tamper Proof Storage

The proposed Framework TUDocChain implanting on Ethereum Blockchain, On Ethereum based framework identities of certificate authority, authorization authority, issuer and students recognized by the Ethereum address i.e. hash of their generated public key. This provides the privacy of identities and third person not access the personal information.

IPFS add the identities and certificate on distributed web. All the hash value stored as a binary tree known as Merkle tree. Hash value build a distributed hash table(DHT). Transaction has been retrieved from the distributed hash table.

When the academic authority wants to register the new certification authority into the system first they add the information of individual by submitting public key on IPFS. Personal data has not been stored on the distributed web but their identity stored on Blockchain using the address as a public key's hash value. IPFS also contain the mutable files. If anyone wants to make the changes on records the content address changed means

crypto hash value has been changed. When verifier accesses the same documents he easily identifies the change of content address. IPFS provides the privacy and tamper proof ledger.

4.3.2 Work Flow of Proposed System TUDocChain

Workflow of the proposed system TuDocChain described in Figure 15. Five steps are followed for implementation process.

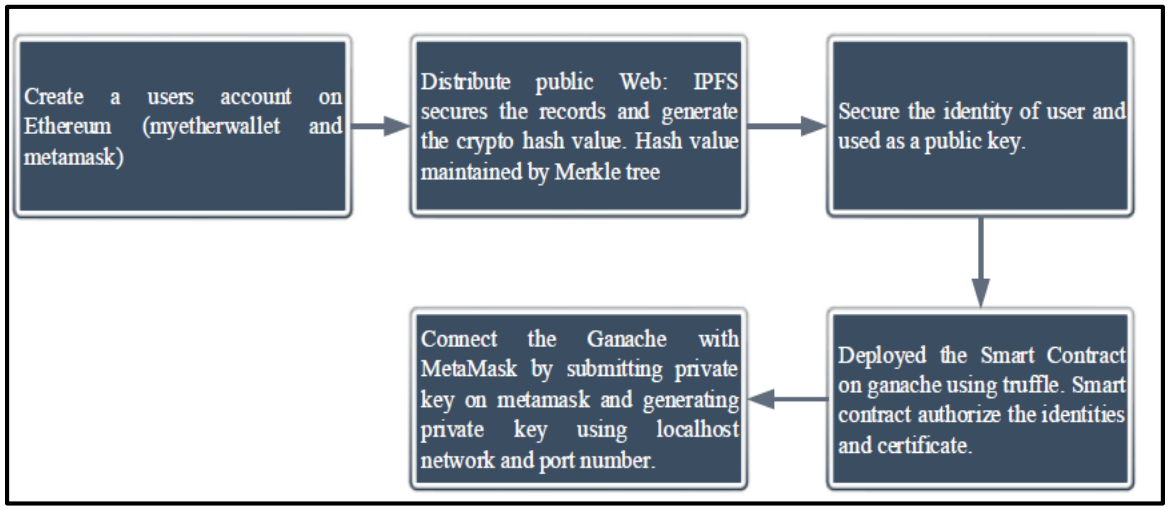


Figure 15: Work Flow of TuDocChain

4.3.3 Query Processing on Ethereum based application

In proposed system TUDocChain Certificate are stored on centralized database using NoSQL MongoDB. The records of students i.e. name of the students, grades, institute name, country, saved in the JSON file on MongoDB. These JSON file converted into the PDF format. Figure 15 described the query layer system.

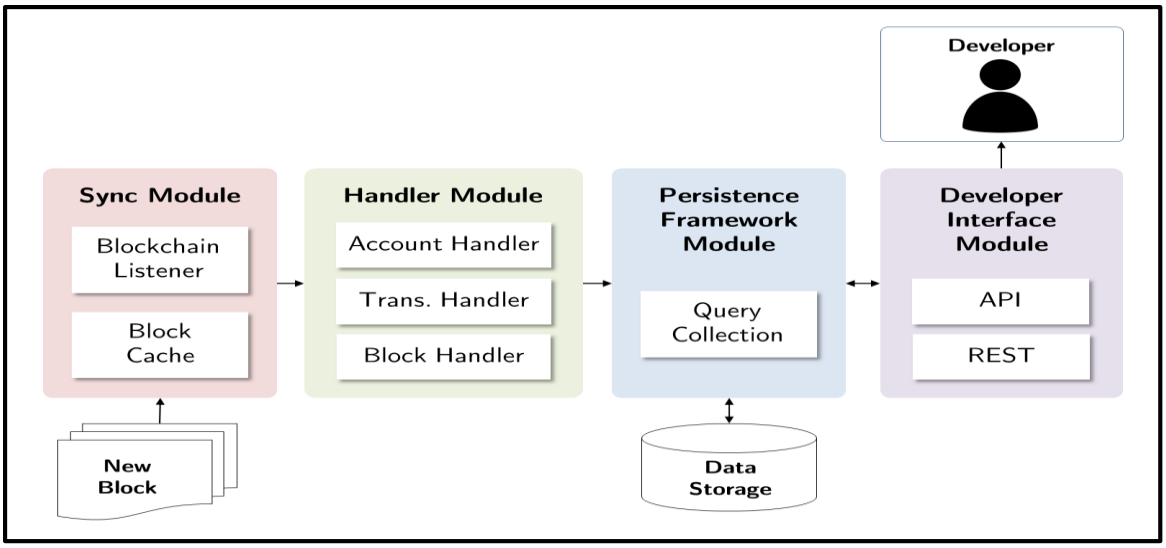


Figure 16: Query Layer System[33]

4.4 System Requirement

TuDocChain implemented on Ethereum Blockchain. Ethereum is the platform where Blockchain application has been operated. To implement Ethereum on system Ethereum Virtual Environment has been installed on system.

4.4.1 Tools

Following software is required for the implementation of system: -

1. **IPFS**

   IPFS is the interplanetary file system. IPFS is a distributed file system used to storing and retrieving the record, website and applications[32]. Record is uploaded on the IPFS and generated the content address. Based upon the content it generates the address as a crypto hash value. If the content is altered, then hash value of content changed according to the content. Crypto hash value is unique, deterministic, co-related and one-way. The length of content address varies according to the size of content [34]. The IPNS (interplanetary name system) contain the content address of content it changes according to modification in content. It secures the mutable links. The name in IPNS hash act as a public key [35]. It works on a command line prompt. IPFS work with the Go language. It works with the Java script files and NodeJS.

Figure 17: IPFS Logo [32]

2. Ganache

Ganache is a private Blockchain of Ethereum development used to deploy contracts, execute the application deploy by the truffle [36].ganache contains following components:

- Accounts: number of accounts deployed by the smart contract and individual participants in the smart contract [37].
- Blocks: number of blocks mined by the miners and shows the transactions used gas value. Balanced gas value [37].
- Transaction: Count of transaction stored on Blockchain.
- Contracts List: Deployed contracts used in smart contract
- Events: Describe the fired events during the chain's life [37].
- Logs: server require the logs for debugging [32].

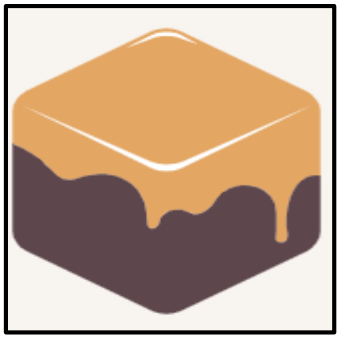


Figure 18: Ganache Logo [36]

3. Truffle

Truffle gives a development environment for Blockchain using Ethereum Virtual Machine(EVM)[38]. Truffle deploys, migrate and compile the smart contract. truffle perform the contract testing. Truffle managed the packages with EthPM and NPM. Truffle deployed the smart contract on ganache. Truffle configuration file has been created while developing the application on Blockchain.

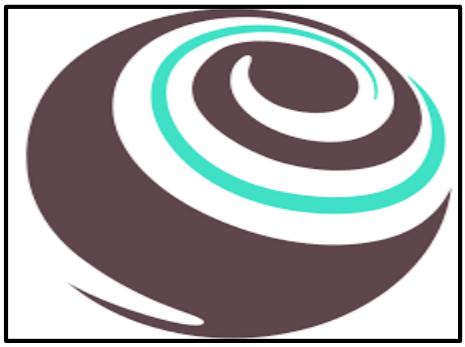


Figure 19: Truffle Logo[38]

4. MetaMask

MetaMask provide the interaction between the Blockchain application and the browser. Google chrome and Firefox provide the extension that connects to the Ethereum network without executing full node on browser's machine[39]. Metamask introduced its own web3 instance[39]. Blockchain application on localhost with metamask on network 127.0.0.1:7545. Account has been generated on the Metamask extension on browser. Choose the network as the localhost network and connect with Ganache. When transaction has been deployed, ganache sends Ether to the metamask and application is executed on localhost.

Figure 20: Metamask[39]

5. NodeJS

JavaScript is base of NodeJS, it is used for developing server based applications[40].NodeJS uses the library of JavaScript [40].The required packages installed using NPM. According to the requirement of application of system modules are installed using NPM. Truffle, IPFS installed using NPM. Using NodeJS our own module has been created using JavaScript. JSON package has been created using NPM. In our system we used 12.4.0 version of NodeJS and NPM version is 6.9.0. NodeJS run on PowerShell and nodejs command prompt. NodeJS uses the JavaScript runtime engine, same which is used by the google chrome[40]. NodeJS provide an additional feature over the JS engine makes the execution faster and processing of transaction on node increases. NodeJS manages all the simultaneous connection using single process.

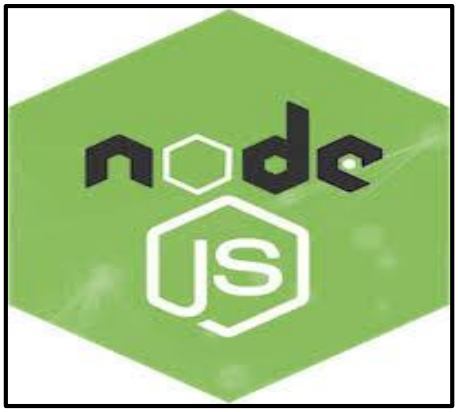


Figure 21: NodeJS [40]

Chapter 5

Implementation and Results

This chapter discusses about the implementation in detailed manner as well as the results of proposed system TUDocChain.

5.1 Implementation of Proposed System

This subsection presents the implementation steps: -

At initial step, install the IPFS on system. IPFS is the distributed web[32]. All the academic certificate secured on IPFS. Firstly, download the Go language on system then install the IPFS from https://docs.ipfs.io and kept the setup of ipfs on Go bin folder. IPFS works on Command prompt. On command prompt first initiate the IPFS using ipfs init. It stores all the documents on repository. Ipfs add the certificate after starting its Daemon and describe all the connection with swam. As shown in figure :21

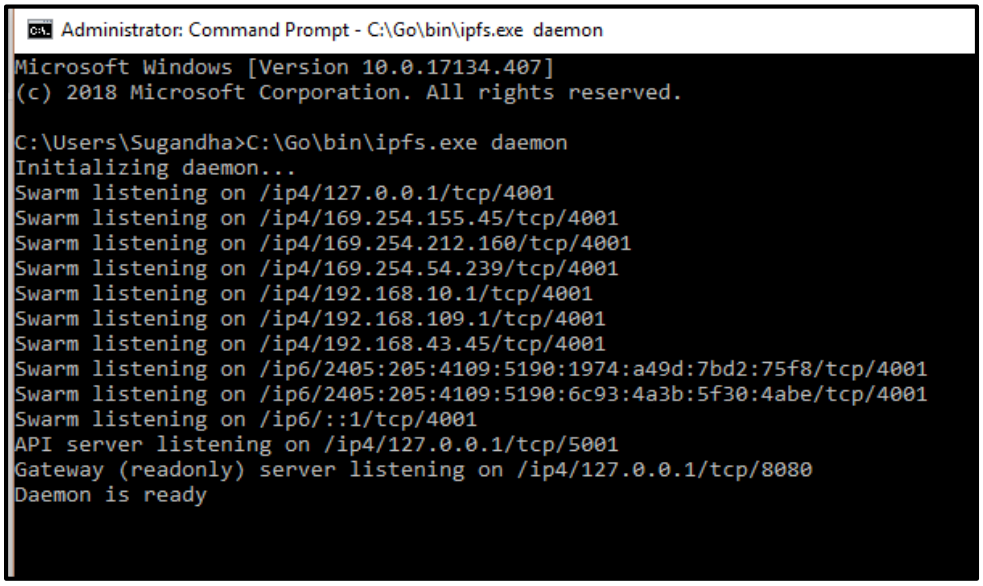


Figure 22: IPFS Daemon API

Add the file on IPFS as shown in figure 22. Crypto hash value is generated by adding the file on IPFS. It acts as public key address of the records. Multiple files are added on the IPFS as distributed file system. Merkle tree is generated; we retrieve the content address

of the records from merkle tree build on distributed web. The transactions are stored chronological order. IPFS maintain the transparency between the user and verifier.

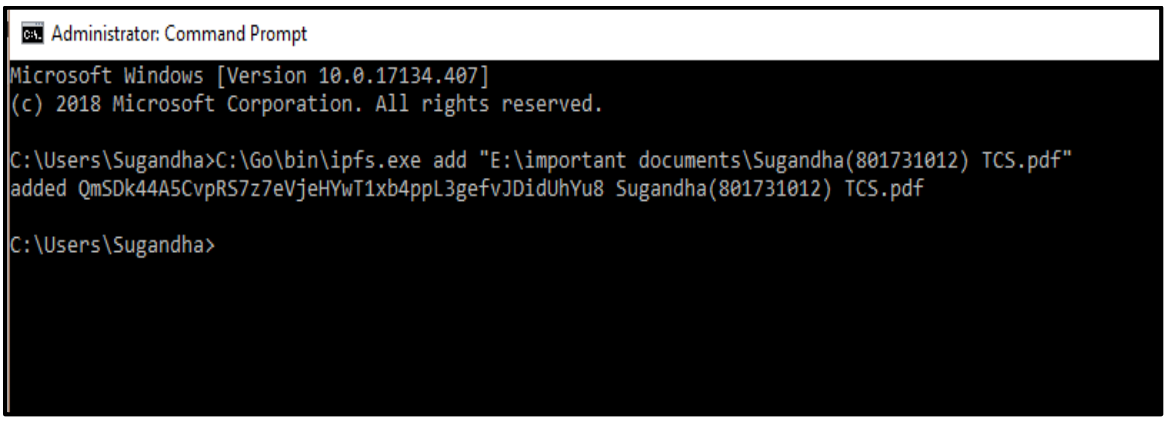


Figure 23: Adding File on IPFS

Then, established a server network by installing NodeJS. NodeJS based on JavaScript. NodeJS contain all the library of JavaScript. Using NPM installed all the required packages. In our proposed system we have been worked on nodejs version 12.4.0 and NPM version 6.9.0. Install the packages using npm install web3. We install all the packages on NPM using Command Prompt. On Window PowerShell install the following setup using Choco

i. Choco install nodejs. Install –y
ii. Choco install git-y
iii. Choco install visualstudioCode –y
iv. Npm install –g npm
v. Npm install –g – product
vi. Npm install –g ethereum js-testrpc truffle
vii. Npm install web3
viii. Npm install –g –production windows-build-tools

5.1.1 Implement Smart contracts

Three smart contracts have been implemented using solidity language on Ethereum Blockchain. User Contract, Certificate Contract and the migration contract. User Contract manages the identities and account balances between the individuals. Migration contract

migrate the contracts using truffle. Certificate contract authorize the certificates stored on IPFS. Figure 23 describe the UserContract, and Figure 24 describe the migration contract.

```
pragma solidity ^0.5.0;
contract Users {
mapping(address => bytes32) public users;
event UserCreated(address indexed _address, bytes32 _pseudo);
event UserDestroyed(address indexed _address);
function exists (address _address) public view returns (bool _exists) {
        return (users[_address] != bytes32(0));
    }
function authenticate () public view returns (bytes32 _pseudo) {
        require(exists(msg.sender));
        return (users[msg.sender]);
    }
function create (bytes32 _pseudo) public {
        users[msg.sender] = _pseudo ;
        emit UserCreated(msg.sender, _pseudo);
    }
function destroy () public {
        require(exists(msg.sender));
        delete users[msg.sender];
        emit UserDestroyed(msg.sender);
    }
function get (address _address) public view returns(bytes32 _pseudo) {
        require(exists(_address));
        return (users[_address]);
    }
}
```

Figure 24: User solidity

5.1.2 Truffle Configuration JS File

Truffle configuration file consist of network ID attached which network connected with the ganache. Both Ganache and truffle install from Truffle Suit. Truffle JavaScript file configure the JSON file on Ganache. Figure 24 describe the truffle Java Script file. Truffle migrate the contracts. Further in next step we discuss the truffle linking with the ganache.

```
module.exports = {
    networks: {
        development: {
            host: "localhost",
            port: 7545,
            network_id: "5777" // Match any network id
        }
    }
};
```

Figure 25: Truffle JavaScript file

5.2 Ethereum Account

User has been created an account on Ethereum platform mainly on myetherwallet and metamask. All the transaction fees transmitted from the user's account. According to the transaction payment fees gas value has been debited from the account. Firstly, generate a Node on myetherwallet select the option generate custom node. Figure 25 present the custom node, enter the private network address and port number.

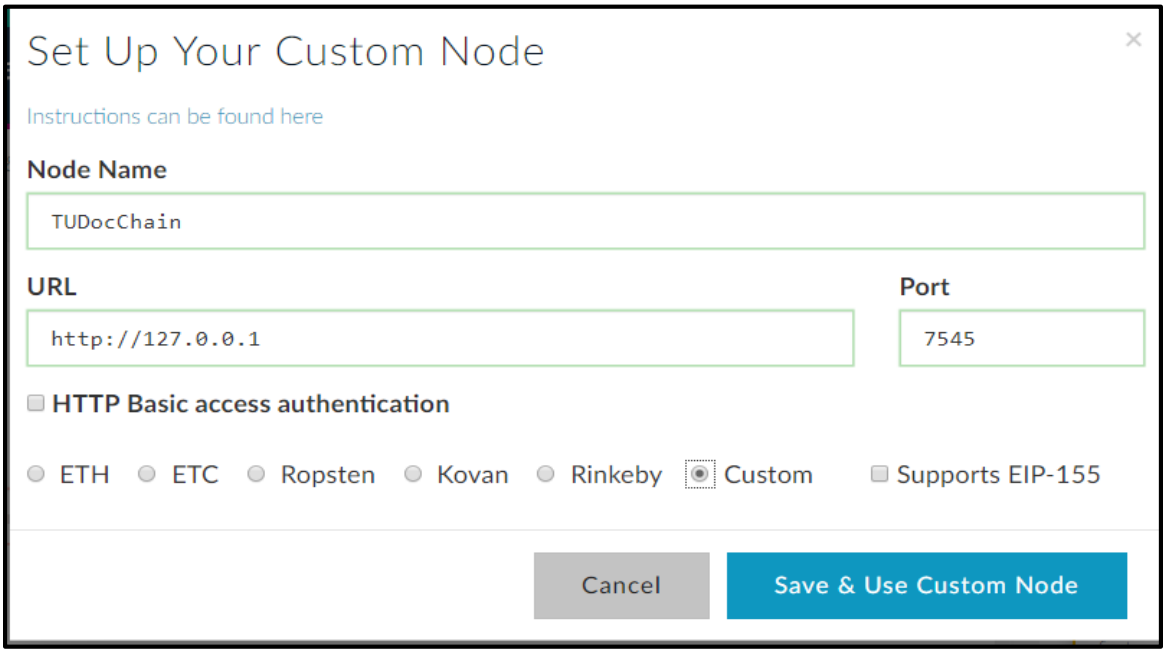


Figure 26: Generate a Custom Node

Generate an ethereum account using following steps:

Step1: Open www.etherwallet.com

Step2: Click on Create a new wallet in figure 26.

Step3: Create wallet by using JSON File mentioned on the webpage Figure 27.

Step4: Enter a strong password used for the generation of wallet.

Step5: Download the JSON file on system used for connecting with the metamask figure 28.

Step6: Wallet is created with private key and address key.

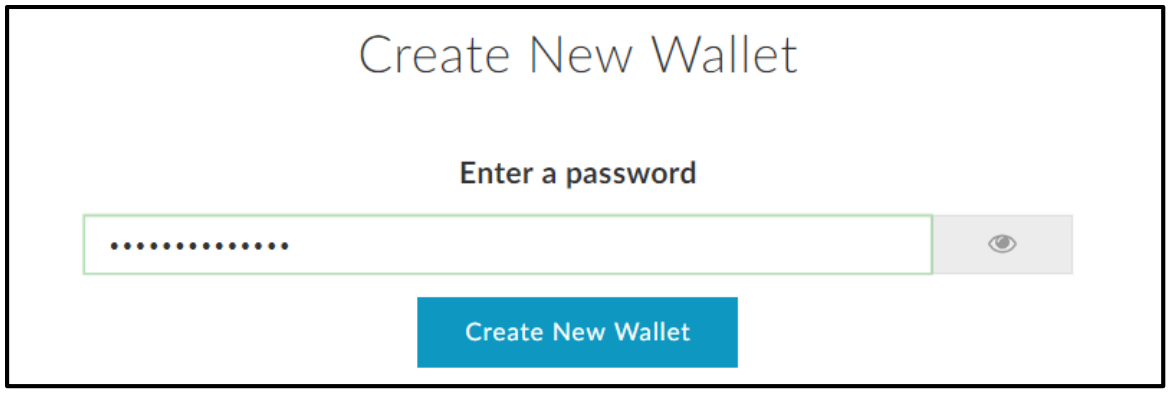


Figure 27: Create Password

Figure 28: Download JSON File

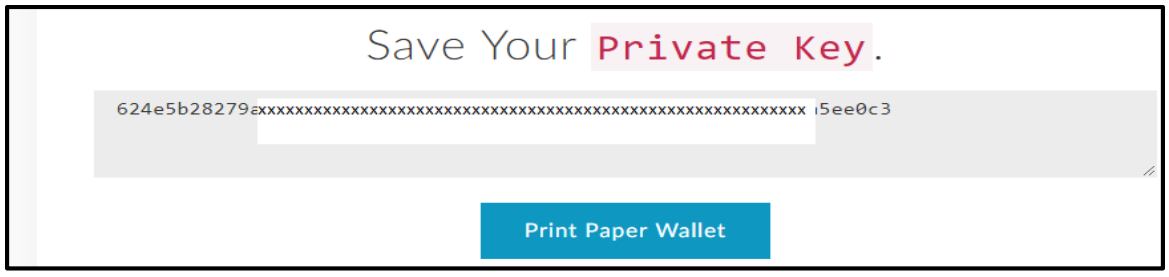


Figure 29: Save the Private Key

Figure 30: Private key and address

5.3 Truffle compile on Ganache

Ganache is the private Blockchain on Ethereum framework. Install Ganache on Desktop from Truffle Suit. First create a workspace on Ganache and compile the truffle.js file on Ganache. Figure 30 presents the compilation of project.

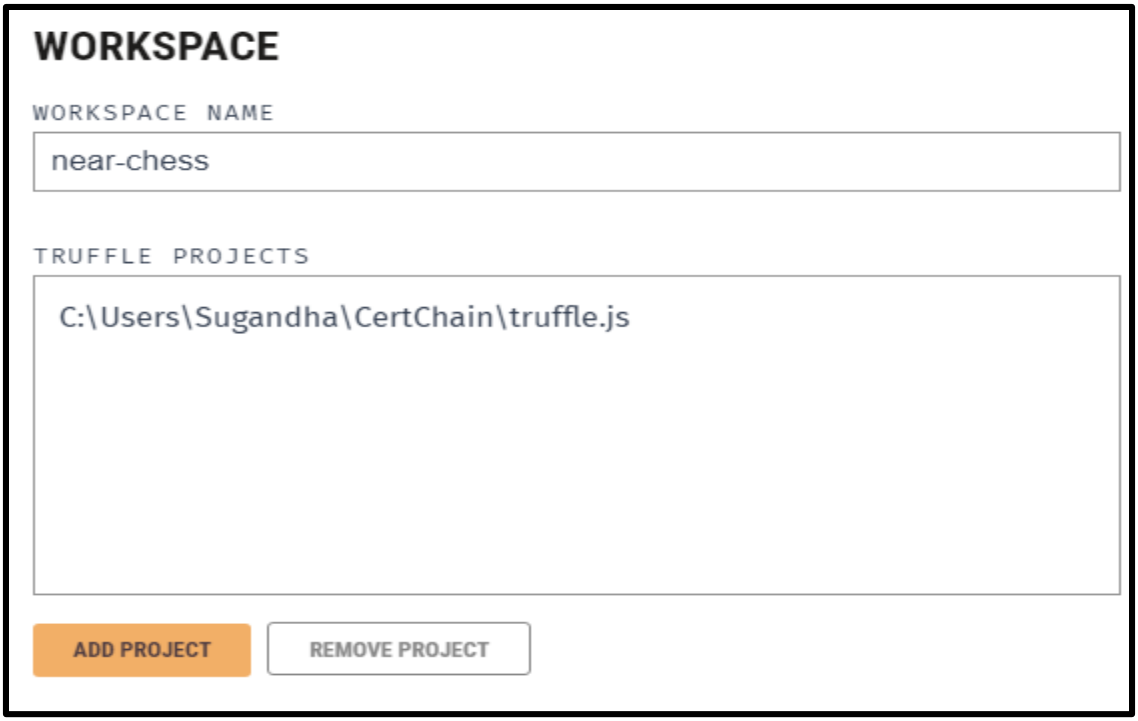


Figure 31: Ganache Work Space

Open the Window PowerShell on system. Here compile truffle all contracts compiled as shown in Figure 31.

```
Windows PowerShell
Copyright (C) Microsoft Corporation. All rights reserved.

PS C:\Users\Sugandha> cd..
PS C:\Users> cd sugandha
PS C:\Users\sugandha> cd certchain
PS C:\Users\sugandha\certchain> truffle compile
Warning: Please rename truffle.js to truffle-config.js to ensure Windows compatibility.

Compiling your contracts...
===========================
> Compiling .\contracts\CertChain.sol
> Compiling .\contracts\Migrations.sol
> Compiling .\contracts\Users.sol
> Artifacts written to C:\Users\sugandha\certchain\build\contracts
> Compiled successfully using:
   - solc: 0.5.0+commit.1d4f565a.Emscripten.clang
```

Figure 32: Truffle Compile

Now migrate all the contracts shown in Figure 32.

```
PS C:\Users\sugandha\certchain> truffle migrate
Warning: Please rename truffle.js to truffle-config.js to ensure Windows compatibility.

Compiling your contracts...
===========================
> Everything is up to date, there is nothing to compile.

Warning: Please rename truffle.js to truffle-config.js to ensure Windows compatibility.
Network up to date.
PS C:\Users\sugandha\certchain> npm run start
```

Figure 33: Truffle Migrate

Now execute npm run start in Figure 33.

```
PS C:\Users\sugandha\certchain> npm run start

> truffle-vue@0.2.0 start C:\Users\sugandha\certchain
> npm run dev


> truffle-vue@0.2.0 dev C:\Users\sugandha\certchain
> node scripts/dev-server.js

> Starting dev server...


 DONE  Compiled successfully in 30943ms                                                                1:52:16 PM
> Listening at http://localhost:8080

(node:3108) UnhandledPromiseRejectionWarning: Error: spawn cmd ENOENT
    at Process.ChildProcess._handle.onexit (internal/child_process.js:264:19)
    at onErrorNT (internal/child_process.js:456:16)
    at processTicksAndRejections (internal/process/task_queues.js:84:9)
(node:3108) UnhandledPromiseRejectionWarning: Unhandled promise rejection. This error originated either by throwing inside of an async function without a catch block, or by rejecting a promise
 which was not handled with .catch(). (rejection id: 1)
(node:3108) [DEP0018] DeprecationWarning: Unhandled promise rejections are deprecated. In the future, promise rejections that are not handled will terminate the Node.js process with a non-zero
 exit code.

 WAIT  Compiling...                                                                                    2:00:26 PM

 DONE  Compiled successfully in 760ms                                                                  2:00:27 PM
```


Figure 34:Execute Run Command

Ganache transactions are described in Figure 34. The accounts address, balance of Ethereum transaction. Number of transactions, Index value of the Block and Key provide the key address of transaction and account.

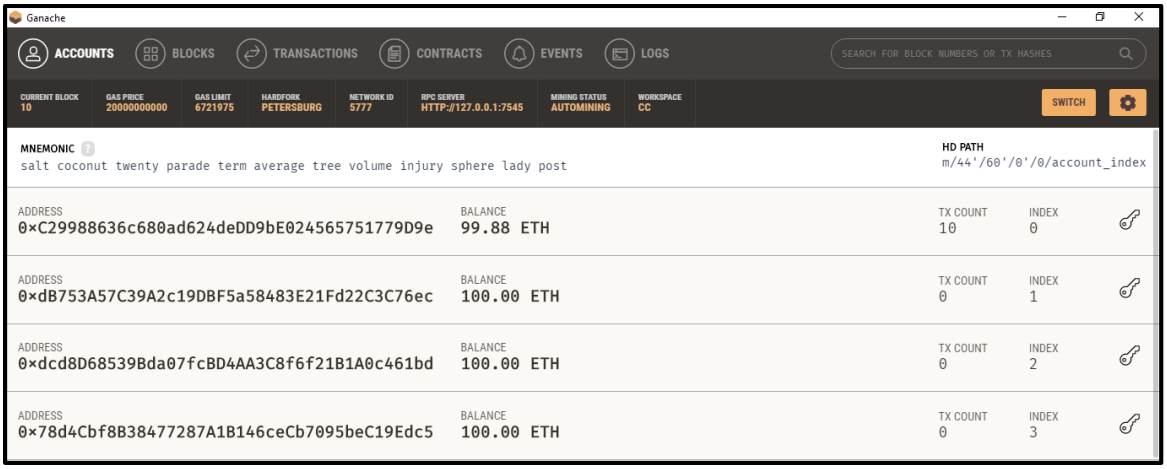


Figure 35: Ganache accounts

Ganache Shows the number of Blocks implemented on the Chain. Every Block is connected with the hash value of the previous block. Figure 35 presents the Number of Blocks in Chain.

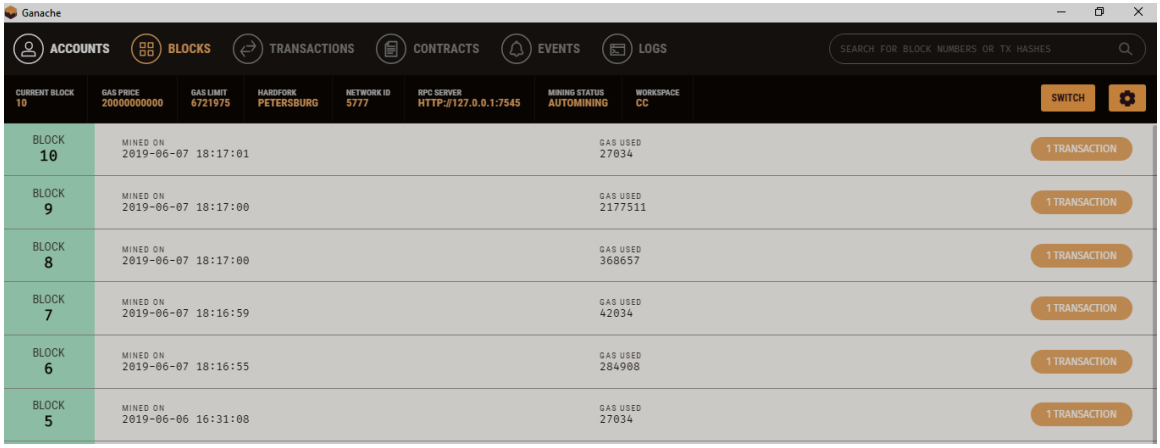


Figure 36: Ganache Blocks

Transactions executed on the Blockchain shown in figure 36 and figure 37 describe the contracts deployed on Ganache. Figure 36 shows the contract call and creation of contract.

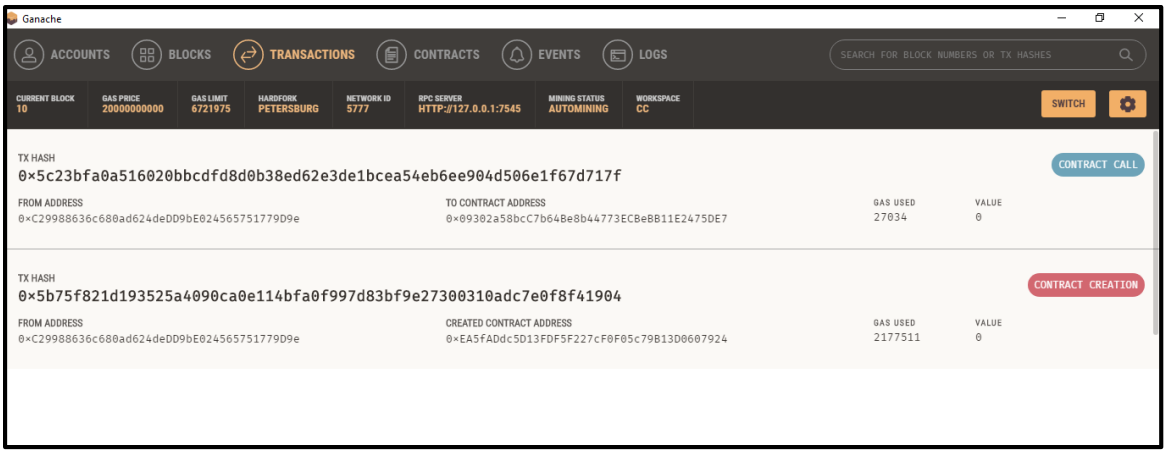


Figure 37: Ganache Transactions

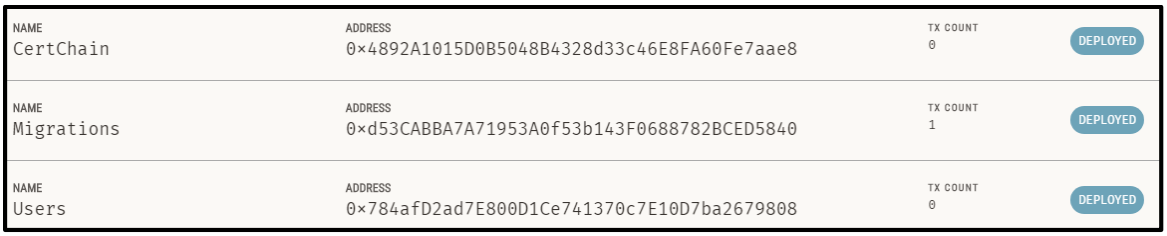


Figure 38: Contract deployed on TUDocChain

5.4 Results

The homepage has been presented on localhost localhost: 8080 network. TUDocChain manages the certificate on Ethereum based platform. Index page consists of two three pages Issuer page. On Issuer page issuer issue the certificate as the address of the certificate. All the transactions secured on TUDocChain in the form of address. Certificate secured using crypto-hash value of the document generated from the IPFS distributed storage. Recipient Page has been implemented for the students or alumni who want to view the certificate. Students shared their address with the verifier. Verifier enters the address of certificate on platform and view the existing certificate of students. Figure 39,40 and Figure 41 shows the home page, issuer page and the certificate view page.

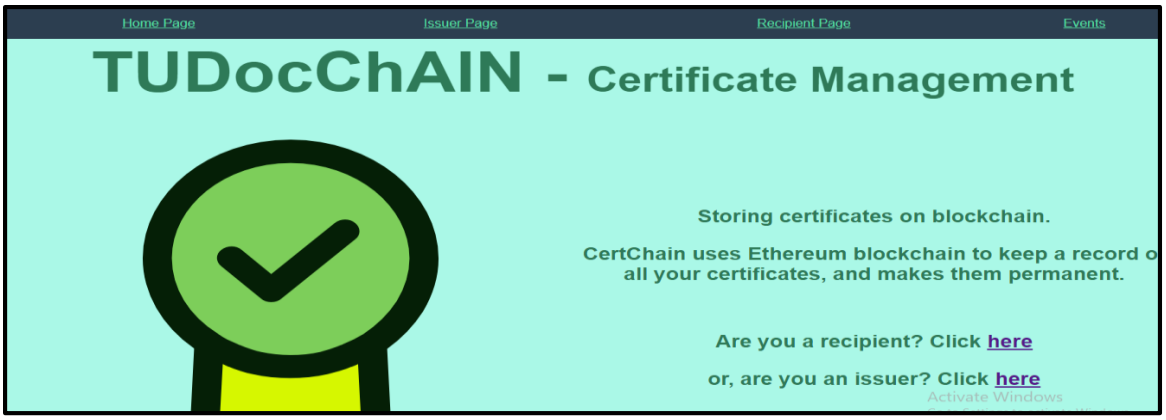


Figure 39: Index Page

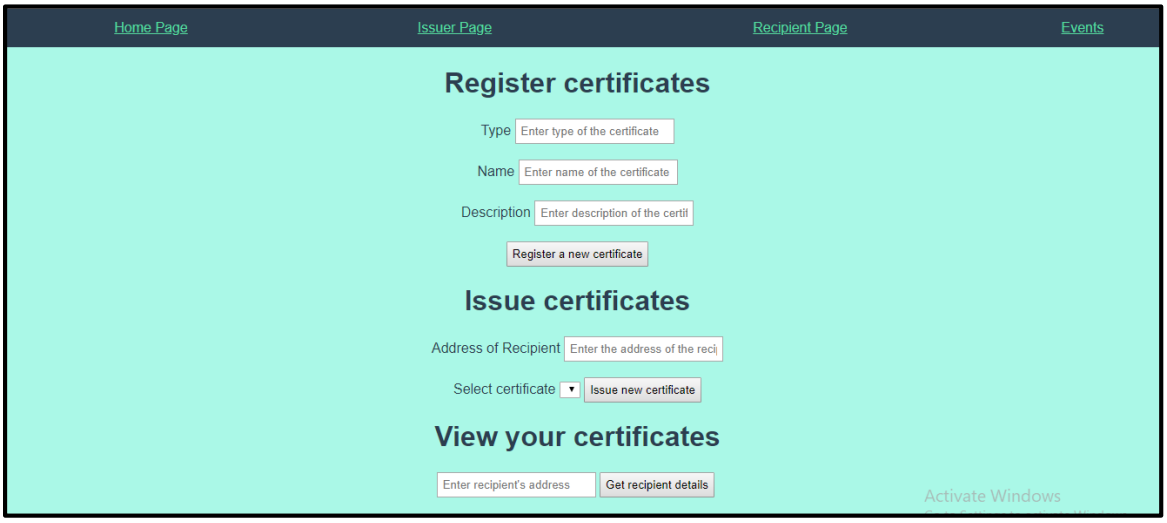


Figure 40: Issuer Issue Certificate using address

Figure 41: Certificate Page

Chapter 6

Conclusion and Future Work

In this work, we proposed a solution of authorizing the documents and securing school level documents and college academic certificates on one platform. The primary benefaction of presenting execution of Blockchain framework on Ethereum entitles security and immutability of records. The system provides digital records of students credentials that are easily verifiable by transact a gas value on Ethereum platform. It provides a verification feature for other organization employee (Third Party Stakeholders). Employee easily verifies the student's records using P2P Blockchain. The documents shared securely on distributed File management as a public distributed ledger. Through this public ledger multiple entities verify the data without the need for a centralized system. But transactions required a lot of computing energy and transaction fees which is paid by the certifier.

In future work, system main focus on connecting multi-institution records and online course certificate without using any transaction fees. Primary concern is maintaining privacy of individual identities while implementing standard permission less Blockchain.

List of Publications

[1] Sugandha Budhiraja and Dr. Rinkle Rani "TUDocChain-Securing Academic Certificate Digitally On Blockchain", 4th International Conference on Inventive Computation Technologies (ICICT- 2019), Coimbatore, TamilNadu, 29-30 August 2019. [Accepted].

References

[1] A. Grech and A. F. Camilleri, Blockchain in Education Inamorato dos Santos,A.(ed.) EUR 28778 EN ; DOI :10.2760/60649 Luxembourg : Publications Office of the European Union. 2017.

[2] G. Chen, B. Xu, M. Lu, and N.-S. Chen, "Exploring blockchain technology and its potential applications for education," *Smart Learn. Environ.*, vol. 5, no. 1, pp. 1–10, 2018.

[3] P. Ocheja, B. Flanagan, H. Ueda, and H. Ogata, "Managing lifelong learning records through blockchain," *Res. Pract. Technol. Enhanc. Learn.*, vol. 14, no. 1, 2019.

[4] Z. Zheng, S. Xie, H. N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: a survey," *Int. J. Web Grid Serv.*, vol. 14, no. 4, p. 352, 2018.

[5] "Blockgeeks" https://blockgeeks.com/guides/what-is-blockchain-technology/.

[6] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," *Proc. - 2017 IEEE 6th Int. Congr. Big Data, BigData Congr. 2017*, pp. 557–564, 2017.

[7] L. UG, "Blockchains & Distributed Ledger Technologies," *Blockchain hub*. https://blockchainhub.net/blockchains-and-distributed-ledger-technologies-in-general/.

[8] B. A. Tama, B. J. Kweka, Y. Park, and K. H. Rhee, "A critical review of blockchain and its current applications," *ICECOS 2017 - Proceeding 2017 Int. Conf. Electr. Eng. Comput. Sci. Sustain. Cult. Herit. Towar. Smart Environ. Better Futur.*, no. August, pp. 109–113, 2017.

[9] T. M. Fernández-Caramés and P. Fraga-Lamas, "A Review on the Use of Blockchain for the Internet of Things," *IEEE Access*, vol. 6, pp. 32979–33001,

2018.

[10] V. Arushanyan, “Nooor.io,” *Nooor Armenian Blockchian Association*, 2017. https://nooor.io/blockchain-in-education/.

[11] R. Arenas and P. Fernandez, “CredenceLedger: A Permissioned Blockchain for Verifiable Academic Credentials,” *2018 IEEE Int. Conf. Eng. Technol. Innov. ICE/ITMC 2018 - Proc.*, pp. 1–6, 2018.

[12] C. Colle and W. Knottenbelt, “Decentralised academic record verification using the Bitcoin block chain,” 2015.

[13] A. S. de P. Crespo and L. I. C. García, “Stampery Blockchain Timestamping Architecture (BTA) - Version 6,” pp. 1–18, 2017.

[14] S. LABS, “No Title,” *SAP LaBS*, 2017. [Online]. Available: https://news.sap.com/2017/07/meet-truerec-by-sap-trusted-digital-credentials-powered-by-blockchain/.

[15] SONY Global Education Team Sony develops system for authentication, sharing and right management using Blockchain Technology, https://www.sonyged.com/2017/08/10/news/press-blockchain/(2017).

[16] M. el Maouchi, O. Ersoy, and Z. Erkin, “TRADE : A Transparent , Decentralized Traceability System for the Supply Chain,” *Proc. 1st ERCIM Blockchain Work. 2018. Eur. Soc. Soc. Embed. Technol. (EUSSET)*, 2018.

[17] K. Al Harthy, F. Al Shuhaimi, and K. K. Juma Al Ismaily, “The upcoming Blockchain adoption in Higher-education: Requirements and process,” *2019 4th MEC Int. Conf. Big Data Smart City, ICBDSC 2019*, pp. 1–5, 2019.

[18] B. Wu and Y. Li, “Design of Evaluation System for Digital Education Operational Skill Competition Based on Blockchain,” *Proc. - 2018 IEEE 15th Int. Conf. E-bus. Eng. ICEBE 2018*, pp. 102–109, 2018.

[19] X. Gong, X. Liu, S. Jing, G. Xiong, and J. Zhou, “Parallel-Education-Blockchain Driven Smart Education: Challenges and Issues,” *Proc. 2018 Chinese Autom.*

Congr. CAC 2018, pp. 2390–2395, 2019.

[20] S. Goswami, S. Misra, and M. Mukesh, "A PKI based timestamped secure signing tool for e-documents," *2014 Int. Conf. High Perform. Comput. Appl. ICHPCA 2014*, pp. 1–6, 2015.

[21] M. J. M. Chowdhury, A. Colman, M. A. Kabir, J. Han, and P. Sarda, "Blockchain as a Notarization Service for Data Sharing with Personal Data Store," *Proc. - 17th IEEE Int. Conf. Trust. Secur. Priv. Comput. Commun. 12th IEEE Int. Conf. Big Data Sci. Eng. Trust. 2018*, pp. 1330–1335, 2018.

[22] H. G. Do and W. K. Ng, "Blockchain-Based System for Secure Data Storage with Private Keyword Search," *Proc. - 2017 IEEE 13th World Congr. Serv. Serv. 2017*, pp. 90–93, 2017.

[23] Z. Wang, Y. Tian, and J. Zhu, "Data Sharing and Tracing Scheme Based on Blockchain," *8th Int. Conf. Logist. Informatics Serv. Sci. LISS 2018 - Proceeding*, no. 61662009, pp. 1–6, 2018.

[24] I. Zikratov, A. Kuzmin, V. Akimenko, V. Niculichev, and L. Yalansky, "Ensuring data integrity using blockchain technology," *Conf. Open Innov. Assoc. Fruct*, vol. 2017-April, pp. 534–539, 2017.

[25] D. Augot, H. Chabanne, O. Clemot, and W. George, "Transforming face-to-face identity proofing into anonymous digital identity using the bitcoin blockchain," *Proc. - 2017 15th Annu. Conf. Privacy, Secur. Trust. PST 2017*, pp. 25–34, 2018.

[26] S. Mthethwa, N. Dlamini, and G. Barbour, "Proposing a blockchain-based solution to verify the integrity of hardcopy documents," *2018 Int. Conf. Intell. Innov. Comput. Appl. ICONIC 2018*, pp. 1–5, 2019.

[27] M. Labs, "MIT Media Labs," *MIT Media Lab*, 2016. [Online]. Available: https://medium.com/mit-media-lab/what-we-learned-from-designing-an-academic-certificates-system-on-the-blockchain-34ba5874f196.

[28] Ethereum wikipedia, "Ethereum," *wikipedia*. .

[29] Pretti Krisireddy, “how does ethereum works? anyway?,” *Medium Blogs*, 2017. https://medium.com/@preethikasireddy/how-does-ethereum-work-anyway-22d1df506369.

[30] Ethereum, “Ethereum,” *Ethereum*. 2016.

[31] Solidity, “Solidity,” *Github*. https://solidity.readthedocs.io/en/v0.5.10/index.html.

[32] P. Labs, “IPFS,” *Protocol Labs*. https://docs.ipfs.io/.

[33] F. A. Pratama and K. Mutijarsa, “Query Support for Data Processing and Analysis on Ethereum Blockchain,” *ISESD 2018 - Int. Symp. Electron. Smart Devices Smart Devices Big Data Anal. Mach. Learn.*, 2019.

[34] P. Labs, “hashes.”Available: https://docs.ipfs.io/guides/concepts/hashes/.

[35] P. Labs, “IPNS.” https://docs.ipfs.io/guides/concepts/ipns/.

[36] Truffle, https://www.trufflesuite.com/docs/ganache/overview.

[37] Truffle Suite Ganache .” https://www.trufflesuite.com/docs/ganache/quickstart.

[38] *Truffle*. https://www.trufflesuite.com/docs/ganache/overview.

[39] Truffle, “what is metamask.” https://www.trufflesuite.com/docs/truffle/getting-started/truffle-with-metamask.

[40] Guru99, “NodeJs.” https://www.guru99.com/node-js-tutorial.html.

[41] K.Kremanko "Blockchain A-Z Learn how to build your first Blockchain" http://www.udemy.com/build-your blockchainaz/learn/lecture/10005642?start=0#overview.

[42] R. Deol "Ethereum Decentralized Application Design and Development"

https://www.udemy.com/blockchain-developer/learn/lecture/8798028?start=0#overview.