MODELLING AND SIMULATION OF BLOCKCHAIN BASED EDUCATION SYSTEM

Navneet Kaur Bajwa

A Thesis

In

The Department of

Concordia Institute for Information Systems Engineering (CIISE)

Presented in Partial Fulfillment of the Requirements

For the Degree of Master of Applied Science (Quality Systems Engineering) at

Concordia University

Montreal, Quebec, Canada

August 2018

School of Graduate Studies

This is to certify that the thesis prepared

By: Navneet Kaur Bajwa

Entitled: Modelling and Simulation of Blockchain based Education system

and submitted in partial fulfillment of the requirements for the degree of

Master of Applied Science (Quality Systems Engineering)

complies with the regulations of the University and meets the accepted standards with respect to originality and quality.

Signed by the final examining committee:

Dr. Amin Hammad Chair

Dr. Jun Yan Examiner

Dr. Chunyan Lai Examiner

Dr. Anjali Awasthi Thesis Supervisor(s)

Approved by ______________________________

Chair of Department or Graduate Program Director

____

Dean,

Date ______________________________

ABSTRACT

Modelling and Simulation of Blockchain based Education system

Navneet Kaur Bajwa

Since Bitcoin's launch in early 2009, the industrial and academic interest in Blockchain and other cryptocurrencies have grown rapidly. Blockchains have been applied in many areas outside of finance such as healthcare, commerce and judiciary already. This technology promotes the creation of a decentralized environment where transactions and data are not under the control of any third-party organization. Blockchain is a fundamentally new technology that could revolutionize the future of transaction-based exchanges. Extensive research is being done in order to implement this technology various sectors. Blockchain technology comes with an edge of inbuilt auditability, trust and transfer of value which also makes it irresistible.

This work explores an agent based Blockchain-based Education System through mathematical modeling and simulation tools. The model is constructed to explore how Blockchain technology can be used to verify credit score of students, identify the occurrence and prevention of potential attacks. Along with technical characteristics of Bitcoin and Blockchain; cost, time and behavioural considerations of the system are also made. This is followed by analysing of the number of transactions, size of blockchain, network efficiency, cost analysis of the system along with the network efficiency. The proposed model, based on the blockchain technology shifts the education grading and credit rewarding system from the analog and physical world into a globally efficient, transparent and universal version. The work contributes a foundation for advancing current understanding of blockchain systems, and to further the development of simulation models of blockchains.

ACKNOWLEDGEMENTS

At this stage of work, I am becoming increasingly present to the fact that research can indeed be an enjoyable and rewarding experience, despite the tedium and hard work involved. This thesis report is truly the culmination of the support, motivation, generous help and teachings of my Supervisor, Prof. Anjali Awasthi. I can never forget the cheerful moment of my life when she accepted me as a research scholar. I must record my sincere gratitude to her for not only the great store-houses of knowledge she bestowed upon me but also for the chiseling and grooming that I received in large measure in spheres of academic, professional and personal life. Without her constant chase and help, this work could not have taken this shape.

My sincere thanks are also due to all my teachers at Concordia University for teaching and providing me with the knowledge which served as basics in compiling tis thesis. I would also like to extend my thanks to administration staff for the help and support they provided to me through my academic journey.

I would also like to extend my gratitude to my family who always believed in me and stood by me in every condition. Finally, I must thank GOD for giving me the environment to study and the potential to succeed.

Table of Contents

List of Figures

List of Tables

Chapter 1:

Introduction

1.1 Definition

Today's world has a never-ending need for improved efficiency. This statement can be extended to almost every field and industry like finance, jurisdiction and healthcare. Educational systems are no exception for a need of incorporating latest technology to improve their overall coherence. Blockchain technology allows the foundation of a decentralized environment where data is not under the control of any third-party organization. All the transaction ever completed is recorded in a public ledger permanently. This technology is anticipated to revolutionize the functioning of commerce, industry, and education and promote the rapid development of knowledge-based economy on a global scale. Blockchain technology is distributed in nature and uses the consensus algorithms and cryptograph techniques to determine the features of decentralization, immutability, traceability, and service properties [1]. These properties have the probable potential to prompt many innovative applications for education. Blockchain can gather and save a complete set of records of all the educational activities including the procedure and results in formal as well as informal learning environments. Also, it records teachers' teaching behaviors and performance and hence provides a reference for teaching evaluation. In this way, blockchain has great potential applications for both students and teachers [2].

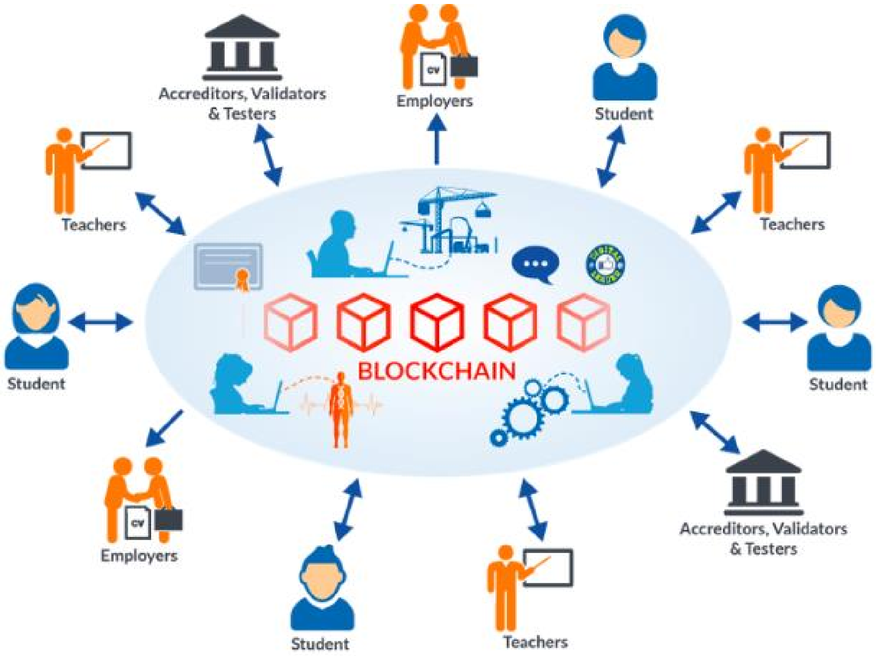


Figure 1-1: Educational Stakeholders likely to use Blockchain Technology [2]

Educational institutes spend millions every year to attract students from all around the globe in their programs and courses. This expenditure increases as their approach to do so widens which comes with an added costly and time-consuming activity of verifying each student's credentials and making sure of their authenticity. With the introduction of blockchain on system, the cost and time of this process can be immensely reduced. The Professors in the system will not be challenged for evaluating exams and awarding credits as every single detail for awarding marks and credits can be covered using pre-programed smart contracts. The students will have a say in their assessment before their results get published and recorded on the blockchain resulting in a fair formative crediting system. The students can also apply for further studies, internships and jobs anywhere in the world without the constriction of language time or distance. The potential employees are also set to profit from such a system as they can approach the upcoming talent globally.

1.2 Motivation

Most of the higher education institutions store their students’ completed course records in proprietary form. These databases are formed to be exclusively used by that institution's staff in a committed online system with almost no interoperability. These institutions also have their own specialized system to which students can have external access in a restricted and password protected manner to view or print their completed course records. There are numerable important points in regard to such systems which include storage location, standardization of data and safety. How to analyze, filter and securely share this data is also an important issue. Further, for legal reasons the Educational institutes must maintain the anonymous nature of students' completed course records. These records are mostly stored in different standards hence making it difficult to exchange records between different institute. Depending on the country’s policy some institutions do not share their students' information, not even the completed course records. This results in students experiencing difficulties in transferring to another Institute. This problem is even more complicated in cases when a student wants to transfer to another country, where more language, script and administrative barriers exist. When the student applies for a job position and has to prove his academic degree in a foreign country, problems arise from the centralized storage of students' complete course records due to their inaccessibility and lack of standardization. The students have to translate and notarize their academic certificate which is always a difficult and lengthy procedure. The notarization of documents includes the translation of all official documentation into the language of the applying institution, which is still subjected to reviewing and validation so as to examine matching or similar content. The problem faced by majority of graduates is that they do not have access to the online academic grading system. In such a case, if a student loses his academic certificates, he has to visit his home institute and request a new copy, which is again an expensive and time-consuming process. Although there are some consolidated standards for the academic credit system like the ECTS, the adoption and implementation of a global decentralized, trusted, secure credit platform, is a challenge. Many of the obstacles come from the fact that students' academic records are sensitive and have complex management regulations in place.

With an increasing number of diploma mills all around the world handing out fake degrees and diplomas a need to have a secure and authentic storage and record system is in great need. Currently, it costs universities more than £2m annually to fulfil degree verification requests which can completely be eliminated upon 100% implementation [3].

1.3 Thesis Objectives

The primary objectives of this research are:

- To simulate a Blockchain based Education system.
- To improve the efficiency of verifying student’s credit records using Blockchain.
- To reduce the possibility of attack on the Blockchain-based Education system.

These objectives are expected to be met by addressing the following study questions:

- What are the existing vulnerabilities in the Education systems?
- How these existing vulnerabilities be overcome using Blockchain?
- What are the attack vectors for the security threats posed on Blockchain systems?
- How can these problems be addressed and what are the possible solutions?

1.4 Thesis Contribution

This study presents an analysis of a blockchain-based Educational system. A simulation model is built that uses agents to form a framework of a working education system. An important insight is provided to the current issue of frauds being committed in the form of fake degrees, experience and faulty resumes to get into a university or a job. The proposed model uses a distributed ledger technology to create a globally trusted education grading system that would produce universally approved and adopted "learning passports". The model developed in Netlogo, differentiates the working of a blockchain based education system and the current education system. The five main agents used in the model include: main, participant, transactions, blocks, and local records. The participants are: Blockchain manager, Administration, Professor and student. Each of the participant uses their multi-signature private key to use the blockchain services. This multi-signature private key consists of the participant information (that is also stored in the central database) and biometric information. If this private key is lost or hacked, it will not be possible to use the services unless both the signatures are put together to revive the account. A comparison is made between the frauds and faulty practices being identified by the current system and the new proposed system. The model is formed using Gresham's Law and Trust function associated with Bitcoin and blockchain. Any model is considered to play three potential roles: generators, mediators, or predictors, as shown below in Figure 2. Generator is used to develop new theories about how systems behave, predictors provide specific outputs to study already well understood systems, while mediators have properties of both generator and predictor models [97].

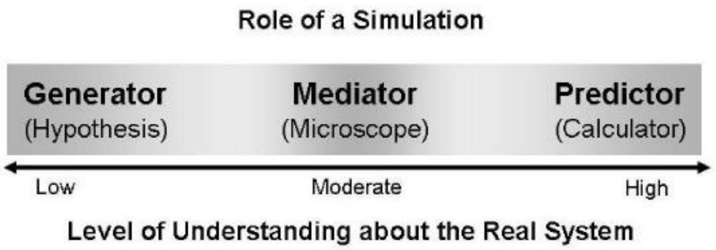


Figure 1-2: Role of a Simulation [97]

The proposed model is a mediator model as it provides insight into the behavior of the Bitcoin network while also providing some computational results. Three different experiments are performed on the system if a fraud is identified on the system or if the blockchain system is attacked (51% attack). The possible solutions identified for this problem are: Increase the waiting time and number of confirmations required for each transaction, Boycott the attacking entity, Attack the attacking entity using Distributed Denial od Service (DDOS). Our study sets a path for future research to expand the model for extended services like: payment of fee using and student registration using blockchain and the potential employees collaborating with the universities for starting specified courses to increase employment for the future graduates.

1.5 Organization of Dissertation

The remainder of this report encompasses the following chapters:

Chapter 2 provides a literature review of Education Systems Blockchain and blockchain based systems, agent-based modeling and simulation.

Chapter 3 presents the methodology including proposed model, simulation framework, agents, parameters and state variables.

Chapter 4 The results and discussion found during the analysis.

Chapter5 presents the conclusions and future scope of this research summarizing the outcomes of the analysis and gives recommendations for future work.

Chapter 2:

Literature Review

This literature review is broken into sections that describe modeling and simulation related works, blockchain or Bitcoin related works and blockchain in education. Some resources are multidisciplinary in nature, such as the application of modeling and simulation to education networks and application of modeling and simulation to blockchain networks.

2.1 Simulation

A predictor model can be built in a way that a simulation will behave in a precise manner if a system is well understood. Such a model will provide realistic outputs when given realistic inputs. The role of simulation moves towards being a generator model as less information is known regarding the behavior of a system. Generator models can be used to hypothesize about the underlying structure and resulting behavior in a complex, poorly understood system. Agent based modeling is particularly useful as generator models by observing, modeling, and then simulating individual behaviors for agents, one can try to duplicate emergent properties from the real world from the interactions that occur between the simulated agents.

An insight to the purpose of developing models and simulations is revealed by assuming that simulations can give valuable information without needing to completely replicate a true system. The simulation is used as a representation of the true system. Heath identifies three roles that a simulation may serve depending on the level of understanding about the real system [3].

Simulation is best adapted to analyze complex practical problems when it is not possible to solve them through a mathematical method. The simulation software used in this thesis is Netlogo [4]. It is a multi-agent programming language and modeling environment for simulating complex phenomena. It is outlined for both education and research purposes and is used across a broad range of disciplines and education levels. In this paper, though, we focus on NetLogo as a tool for research and for teaching at the undergraduate level and higher. Simulation in Netlogo is flexible, hence changes in the system variables can be made to select the best solution among the various alternatives. The experiments in simulation are carried out with the model without disturbing the system. Moreover, Policy decisions can be made much faster by knowing the options well in advance and by reducing the risk of experimenting in the real system [4]. Also, NetLogo is an environment that is simple and enable researchers and students to create their own models, even if they are not professional programmers. After five years of development, NetLogo is a mature product that is stable and reliable. It comes with extensive documentation and tutorials and a large collection of sample models. The software was best suited to represent a complex and distributed network like Blockchain and any blockchain-based model.

2.2 Blockchain

A blockchain is a distributed database of records of all transactions or digital events that have been executed and shared among participating parties. The participants of the system validate all the transaction in the public ledger is validated by consensus of most of the participants of the system. And, once entered, information can never be erased. The blockchain holds a verifiable record of every single transaction ever made thus resulting in universality of these records.

2.2.1 How can Blockchains add value to the Education systems? Strengths

Through its typical features, the blockchain can add value to education systems and education systems digitalization in several ways and are connected to building trust, network expansion, visibility, provision of secure data [1].

- **Trust:** Because blockchain is based on shared consensus among different parties, the information on the blockchain is reliable. The participants build up a reputation on the blockchain over time which demonstrates their credibility to one another. Moreover, a third party, that arranges trade between two partners will no longer be necessary because of the trust present in the blockchain network. To establish enough trust and to become connected in a blockchain network, the motives of the involved parties must be clear [27]. The reputation of the participating organizations is now transparent and grows over time. In the education systems, it is important that companies in the chain can trust each other to share information and increase efficiency in shared processes.
- **Enhanced Security:** The validity of the information stored on the blockchain is ensured by an encryption mechanism. This results in a solution for the difficult process of writing information on the ledger and validating it. The complex technique not only ensures the authenticity of the information, but also prevents fraud. Practically, changing the information stored on the block becomes highly unlikely after six blocks have been added onto each other.

- **Greater transparency**: Transaction histories are becoming more and more transparent by using blockchain technology and can thus only be updated through validation, which means everyone must agree on it. All subsequent records and the collusion of the entire network needs to be changed to alter a single transaction. It is also available to all participants who have permissioned access [2].

- **Network Expansion:** The blockchain technology stimulates interconnectivity and network expansion thus adding value to the education systems. In the case of a public and open blockchain solution, the network would become decentralized and the participants (learners, teachers, employers) would be able to connect individually and not just via a centralized party. This will result in standardisation of technology used in education systems all around the world thus allowing different education systems opportunities to work together in a unique way.

- **Improved traceability**: Since all the transactions are recorded permanently on the blockchain network, any exchange of data or requests ever made can be completely and effortlessly traced.

- **Increased efficiency and speed**: When paper-heavy processes are used all the processes are time-consuming and prone to human error. By automating and streamlining these processes with blockchain, processes can be completed faster and more efficiently. When all the participants have access to the same information, it becomes easier to trust each other without the need for several intermediaries [5,6,7].
- **Reduced costs**: Cost reduction is a priority for most of the enterprises. With blockchain, no middlemen are needed to make guarantees. Instead, all the participants just must trust the data on the blockchain. Also, participants must review all the included documentation to complete a request because everyone will have permissioned access to a single, immutable network.

2.2.2 Limitations of Blockchains

The blockchain industry is still in the infancy of development and comes with many kinds of prospective limitations. These external and internal limitations comprise of technical issues with the underlying technology, public perception, government regulation, and also the thought adoption of technology [23].

2.2.3 Issues in Practical implementation

Prior to the development of current applications of blockchain technology, there are many considerations that must be addressed. These are largely associated with the transformation that must happen within the institute and therefore the amendment in mental attitude that must occur. The subsequent main considerations will be outlined: issue of adoption, lack of trust, want for governance and legal problems.

- **Difficulty of adoption:** The difficulty of adoption is divided into technical and functional considerations. Consultants within the field of blockchain technology foresee an eternal method of trial and error of single-use applications that may cause uncertainty among educational institutes to take a position. First, single-use applications should be developed. Over time, the paradigm shift of innovation can occur within the type of a single-use application or an extended version of a single-use application, can replace obsolete applications. However, additional computing power is needed to implement the blockchain technology on a very large scale.

- **Lack of trust**: In a nutshell, implementing blockchain technology raises queries regarding the responsible knowledge of the participants. The second concern to relocate data systems would be the resistance to share information with supply chain partners. Corporations don't seem to be doubtless to share important knowledge that might make them vulnerable. A blockchain configuration changes this attitude since the technology itself works as a guarantee of trust within the parties.
- **Need for governance:** Once more participants are connected, queries about the governance of the system can arise, such as who is authorized to access data (accessibility) and who owns the data (ownership) shared in the blockchain. Moreover, within the case of a private blockchain network, there is the question of who the neutral party to blame of setting the network rules and granting access permission is.
- **Legal issues**: No clear regulations are yet in force in this area (need for regulation), since the blockchain remains to be an emerging technology.

2.2.4 Architecture

This section provides a summary on blockchain technology for clarification of its operating mechanism, most of the applications and the key features. It aims to elucidate the practical framework of Blockchain network therefore making further chapters of this thesis simple to understand. A blockchain is a platform for retentive transactions that are shared among all the participants of a network. The peer-2-peer network utilizes a consensus mechanism that records the ledger once ensuring a valid transaction. The participant who wants to make a transaction must experience a validation process transaction by providing the same hash as the other participants of the network. The hash is a unique code that describes a message with specific data. This valid information is registered on a block [5].

- **Blockchain Phenomenon**

There are different measures of blockchain technology on the market. For example, the technologies operating as the backbones of Bitcoin and Ethereum introduce completely different standards and that they represent different platforms, even though they are each decentralized consensus networks. The blockchain applications are implemented on top of a given platform to provide extra functionalities which are not initially available. The blockchain services do not need a technical link to the blockchain and they make use of the present functionalities of a blockchain or an application that is more effective [6].

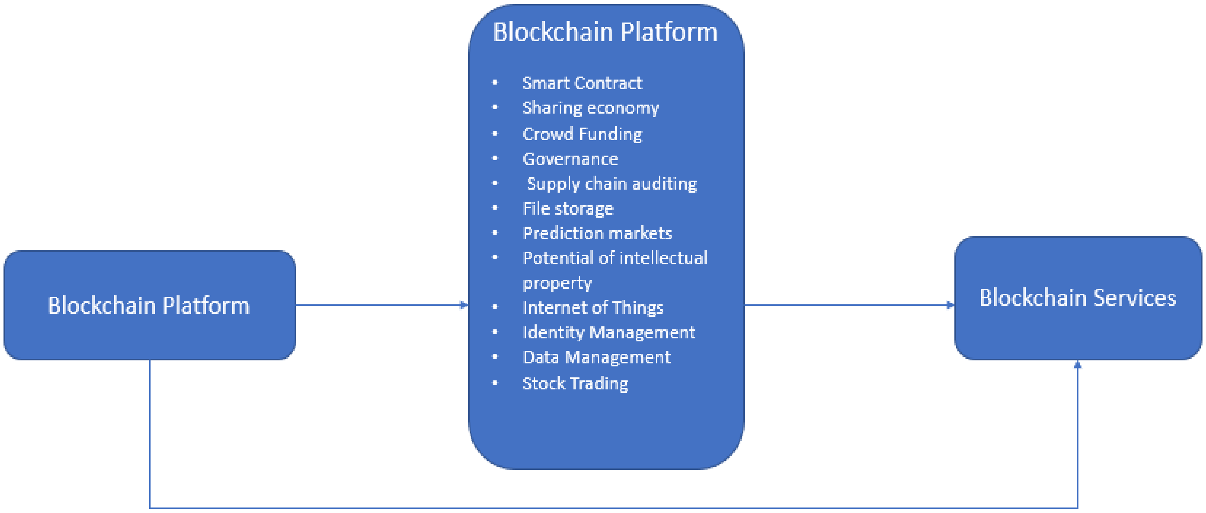


Figure 2-1: Framework of Blockchain analysis (Blockgeeks)

- **The 4 Ps of Blockchain**

  The initial blockchain construct was 100% de-centralized and utterly public. However, since separate applications require separate level of security this structure does not prove economical for all timestamped ledger applications. Thus, blockchain architecture designs are often classified as either public or private and permissioned or permission-less [8]. The public and private blockchain are distinguished at level of platform accessibility. In a Public platform all the participants involved in the Blockchain are allowed to create transactions whereas in a Private Blockchain such authorization is given to a selected participant. [9].

PROPERTY	PUBLIC BLOCKCHAIN	PRIVATE BLOCKCHAIN
CONSENSUS DETERMINATION	All Parties	One party
READ PERMISSION	Public	Public or Private
IMMUTABILITY	Nearly impossible to corrupt	Could be corrupted
EFFFICIENCY	Low	High
CENTRALIZED	No	Yes
CONSENSUS PROCESS	Permission-less	Permissioned

Table 2-1: Comparison between Public and Private Blockchain

Unlike Private and Public Blockchains the distinction between permissioned and permission-less blockchains relies on the authorization of writing and voting on the platform. In a Permissioned ledger the selected participants can counsel an update and participate in validation process. On the other hand, in Permission-less ledgers anyone has equal authorization in these processes. Hence in such system, there is no single owner of the data: everyone who has access to the data is an owner.

PROPERTY	PERMISSIONED BLOCKCHAIN	PERMISSIONLESS BLOCKCHAIN
CONSENSUS DETERMINATION	Selected Parties	All party
READ PERMISSION	Private	Public or Private
IMMUTABILITY	Nearly impossible to corrupt	Could be corrupted
EFFICIENCY	Low	High
CENTRALIZED	Yes	No

Table 2-2: Comparison between Permissioned and Permission-less Blockchain

- **Nodes and ledger Architecture**

The Blockchain is a network that runs on a network of distributed servers. The main application may be a transaction database modeled as a secure ledger. Any node running the Blockchain software will run the complete Blockchain locally. Blockchain data can often be recorded in a file or in a relational database looking on user preferences.

The key feature of Blockchain technology resides in its distributed nature [18]. It is completely different from centralized and decentralized networks because a distributed computing network system could be a system where data and resources are opened out on varied hardware nodes. Moreover, every node maintains an information of historical and valid transactions, which is sent among the nodes within the network. Despite every node holds a replica of the ledger, only those participants that hold the signature on it can access the data.

The nodes determine one another by their IP address, whereas participants address to each other through their public key. Every node represents a physical/virtual machine that communicates via different nodes [17]. Therefore, every node will send a transaction to every other node in the network if it is aware of the receiver's public key, without any central authority involved in the transaction.

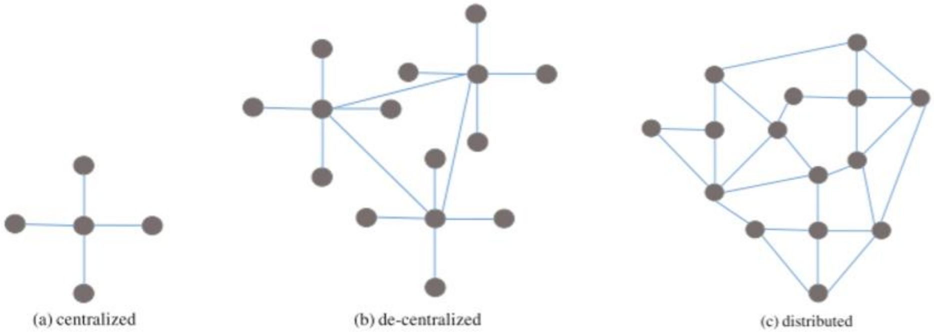


Figure 2-2: Types of networks [17]

The absence of a central server strengthens the system's security, since it makes harder for a network to experience attacks such as 51% attack or Sybill's attack. Moreover, altering a transaction of the chain needs large hash-recalculations for each block registered once the changed block, resulting in an improved security protection. Therefore, the blockchain is constructed on a consensus mechanism that represents a trust-worthy invisible authority [15].

The following architecture diagram captures the main layers of the Blockchain along with their roles.

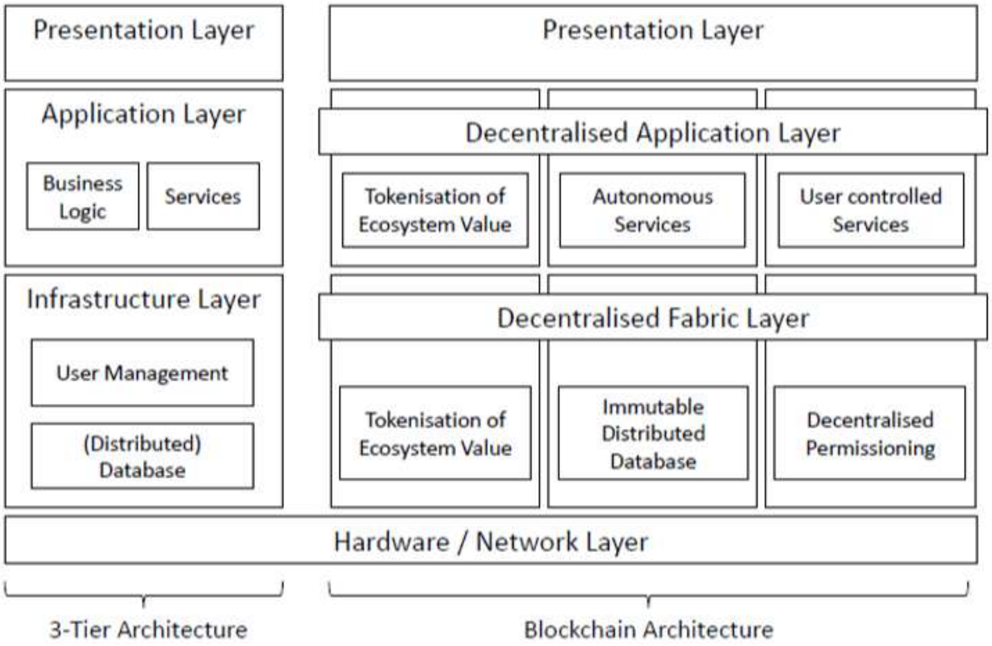


Figure 2-3: Blockchain architecture [15]

The first layer is called fabric layer and is a common conception within the global blockchain development community. The second layer contains the application logic of services enforced in variety of smart contracts. Services based on one or more smart contracts are commonly called Decentralised Applications (DApps) [17].

The Fabric Layer. It is important to notice that there is a robust centralisation of management of the fabric layer. Whoever develops and maintains the fabric layer is in the final control of the full system's functioning. Even if the participant cannot directly modify the state of the system as represented by the blockchain information, the fabric layer is developed by a one institute and also the code base is not open source, the full system can continually be in the hand of this institute. If it is kept open source, the organization of developers and maintenance of the code is a lot more complicated. We refer to [19, 20, 21, 22] for background on open source communities. This is often something that has to be thought about in the context of software system adoption by institutions as is emphasized by [29]. The fabric layer fulfills basic services. Databases typically associate with an integrated module to manage differing kinds of users which will have completely different levels of permission. As an example, a user would possibly be able to browse certain subsets of the information and is not allowed to send any transactions, i.e., changes to the information. The permissioned participant usually has the full set of rights or can grant them. Blockchain systems, thus far build no differentiating between users and user management modules and only offers rudimentary practicality like account creation and basic countersign management. This additionally implies that each user has full transparency concerning the transactions and deployed smart contract code of alternative blockchain system users.

The Application Layer. The blockchain itself is developed by a group of architects and developers and thus is often in restraint of these development groups. On the other hand, the code of the application layer is written to the system by any participant. The code itself is in restraint of the participant who deployed the piece of code. It follows, that the management at the application layer is distributed among the participants who deployed the code. Once the system begins and users start deploying their own code onto the blockchain system. Consequently, the management of the application layer is pushed into the hands of decentralised participants. The code of smart contracts can be in-built so that the management is entirely left over to the piece of code deployed. If a transaction includes a smart contract code, a new user (address) is registered within the system. The code becomes autonomous if there is no access control mechanism implemented by the participant who deployed the smart contract. This results in a setup where only the piece of code itself 'determines' once it is triggered, supported on the programmed rules it contains.

Blockchain is a sequence of blocks which contains a list of transaction records like conventional public ledger [10]. Each consecutive block is connected to the immediate previous block by a reference that is notably a hash value of the previous block referred to as a parent block. The uncle blocks (children of the block's ancestors) hashes would also be stored in Ethereum blockchain [11]. The first block of a blockchain is called genesis block which has no parent block.

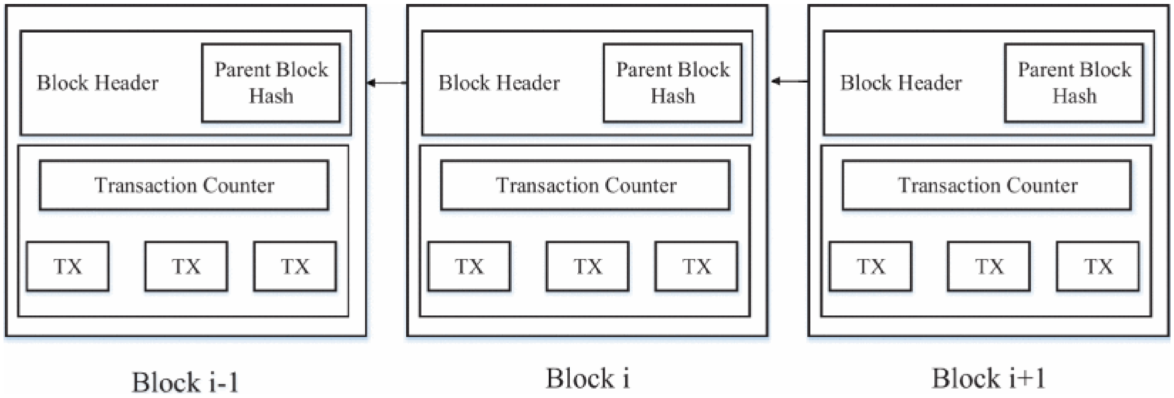


Figure 2-4: Connection of Blocks [11]

Each node within the network features a set of public and private keys. Before a transaction, the sender needs his private key and the receiver's public key. Moreover, before being recorded on the Blockchain, the transaction needs to undergo two phases: a signing phase and a verification phase. On the one hand, the sender's encryption of the data with the private key is defined as the signing phase. On the other hand, the verification phase consists of the solution of a computational problem which ensures that the same transaction is not happening twice [13].

The understanding of Blockchain technology can be made better through the introduction of some of some fundamental concepts:

i. Node: A Blockchain is maintained by software that runs on a computer called a node or peer. Each node is connected to the Blockchain network and might submit and receive transactions. every node collaborating within the Bitcoin network, for instance, has its own copy of the Blockchain, that is synchronic with different nodes employing a peer-to-peer protocol.

ii. Network: Organizations and presumably participants maintain computer systems referred to as nodes, these nodes run Blockchain software to communicate with one other and form a Blockchain network.

iii. Smart Contracts: Transactions or contracts that are converted into code to be executed on a Blockchain are known as scripts or smart contracts.

iv. Submit Transaction: The users submit the transactions to by sending them to nodes on the network, who sends them to all alternative nodes on the network and finally on Blockchain.

v. Transaction Validation: Nodes on the Blockchain network receive, process and cryptographically validate each transaction. The network ignores invalid transactions.

vi. Block: Nodes collect and group valid transactions together into a bundle known as a Block. Blocks should follow a pre-determined set of rules for them to be valid. As an example, they should not exceed a maximum size in bytes, contain more than a maximum number of transactions, and should reference the foremost valid block.

vii. Blockchain: Each new block contains a respect to the foremost recent valid block and is connected to the block. i.e., it's placed afterward block within the database, forming a “chain of blocks”.

viii. Consensus: The process of making sure that every node agrees on the Blockchain.

Block

A block consists of the *block header* and the *block body*.

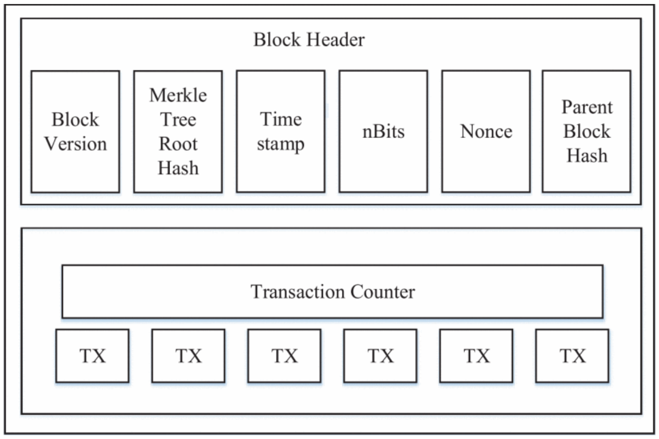


Figure 2-5: Architecture of a block [13]

The block header includes:

1. Block version: indicates which set of block validation rules to follow.

2. Merkle tree root hash: the hash value of all the transactions in the block.

3. Timestamp: current time as seconds in universal time since January 1, 1970.

4. nits: target threshold of a valid block hash.

5. Nonce: a 4-byte field, which usually starts with 0 and increases for every hash calculation

6. Parent block hash: a 256-bit hash value that points to the previous block.

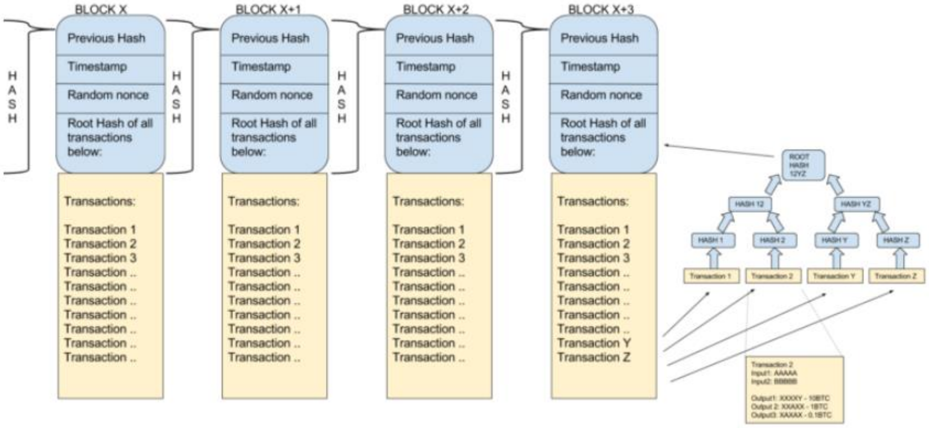


Figure 2-6: Description of a parent block hash [108]

The block body is composed of a transaction counter and transactions. The maximum number of transactions that a block can contain depends on the block size and the size of each transaction. Blockchain uses an asymmetric cryptography mechanism for the purpose of validation and authentication of transactions [13]. Digital signature based on asymmetric cryptography is used in an untrustworthy environment. We next briefly illustrate digital signature.

- **Digital Signature**

  Each user owns a pair of private key and public key. The private key that shall be kept in confidentiality is used to sign the transactions. The typical digital signature is involved with two phases: signing phase and verification phase. For example, a user Alice wants to send another user Bob a message. (1) In the signing phase, Alice encrypts her data with her private key and sends it to Bob. (2) Bob validates the value with Alice's public key in the verification phase. Now Bob could easily check if the data has been tampered. The typical digital signature algorithm used in blockchains is the elliptic curve digital signature algorithm [16].

- **Transaction mechanism**

The transaction mechanism can be described in five key phases [14]:

- *Transaction Definition:* The sender induces the transaction in which the details of the receiver's public key (it consists of the receiver's address) and the value of the transaction is specified. Moreover, this transaction has to be authorized with the sender's cryptographic digital signature, which proves the digital authenticity [13]
- *Transaction Authentication:* Once sent to the network, the transaction is received by the nodes, which authenticate the message validity by decrypting the digital signature. This transaction is waiting in a pool of pending transactions until a block is created [14]
- *Block Creation:* A node of the network takes charge of the transaction by combining it with other pending transactions and creating a block, which is an updated version of the ledger. Once created, a block is broadcasted to the network for validation.
- *Block Validation:* The nodes in charge of validating the block receive the proposed block and they start an interactive process to validate it. However, there might be a divergence among blockchain's branches when the different nodes do not share the same perspective of the entire network state. Therefore, it is necessary to reach a consensus on the block validity among the different nodes based on a validation technique. As previously described, Bitcoin Blockchain is based on a "Proof-of-work" mechanism, while Ethereum is built on "Proof-of-stake". Despite of the consensus mechanism chosen, this phase ensures the validity of every transaction avoiding fraudulent attempts of transaction [12]
- *Block Chaining:* Once every transaction recorded in a block has been accepted, the new block is registered on the being linked to the last block chained in time. The updated chain

is then broadcasted to the network, which accept it as the verified version of blockchain on which future blocks will be recorded. [14]

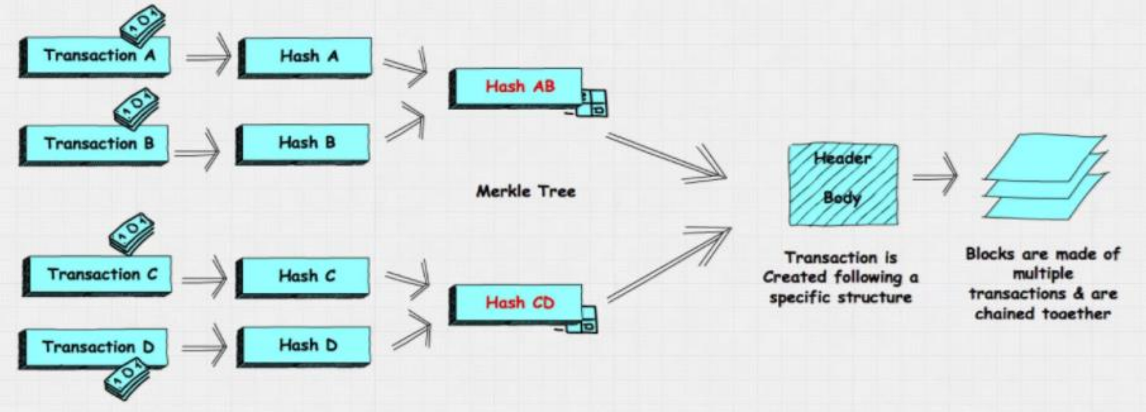

Transaction A
Hash A
Hash AB
Transaction B
Hash B
Merkle Tree
Header
Body
Transaction C
Hash C
Hash CD
Transaction D
Hash D
Transaction is Created following a specific structure
Blocks are made of multiple transactions & are chained together

Figure 2-7: Process of Block-chaining [14]

These technologies are being established for a number of different industries and applications, and as such require a myriad of different specifications. The technologies being developed are aiming to address and solve the scalability and throughput capacity of Blockchains, and ensuring their security, robustness and performance. These areas are presently being self-addressed by a spread of various varieties of distributed ledger technologies with variable degrees of decentralization.

Performance metrices

A Blockchain node processes transactions and stores the current and past state of the entire network. The performance of a Blockchain architecture can be evaluated based on a number of qualitative and quantitative metrics described below:

i. Submission Throughput: The maximum number of transaction possible per second possible by the complete network.

ii. Maximum/Average Validation Throughput: maximum/ average number of transactions/ blocks validated per second possible/ permitted by the network. This parameter determines the maximum/ average transaction processing speed of the network.

iii. Average Transaction Validation Latency: the average length of time it takes for a transaction to be validated from the time of submission. This parameter determines how long on average a user needs to wait for their transaction to be validated and placed in a block.

iv. Latency Volatility: The volatility of transaction validation latency. This is a measure of how varied the transaction processing time could be.

v. Security: System security evaluation requires a threat model that defines the types and scope of adversaries and attacks on the system. Threat models vary across Blockchain applications. A security evaluation may include analysis of:

a. Transaction and block immutability b. Transaction censorship resistance

c. Denial of Service (DoS) resilience d. Trust requirements of users and oracles

e. Protocol governance and node membership services f. Transaction confidentiality and user anonymity.

vi. Confidentiality: Two nodes transacting on a Blockchain may not want other nodes to "know" the contents of the transaction and in some cases may not want other nodes to even "know" their identity as having participated in that transaction.

vii. Transaction fees: In many of the technologies users must pay a small transaction fee to the network in order to process transactions or execute smart contracts. These fees support the upkeep prices of the Blockchain and supply protection from light or malicious procedure tasks like spam transactions or infinite loops in smart contracts.

viii. Hardware requirements: a. Memory/storage: total memory/storage capacity required per node b. Processor: amount of processing resources required to validate transactions and blocks c. Network usage over time, including throughput and latency requirements d. Hardware requirements will change as the network scales.

ix. Scalability a. Number of nodes: system performance change as the number of nodes increases b. Number of transactions: system performance change as the number of transaction submissions per second increases c. Number of users: system performance change as the number of active users submitting transactions increases d. Geographic dispersion: system performance change as the geographic dispersion of nodes increases.

x. Validation process: not a performance metric but an important factor in determining the performance of the network.

xi. Complexity: a measure of the maintenance, development and operation complexity of Blockchain infrastructure.

xii. Smart-contract limitations: There are a number of private and public Blockchain infrastructures provided by various market participants who offer different levels of performance with respect to the metrics discussed above. Some of the key market participants, products, and infrastructures are presented below.

2.3. Applications

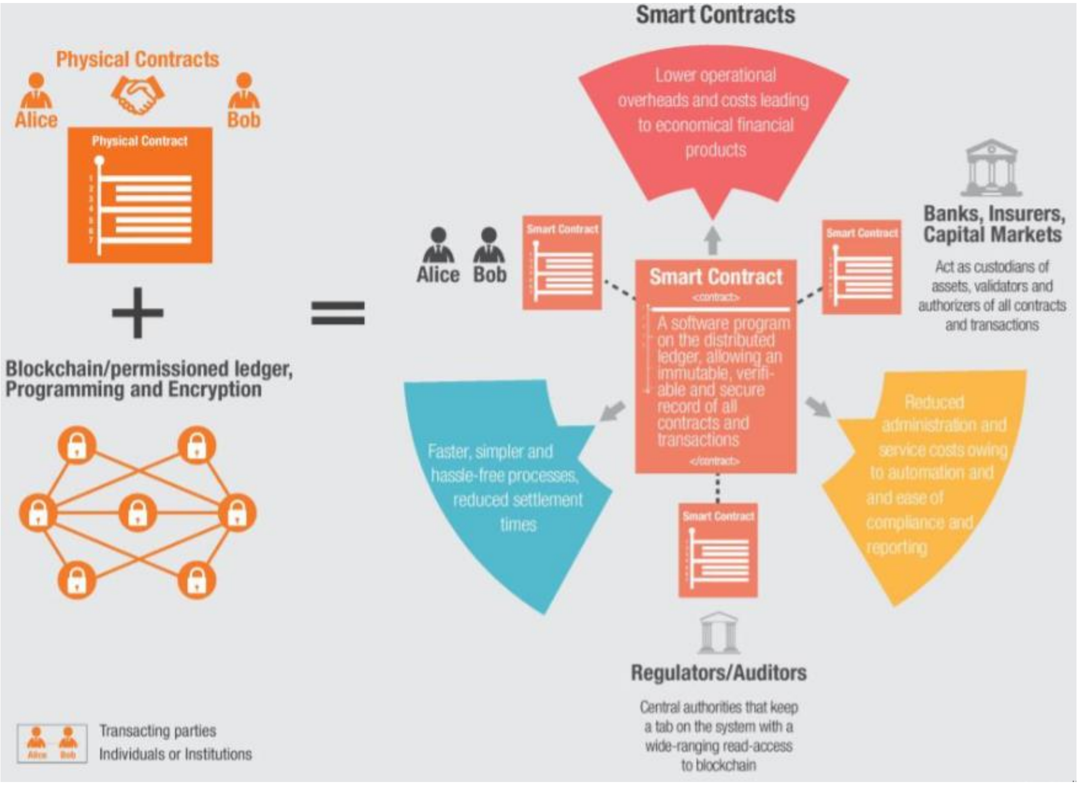
2.3.1 Smart contracts

Contract law has been critical to the formation of sophisticated human societies. Self-enforcing "smart contracts" were proposed by Nick Szabo in 1993, but the communications infrastructure at that time weren't adequate to support them [28]. Ethereum's feature for complex smart contracts gives insurance contracts, financial exchanges and many other kinds of transactions to be accurately defined and executed. Extending contracts to include information and interactions in the physical world are additionally simple to actualize. These include ownership records for real estate, vehicles and automated room rental [29]. A discussion of legal issues is available [30]. Modern corporations are defined by a set of contracts with investors, management, employees, customers, and suppliers. These entities might buy and sell things, make decisions, and hire and fire contractors without human management. It is also possible to create human-run organizations which make decisions by voting on the blockchain [31].

- **Definition**

Smart contracts are self-executing contracts with the terms of the agreement between customer and marketer being directly written into code. The pre-programmed agreement contained in the code exist across a distributed, decentralized blockchain network. Smart contracts allow transactions to be carried out among random parties without the actual need for an external enforcement mechanism. They render transactions, traceable, transparent, and irreversible. Take an example of two Transaction parties headed by Bob and Alice. These two parties are considering of signing a contract which include Regulators and auditors of both the parties, Banks/Insurers of both the parties along with the current Capital market conditions. A smart contract records the Terms of a contract between both the parties and share it on a distributed ledger between all participants. It makes a connection and serves as a platform for Bank's internal systems (Oracle services) and external world (account balance, prices). The smart contract waits for external triggers to evaluate pre-defined conditions and rules hence making Data available for the Auditors and Regulators for compliance and reporting. Upon fulfilment of all the conditions the contract self-executes via triggers resulting in completion of the process [32].

Smart contracts in blockchains are typically programmed in a step wise procedure. Solidity is one procedural language in which these contracts can be coded [33,34]. In this language, the programmer writes a particular sequence of steps that are performed to produce what must be done. [35].



Physical Contracts
Alice
Bob
Physical Contract
+
Blockchain/permissioned ledger, Programming and Encryption
=
Smart Contracts
Lower operational overheads and costs leading to economical financial products
Alice
Bob
Smart Contract
Smart Contract
<contract>
A software program on the distributed ledger, allowing an immutable, verifiable and secure record of all contracts and transactions
</contract>
Smart Contract
Banks, Insurers, Capital Markets
Act as custodians of assets, validators and authorizers of all contracts and transactions
Faster, simpler and hassle-free processes, reduced settlement times
Reduced administration and service costs owing to automation and and ease of compliance and reporting
Smart Contract
Regulators/Auditors
Central authorities that keep a tab on the system with a wide-ranging read-access to blockchain
Alice Bob
Transacting parties
Individuals or Institutions

Figure 2-8: Smart contracts [35]

- **Smart contract licensing**

Smart contracts have the capability of disrupting the way licensing is presently done all Supply chains and has the potential to revolutionize the software industry. For example, using smart contracts the mass distribution of software products under a smart license from the developer can be monitored. Upon expiry, the software product stops working based on the terms of the smart contract and the users renew their software license by purchasing tokens on the blockchain network. Other users who are no longer interested in using some software could also re-sell their license on such distributed networks [36]. A micropayment system permits Supply chain members to be share digital copies of their content by the piece. In other words, this personally grants participants the license to use the content (they want to share via Blockchain platform) in a 'smart' way.

- **Smart contract types**

Blockchain networks like Ethereum and Bitcoin have input and output limitations due to their security constraints that limit access to external data (e.g., price, weather, location, etc.) which are needed for contractual performance and forms of payment preferred by parties involved in these contracts. Because of this, trusted links to external data sources are required for some smart contracts to be executed. Thus, smart contract can be further divided into deterministic and non-deterministic smart contracts [37,38].

	Deterministic Smart Contracts	**Non-Deterministic Smart Contracts**
	• For an effective working, these contract codes do not require any outer information other than the	• For an effective working, these contract codes require some external state (Oracle

Working	public information provided on the Blockchain platform. • There can be 0 or more state transitions for every input that can be internal or external. There is always more than one path for the decision- making process to follow for every transaction and prediction.	etc.) during the process since the network responsible for facilitating the smart code does not include sufficient information to make decisions. • There’s exactly one state transition for every external input ie. no decision, prediction or transition can be made after that outer intervention. For the decision-making process to go further, a new input is needed at every stage.
Example	• Peer-to-peer lottery: the funds are held on the blockchain network and random numbers are also generated by the smart contract code. In the end, the funds are transferred the winners	• Value flow-based decisions on human behavior, events (price drop or hike) or predictions [38].

	account via his or her address on the blockchain network [37].	

Table 3-1: Comparison between Deterministic and non-deterministic smart contracts

2.3.2 Smart contracts for Supply chains

According to Matt Levine at Bloomberg [43], the best opportunity for smart contracts is embedded in business organizations. The capability of the blockchain to eliminate the need for trust will allow people to stop working for aged style organizations, instead everyone will be an entity in a commercial system operating on the blockchain. The functions of a company's leaders and board can be reduced to smart contracts implemented in computer programs. Investors can make decisions over e-voting and such a decentralized organization will be exempt from external influence because it will operate just the way it has been programmed to. The old way was that a group of individuals came together to set up an organization for commercial purpose, another group brought the investment to run it, others ran the business and others worked for it and decisions on how to share the benefits or profit at the end of the day were difficult to make [43]. The new way is that a group of individuals put their money into a company organized with smart contracts without any difficult decisions to make in the future apart from how and whether to retrieve their money if a hacker steals it. Research has shown that people agree with the premise that the smart contract approach is better than the previous approach which requires human activity [43]. The biggest challenge facing the potentials of smart contracts in organizations is likely the human element [44].

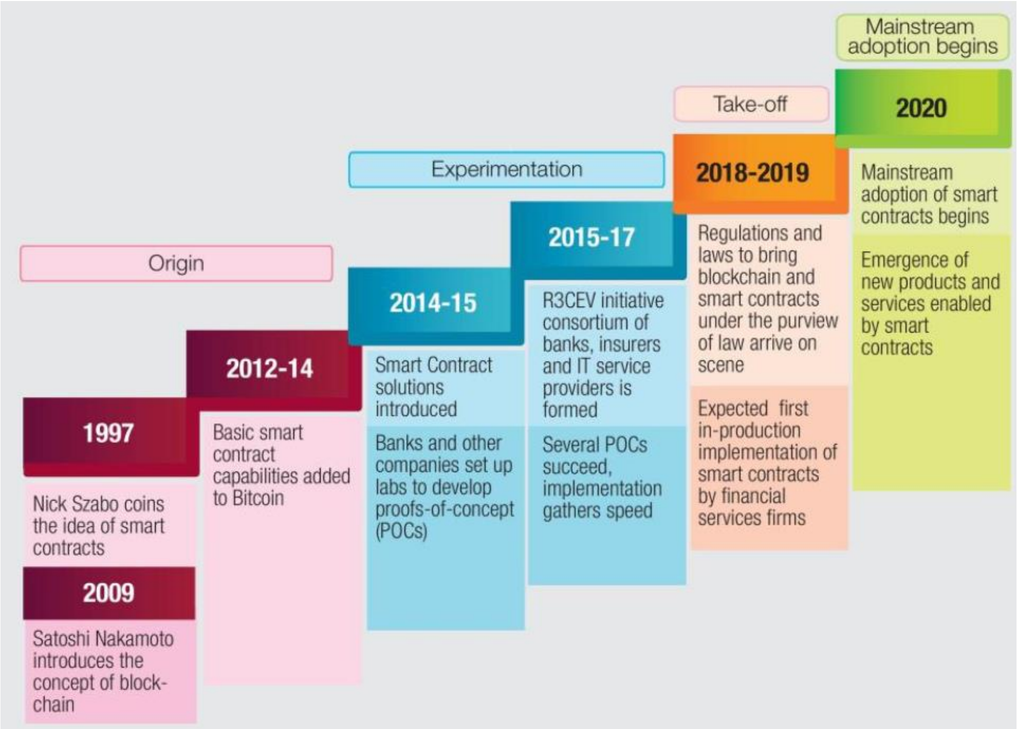

Mainstream adoption begins
Take-off
Experimentation
Origin
2020
Mainstream adoption of smart contracts begins
Emergence of new products and services enabled by smart contracts
2018-2019
Regulations and laws to bring blockchain and smart contracts under the purview of law arrive on scene
Expected first in-production implementation of smart contracts by financial services firms
2015-17
R3CEV initiative consortium of banks, insurers and IT service providers is formed
Several POCs succeed, implementation gathers speed
2014-15
Smart Contract solutions introduced
Banks and other companies set up labs to develop proofs-of-concept (POCs)
2012-14
Basic smart contract capabilities added to Bitcoin
1997
Nick Szabo coins the idea of smart contracts
2009
Satoshi Nakamoto introduces the concept of block-chain

Figure 2-9: Origin to Mainstream adoption of Smart contracts [43]

Individuals like their freedom, and the blockchain must find a way to detach them from organizational hierarchies and not making them subject to a new leader; the blockchain itself. However, smart contract should not be underrated. Some ideas for using smart contracts are amazing. Toyota Financial services has played with the idea of connecting blockchain smart contracts to cars such that if people miss their car finance payments, the car will not turn on and the ownership of the car can be reassigned to a new owner. But people would rather use this option to finance their car because they will get a better deal at a cheaper rate without the need a bank or for an investor acting as a middleman [44], they will pay directly to Toyota and this will reduce finance interests. Smart contracts act in real time and reduce the chance of human error and cases of fraud prone processes, increase privacy and trustworthiness. These are no doubt features of smart contracts that can be added on top of existing business processes for improved efficiency. A company based in San Francisco called SmartContract [45] has developed technology capable of connecting smart contracts to external data feeds, internal infrastructure and external payments.

- **Organizational benefits**

Smart contracts decentralize a centralized or federated service to improve transparency, reduce the need for trust and sometimes gain economic efficiency because you no longer must pay a central arbitrator to do a particular task. Having a central party governing contracts poses so many risks, such as; data privacy, reliability, trust, monopoly, expensive, privacy, and authenticity [39]. Some of the benefits of smart contracts are listed below:

i. Anonymity: participants can be completely anonymous but transfer of value from one party to another is guaranteed. In a commerce scenario, because the system ensures that the buying party can pay, the seller does not need to know the identity of the person buying. The smart contract ensures that the funds reach the account of the seller upon fulfilling a pre-agreed condition. This ensures that peoples credit card information is protected and cannot be stolen or used for fraud [30].

ii. Value can only be spent or transferred the way parties intended.

iii. Self-enforceable. Smart contracts can automatically execute the contract, e.g., allocate resources autonomously regardless of trust between parties. There is no need to trust third parties such as escrow services or credit card companies [40].

iv. The cost of changing the rules is extremely low. Computer code can 'easily' be re-written depending on programmer's experience.

v. Immutability: objects cannot be changed [41].

vi. Permanence: objects are permanent and stored on a blockchain (history of linkable and traceable transactions) [42].

vii. None of the communication or transactional anonymity developed for blockchain platforms must be sacrificed to use smart contracts. For example, anonymous voting system or lottery system.

viii. Atomicity: because of the mining concept of the blockchain where each node in the network is rewarded for carrying out a transaction, an entire operation runs, or nothing does [37].

ix. Synchrony: no two operations can interfere with each other.

x. Immortality: According to Hoskinson, objects can never be deleted, unless they are removed by mutual consent of all the participants [37].

- **Challenges in Implementation**

Despite the enormous potentials of smart contracts, several challenges that need to be addressed still lie in the pipeline. For smart contracts to be 'complete' to a large extent, authors have highlighted some of these challenges and some have also gone further to advocate possible solutions. These challenges are discussed as follows:

i. **Technological challenges:** The main necessity for smart contract code is that the code should execute successfully and accurately to completion, within a reasonable time. During the processing time of this code there can be scalability in speed of execution of the program. In real-world situations, the initial agreement is usually not the final say. Agreements are sometimes negotiated if possible and modified to cater for unforeseen circumstances that were difficult to predict at the beginning. The self-enforcement characteristic of pre-written logic (smart contracts) means that the current smart contracts in distribution are not flexible to changes in the real world.

ii. **Legal challenges:** Legal authorities think smart contracts to be marginally improved legal agreements, without any appreciating the fuller potential of smart contract code to extend beyond law's reach. On the other hand, developers consider smart contracts and see the limitless possibilities of software, without appreciating the subtleties and commercial realities reflected in traditional legal agreements. As with any interdisciplinary field, both must learn from the other [46].

Other challenges include: Organizational challenges (hardware & software, governance of decision making process and code generation), Privacy, security and Inflexibility of the Smart contracts.

- **Recommendations of Adoption of Smart contracts**

1. The first step in designing smart contracts is to understand the problems being solved by any existing paper contracts or legal documents. If a smart contract is to replace the paper contract, then it should be able to solve all the problems or provide benefits to parties that exceed the costs of not solving all the problems.
2. The second step would be to develop smart contracts that preserve some of the abilities of traditional paper contracts. For example, implementing the ability for parties to renegotiate at any point in time in cases whereby the parties increase or decrease or want to reveal their identities. The replacement of one smart contract with another should also not pose any difficulties. This also applies to the use of smart contract templates—the smart contract should be easily editable to provide some flexibility for reuse [46].
3. Finally, the people aiming to implement smart contracts should also give serious consideration to what happens in those circumstances where renegotiation is convenient, but the parties cannot reach an agreement. There are examples of appealing to the relevant

> community for a decision in the paper world, but it is relatively rare. The problem with these types of approaches is that participants in the decision may make a decision based on their own personal interests. What the parties to most contracts are looking for, however, is to place jurisdiction over the contracts in a place where the parties have confidence that their case will be fairly determined by a disinterested court applying well-developed legal standards [40, 47].

Therefore, smart contracts can have an optimistic future but face some problems that must be addressed beforehand, such as dealing with the potential for coding errors. However, to reach their potential fully, smart contracts are going to have to be flexible and adaptable to real life situations because in the real world the initial contract or agreement is not always the final say [40, 47].

2.3.3 Internet of Things (IOT)

The Internet of Things (IoT) is the "network of interconnected sensor-equipped electronic devices that collect data, communicate with each other, and can be monitored or controlled remotely over the Internet" [48]. The main objective of the IoT's is to make a connection between the physical world and the Internet or to wireless networks and allow making objects, machines and work environments interactive. By using sensors, objects will be capable of exchanging data with other machines without the need of human intervention [49]. The IoT is not an anticipation but a plausible trend that is moving forward, rapidly. It is estimated that by 2020, 50 billion devices around the world are anticipated to be connected to the Internet. One third of these devices will be computers and smartphones and remaining will be sensors and newly invented intelligent devices [50,53,54].

IoT is turning into a rising Internet-based industrial data design that's used to facilitate data flows among supply chain networks across the world. The importance of IoT lies in streamlining supply chain operations, providing real time data, and in pursuit of business processes at numerous stages. Several new opportunities in applying IoT to produce efficient supply management are out there these days or may be foretold in close to future. [55,56,57].

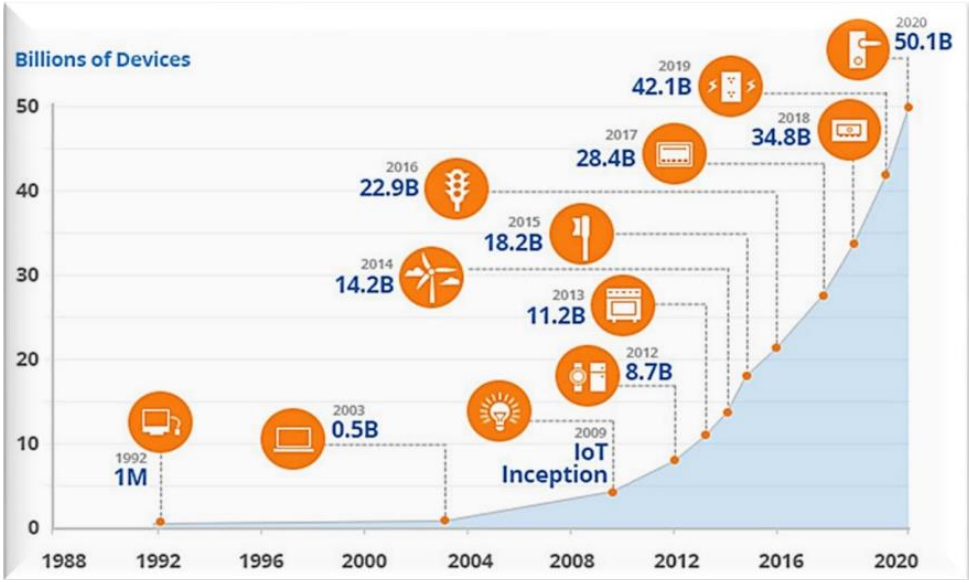


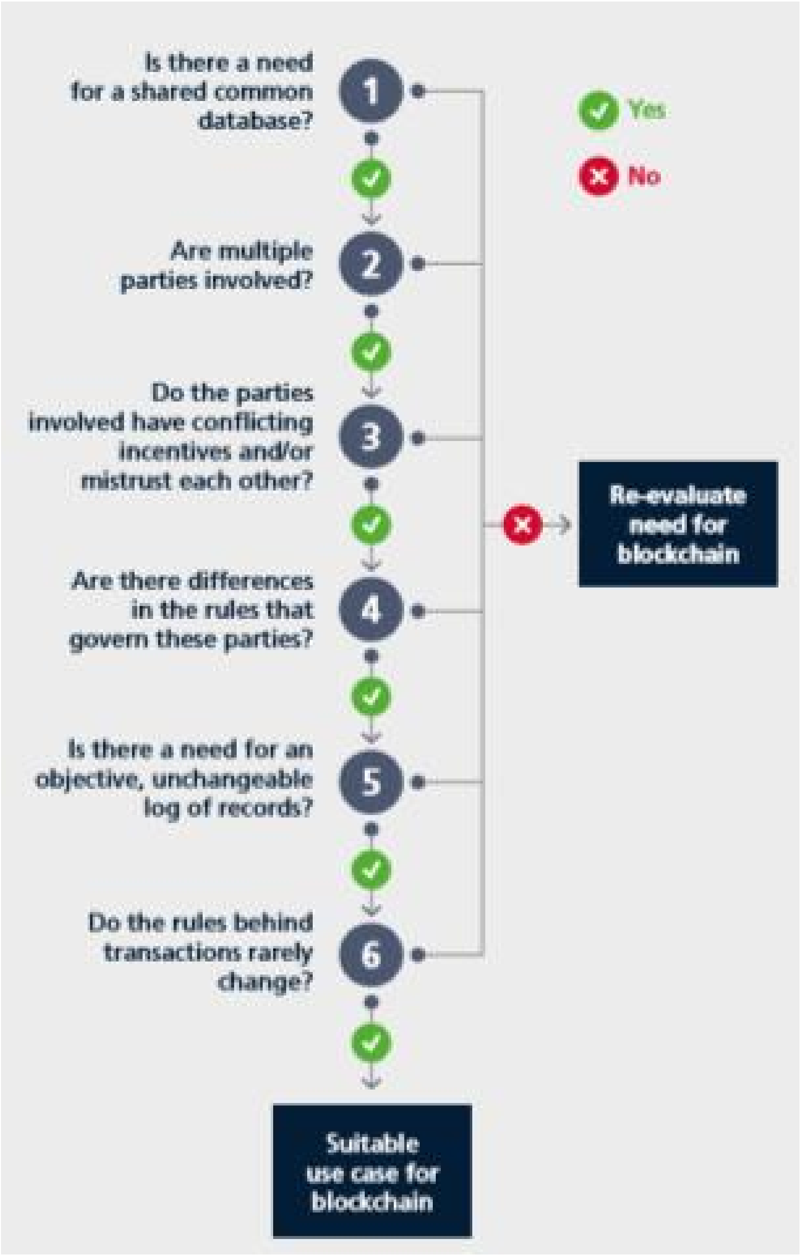
Figure 2-10: Growth of Internet of Things [58]

By the 2020 around 50 to 100 billion things will be connected electronically by internet [59]. The above figure shows the growth of the things connected to the internet from 1988 to forecast 2020. The Internet of Things (IoT) will provide a technology to creating the means of smart action for machines to communicate with one another and with many different types of information [60]. The success of IoT depends on standardization, that provides ability, compatibility, dependability, and effective operations on a world scale [61]. Nowadays many firms are operating with standards, like IETF, IEEE and ITU to specify new scientific discipline primarily based technologies for the web of Things [62]. The planning of the IoT standards is needed to contemplate the economical use of energy and network capability, furthermore as respecting different constraints like frequency bands and power levels for frequency communications [63,64]. As IoT evolves, it should be necessary to review such constraints and investigate ways that to make sure enough capability for growth, for instance just in case of extra spectrum allocation because it becomes obtainable [65].

Internet of things promises many applications to make life easier, smart and safe. There are many applications such as smart cities, homes, transportation, energy and smart environment. Internet of things faces two major challenges to guarantee efficient network access: the first issue is the fact that today different networks coexist, the second issue is related to the big data size of the IoT.

2.4 Getting Started with Blockchain

Once a corporation understands and acknowledges the potential of blockchain technology to drive potency and worth, consequent step is to determine a roadmap for application. this could begin from a mindset to collaborate and involve building blockchain data and capabilities with target driving worth for all stakeholders.


Is there a need for a shared common database?
1
Yes
No
Are multiple parties involved?
2
Do the parties involved have conflicting incentives and/or mistrust each other?
3
Re-evaluate need for blockchain
Are there differences in the rules that govern these parties?
4
Is there a need for an objective, unchangeable log of records?
5
Do the rules behind transactions rarely change?
6
Suitable use case for blockchain

..

Figure 2-11: Simplified decision tree for identifying blockchain use cases [58]

- **Create a culture of collaboration**

When an institution accepts the idea of blockchain technology, it is signing up for an intensely collaborative journey because a huge portion of this journey includes facilitating trusted collaboration between different parties including both public and private entities of all kinds. These can be government agencies, industrial organizations and even competitors.

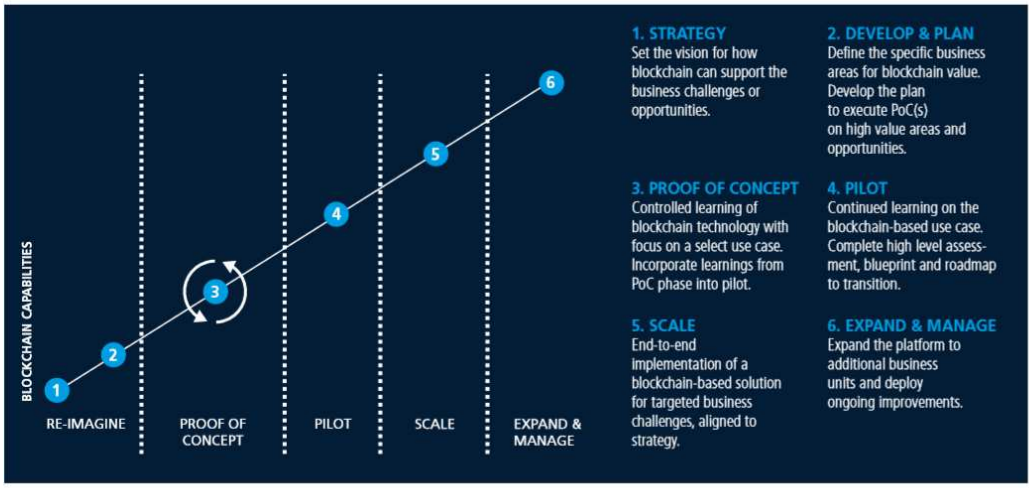
Collaboration platforms have been created for competitors in highly competitive financial services industry, to work together researching the application of blockchain technology. More value is created for each participating organization when more parties agree to use a single blockchain solution.

- **Build up blockchain knowledge and capabilities**

Knowledge and capabilities change organizations to spot and notice the worth of recent operative models. So, it is essential to supply empowering partner organizations and individual contributors with the time, tools, and resources they have to with success contribute to every blockchain project. These contributors should be ready to negotiate effectively among the blockchain system and with relevant technology players, implementation partners and associations.

- **Focus on value and engage with stakeholders on blockchain opportunities**

Realizing the complete worth of this technology depends on collaboration with the complete neutral scheme, and participants should be prepared for this. When distinguishing promising blockchain use cases, firms ought to scrutinize every plan to ascertain its dependency on blockchain technology. The design-and-plan part builds toward a image for the proof of construct. throughout the proof-of-concept part, stakeholders ought to learn all the nuances of mistreatment blockchain technology within the planned application. within the pilot part, stakeholders ought to check the appliance on low scale whereas finishing a high-level assessment of roll out at scale. it's imperative to incorporate all stakeholders during this pilot part, therefore this step involves a shift of perspective – from achieving success with an inside answer to currently onboarding multiple parties and testing the answer across a network. The final stage in an exceedingly blockchain implementation involves scaling the answer and realizing comprehensive edges. this needs a big transformation of business processes across not simply internal parties however additionally multiple stakeholders, as well as business partners and even competitors. Therefore, answer success depends heavily on neutral uptake and acceptance. The success of the project hinges on everybody adjusting their business practices and full investing the blockchain implementation. Neutral participation is arguably the foremost crucial success step about blockchain adoption.



1. STRATEGY
Set the vision for how blockchain can support the business challenges or opportunities.

2. DEVELOP & PLAN
Define the specific business areas for blockchain value. Develop the plan to execute PoC(s) on high value areas and opportunities.

3. PROOF OF CONCEPT
Controlled learning of blockchain technology with focus on a select use case. Incorporate learnings from PoC phase into pilot.

4. PILOT
Continued learning on the blockchain-based use case. Complete high level assessment, blueprint and roadmap to transition.

5. SCALE
End-to-end implementation of a blockchain-based solution for targeted business challenges, aligned to strategy.

6. EXPAND & MANAGE
Expand the platform to additional business units and deploy ongoing improvements.

Figure 2-12: The steps for a blockchain implementation [58]

2.5 Blockchain in Education

The blockchain technology is proposed as a disruptive technology that has the ability to transform the finance and commerce sectors. But for its relevance in education, it is imperative to understand its features before adapting it for educational use. The best known, but not the only, blockchain is the one at the heart of the Bitcoin system of digital money [93,94]. There is the 'distributed consensus' method to check if a new block is legitimate and whether or not should it be added to the chain. Each block in the blockchain can hold a small amount of data (typically up to 1 Mb) which could be any information that is required to be kept secure yet distributed. These records of currency transactions can be exam credentials or records of learning. This information is recorded for all participants and can be viewed by anyone possessing the cryptographic 'public key' but cannot be modified, even by the original author. The data records are timestamped, providing a trusted and timed record of the added data [95].

- **Education market Analysis:**

  The global market for education is $4.4 trillion and is anticipated to grow on a regular basis. A survey in 2015 showed that in countries like China, India and Malaysia this industry is grows around 50% every year. Three of the best universities in the world: Harvard, Yale and Stanford account for around $70 billion with an average tuition of an undergraduate $45,000and average salary of the professor $200,000. Top 100 universities in the world have a total of around $433 billion endowment in 2015 [96].

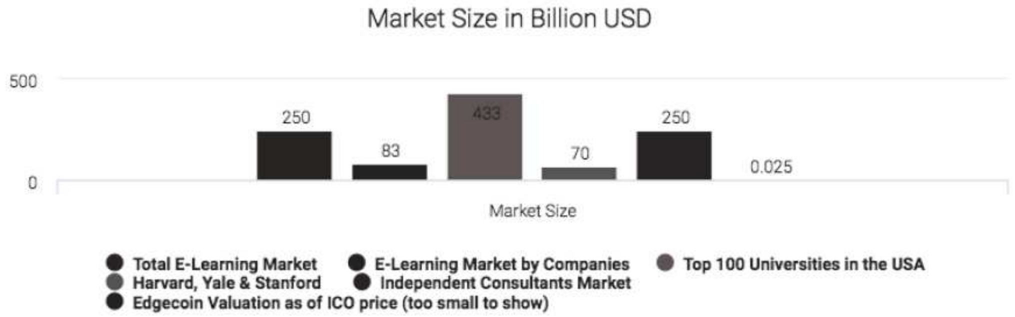


Figure 2-13: Education market [96]

- **Problems in Education Systems:**

  i. **Non-immutable record keeping-** Since there is no standard guideline accepted by all the companies, countries and institutions, verification of services and validation of skills remain to be a big issue. Finishing a course gives a certificate but does not provide with the skills achieved and hence there is a huge gap in workforce.

  ii. **Poor data protection and security-** Current technical infrastructures and software systems used in the education sector lack the adequate data protection and security. Data can be easy stolen, and fraud is very hard to prevent with the current way of issuing and storing certificates. This results in fines and security violations related to data protection laws and regulations. This results in a big risk for not only the universities but also for the companies looking for potential employees.

  iii. **Data storage-** Data storage is an increasing problem faced by the universities today. As more and more students enroll in the universities, it will eventually become impossible to store a paper database of the certificates up to date.

  iv. **Inefficient degree transfer process-** Growth in admissions and complexity of degree programs makes it harder to maintain and stores certificates and transcripts. Creating such certificates on paper is also a long and insufficient process. Graduates seeking copies of their certificates have to wait for months due to the presence of many middlemen like translators, official authentication etc.

- **Blockchain Solutions:**

i. **Cost efficiency-** The average price of issuing and verifying diplomas in traditional way is around 50 USD per student. By implementing blockchain services, universities will cut their costs down to 10 USD thus resulting in 80% saving [115].

ii. **Fraud protection-** Blockchains not only protects the front-end design of certificates but also makes them immutable while validating them. This results in their protection against fraud, loss or damage. With specifying the fingerprint of certificates like font size, signatures and other features, unique documents can be created.

iii. **Time saving-** By using blockchain technology as a decentralized service, a paper-free and thus environment friendly validation process can be created in a matter of seconds thus being dramatically faster than current processes which take weeks and sometimes months.

iv. **Indestructible certificates-** All the blockchain data is unalterable and is therefore indestructible.

2.6 Research Gap

The cited research papers provide an insightful background and technical concepts of Blockchain and blockchain-based systems. There are a numerous other research papers that focus on the simulation aspects of various distributed systems. The review of these papers points out a research gap in these studies especially in the analysis of a blockchain based education system. These analyses have been done in the field of commerce, jurisdiction and health-care but education systems have not gained much attention. The three main research gaps found in the existing literature and addressed in this work are:

- Most of the research papers execute mathematical modelling of Bitcoin and blockchain by considering only the traditional equations like: Metcalf's law and Gresham's law and a limited research is done by considering the Trust function.
- Secondly, most of the literature focuses on the technical characteristics while performing mathematical modelling and not on the other parameters like cost and time analysis and the behavioural aspect of such a system if it is subjected to attack.
- Further, there is no simulation work done to construct a model of working of a Blockchain-based education system.

This paper takes a step ahead by considering these three research gaps as following:

- While performing mathematical modelling, the most important aspect of any distributed ledger system: trust was taken into consideration. This is done to increase the security of such a system and avoiding attack.
- To address the second research gap, along with technical characteristics, other parameters of the system are also modelled which are cost, time and system behaviour under attack.
- Finally, a preferential network system is modelled for the blockchain based education system.

Chapter 3:

Methodology and Model Design

3.1 Simulation Objective

The main objectives of this simulation are:

- To generate a model that shows the basic working of a blockchain-based Education system
- Reduce time and cost factors for verifying student's credit records.
- Avoid possible Sybill and 51% attack on the Blockchain network.

A proof of concept model was developed to demonstrate how an Education Institute focused blockchain in a hypothetical system involving three agent groups – Administration, Professor and student. All participants in the system can access relevant data in a distributed manner by utilizing a hypothetical blockchain, with a native cryptocurrency – tokens. The model was built using Netlogo modeling software, which uses the Java programming language. The model includes a cryptographic peer-to-peer ledger with a very basic mining algorithm put into place to maintain consensus. Each participant has its own public identifier (known as a public key), a copy of the blockchain data, and a set of local records. Transactions can migrate between states of being initiated, in memory pool, shared and added on blockchain, verified and validated and finally been added to a new block. This design reduces the amount of data stored in the public blockchain, since it only includes the dynamic location of records, rather than the full record. The model also implements functionality allowing any participant to compile a verifiable complete history of any other participant of interest's records by only using the participant of interest's public key. The model concretely demonstrates the auditability, availability, universality and reconciliation of these student records distributed throughout the blockchain network. Such a system may also reduce fraud, reduce costs, incentivize student engagement and improve the overall system. The proposed architecture is simulated and empirically scored based on the technical features, operational capabilities, and requirements discussed earlier. These scores can be used to facilitate future research as to the optimal architecture of a blockchain-based Educational system.

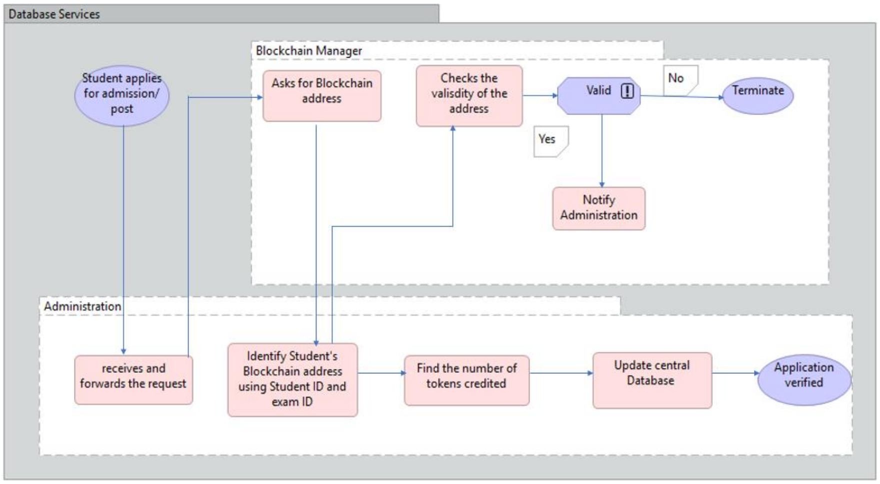

Database Services
Blockchain Manager
Student applies for admission/ post
Asks for Blockchain address
Checks the valisdity of the address
Valid
No
Terminate
Yes
Notify Administration
Administration
receives and forwards the request
Identify Student's Blockchain address using Student ID and exam ID
Find the number of tokens credited
Update central Database
Application verified

Figure 3-1: The flow control of the model for application verification

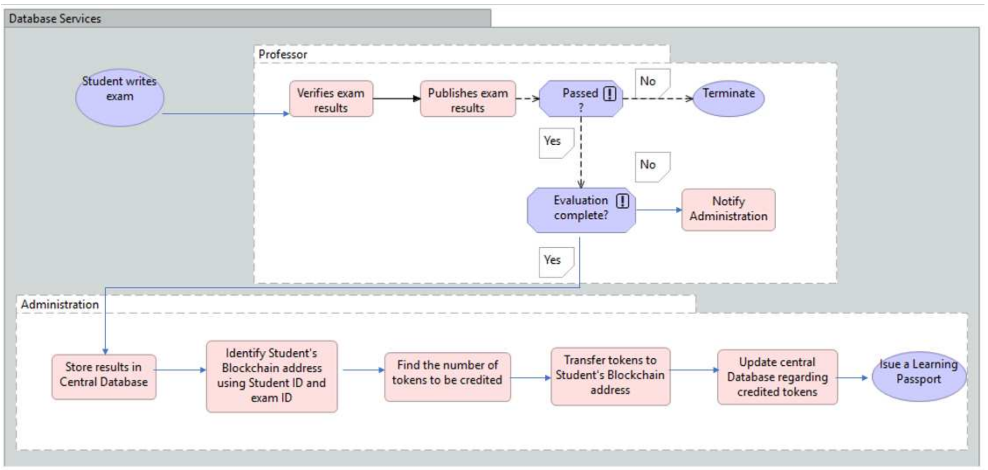

Database Services
Professor
Student writes exam
Verifies exam results
Publishes exam results
Passed ?
No
Terminate
Yes
No
Evaluation complete?
Notify Administration
Yes
Administration
Store results in Central Database
Identify Student's Blockchain address using Student ID and exam ID
Find the number of tokens to be credited
Transfer tokens to Student's Blockchain address
Update central Database regarding credited tokens
Isue a Learning Passport

Figure 3-2: The flow control of the model for issuing a learning passport

The professor verifies the results and publishes them after a student takes an exam. The results are stored in the central database only when professor is able to individually register completion of student's course obligations. If not, the administration office is notified to perform the procedure needed for student’s obligations. The results can be simultaneously stored in the centralized database of the Educational institute and the blockchain system. The administration office along with professor’s consent asks the Blockchain manager to find the student's blockchain address in the central database and find the amount tokens the course has set to transfer to his blockchain address. The transaction is processed through the blockchain network. When the transaction is confirmed, the administration office and the professor are informed so as to record the successful transfer into the central database.

3.2 Mathematical Modelling

3.2.1 Modelling of distributed network

The network is made by using the Barabasi-Albert algorithm [24]: a first number of initial nodes is set, and they are fully connected. Then the number of links per iteration (L) is fixed. At each iteration of the algorithm a new node is created and is connected to L already existing nodes. This process is repeated until the network reaches the desired dimension. In this way a scale-free network is created. Therefore, we will notice that the distribution of degrees of nodes follows a power law, instead of a Poisson distribution as in a random network. This means that our network will have a lot of nodes with a low degree and very few nodes with a high degree. It is a feature of large networks to be scale-free [21]. This means that for large k we will have a power law distribution of degrees. It is observed that random graphs can't reproduce this property, as the distribution results in a Poisson one. It is crucial to underline that a random network assumes that the probability of linking two nodes is independent of the nodes degree, in fact the attribute random means that the probability of creating a link between two nodes is uniformly distributed between 0 and 1.

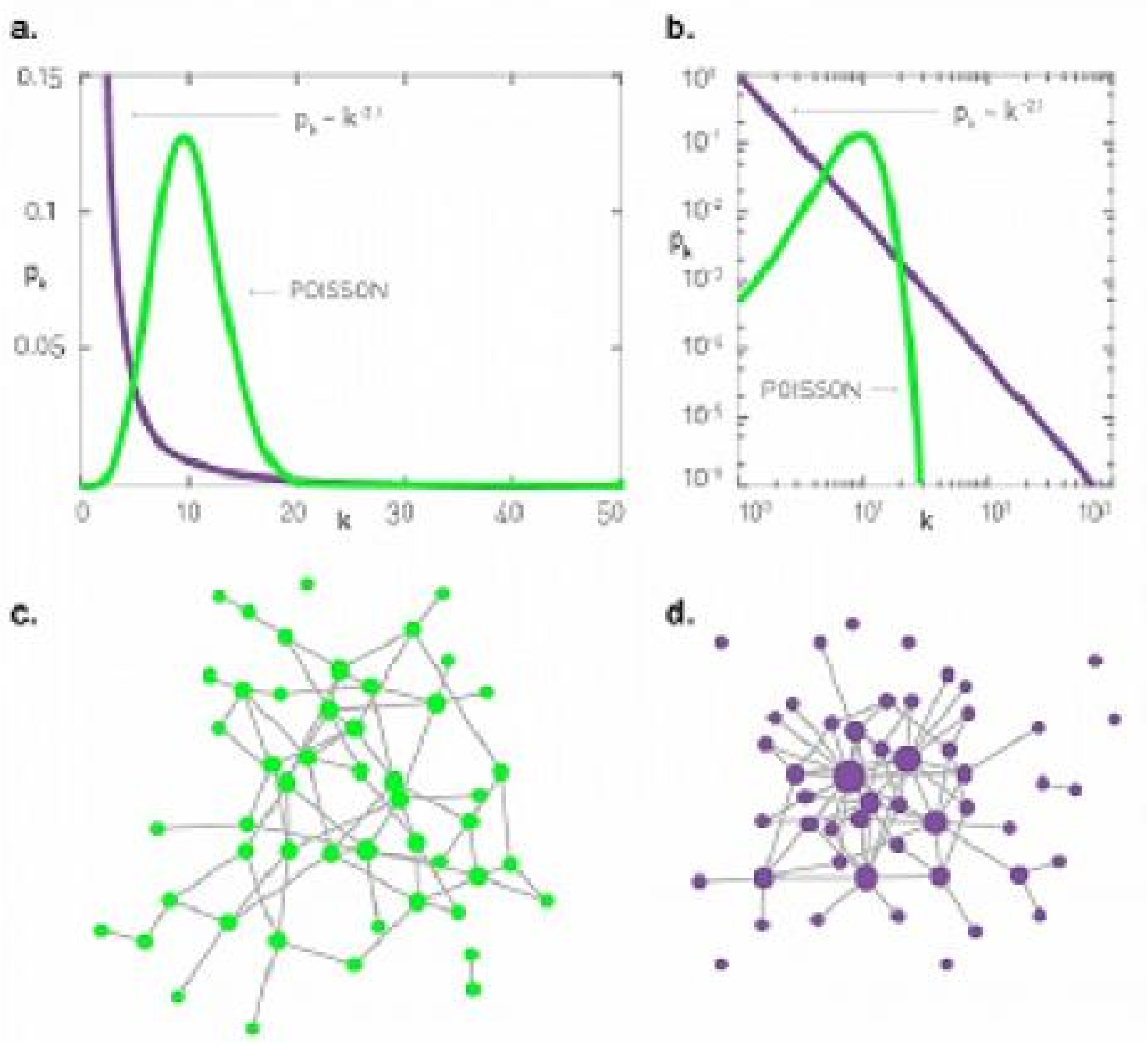


Figure 3-3: Random network versus Barabasi-Albert network distribution of degrees. Source: Albert-Laszlo Barabasi. Network science, chapter 4.

There is a limit in the quantity of tokens that can be mined according to Gresham Law. The probability that a new node will connect to an old node *n* is given by the following:

$$\pi(k)^\wedge n = k/(\sum\_j.k) \qquad (2.1)$$

Numerical simulations show that a network generated with this method evolves into a power law distributed with exponent ŷ= 3. [91] The only two parameters of the model are the initial number of nodes N and the number of links created at each time step. At every time step there is a probability $\pi(k)^\wedge n$ that a new node will link to the node *n.* Therefore, the working equation becomes:

$$(\partial(k)^\wedge n)/\partial t \ = L\pi(k)^\wedge n \qquad (2.2)$$

where L is the number of links and *t* is the time-step function. By assuming that the nodes are added to the network at equal time intervals, the t_i have a constant probability density given by:

$$\mathrm{P(ti\,)} = \ 1/(N+t) \qquad (2.3)$$

where N is the number of nodes at time t = 0. Now the Probability distribution P(k) of the degrees can be represented as:

$$\mathrm{P(k)} = \ (\partial \mathrm{P(k(t) < k)}\ )/\partial k \qquad (2.4)$$

taking the limit t to ∞ we get:

$$\mathrm{P(k)} \sim 1/\beta\, L^\wedge(1/\beta)\, k^\wedge(-\hat{y}) \qquad (2.5)$$

Where ŷ = $1/\beta + 1$, following Power law and putting β= ½ we get ŷ = 2+1 = 3. The resulting number of nodes is independent from L which means the network thus formed is not centralized and does not depend on a single authoritative node hence formation of a de-centralized and distributed network [109].

3.2.2 Modelling of Blockchain and Trust function

Blockchain is a Block of certificates and each block contains a reference to the previous block. It can also be referred to as the ledger of certificates. To understand the mathematics behind this composition, refer to the equations below:

Block = Merkle tree of certificates + header(block)

Header (Block) = Merkle root + Hash (previous block-header) + (date or time)

To create a series of Blocks it is essential to recognize and connect to the official blockchain. The difficulty associated with this process of connecting a block B_i to the Blockchain such that $(B_i)_{0\leq i\leq N}$ can be written as $\sum_{i=0}^{N} D_i$.

Due to this composition it is very easy to check whether the certificate in question belongs to the ledger. If any modifications or changes are made to the ledger, it is automatically detected. The Merkle tree of certificates is basically the tree of hashes where each leaf is considered to be a hash (block) and top hash is the Merkle root [101]. The next step in the creation of Blockchain is to establish that a document was created after a given moment in time. Hence, it is necessary to report events that could not have been predicted before they happened. To establish that a document was created before a given moment in time, it is necessary to cause an event based on the document, which can be observed by others.

Let *D* be a document such that Certificate (*D*: = Hash(*D*); to sequence the appearing of documents along with time each certificate includes hash of the present document and the previous certificate. Thus, the certificates can be timestamped as shown below [102]:

$$\text{Certificate}(D'): = \text{Hash}(D'|\text{Certificate}(D))$$

The transaction of every certificate creation includes the signing script and the public key script. In this thesis, an attempt is made to replace the traditional signing script with a Multi-signature script so that whenever a transaction is made, more than one signatures will be required for the signing process. To model trust in the blockchain network an introduction of gamma functions is made. Let $0 < \mathrm{q} < \frac{1}{2}$ where q is the relative hash power of the group of attackers. Hence the representation of honest miners can be made as p = 1-q. After z blocks have been validated by the honest miners, the probability of success of the attackers is

$$\mathrm{P(z)} = I_{4pq}(\mathrm{z},\tfrac{1}{2}) \qquad (2.6)$$

$$I_x\ (a,b) : = \frac{\Delta(a+b)}{\Delta(a)\Delta(b)} \int_0^x t^{a-1}\,(1-\mathrm{t})^{b-1}\mathrm{dt} \qquad (2.7)$$

where $I_x\ (a,b)$ is the regularized incomplete beta function and t is the trust function, by assuming s= 4pq<1 z and tends to infinity the probability of success of the attackers become:

$$P\ (z) \approx \frac{s^z}{\sqrt{\pi(1-\mathrm{z})\mathrm{s}}} \qquad (2.8)$$

Looking for *y* such that *F*(*xjy*)<Target

*x*1=Version

$x2$=hash Previous Block

$x3$=hash Merkle Root

$x4$=Timestamp

$x5$=Target

Block Header =*xjy*.

The time it takes to mine a block is memoryless

P[$T > t1+t2 \mid T > t2$] = P[$T > t1$]

The random variable T has the exponential distribution with parameter $\alpha = \frac{1}{600}$

$$f_T(\mathrm{t}) = \alpha e^{-\alpha t}$$

where α is the mining speed, E[T]= $\frac{1}{\alpha}$

Inter-block times T1*,....* T_n are independent identically distributed exponential random variables.

The sum

$$s_n = T1 + \ldots T_n \text{ is the time spent to get } n \text{ blocks}$$

The random variable S*n has a Gamma distribution with parameter* (*n, α*)*:*

$$f_{Sn}\ (t) = \frac{(\alpha\ )^n}{(n-1)!} t^{n-1} e^{-\alpha t} \qquad (2.9)$$

Let N (*t*) *be the number of blocks already mined at t-time. Start is at t*=0*. The random process N is a Poisson process with parameter α i.e.*

$$\mathrm{P}[\mathrm{N}(t)=k] = \frac{(\alpha\ t)^k}{k!} e^{-\alpha t} \qquad (2.10)$$

The letters T;s_n *N (resp. T 0; 0;* s_n*0; N) are reserved for honest miners (resp. attacker).*

3.2.3 Interpretation of Speed Mining

Inter-block Time is T. *Time used for mining k-th block*T_k. Mining speed α (honest) and α' (attacker). Probability p (honest) and q (attacker).

We note also ϕ = 600 seconds =10 minutes.

$$p = \mathrm{P}[\mathrm{T}<T']$$

$$p = \frac{\alpha}{\alpha+\alpha'}$$

$$q = \frac{\alpha'}{\alpha+\alpha'}$$

$$\alpha + \alpha' = \frac{1}{\phi}$$

$$\alpha = \frac{p}{\phi}$$

$$\alpha' = \frac{q}{\phi} \qquad (2.11)$$

The random variable Inf(T, T') has the exponential distribution with parameter $\alpha + \alpha'$. Denote by h (resp. h'.) the hashrate of the honest miners (resp. attacker) and t_0 (resp. t_0') the average time it takes for mining a block. Total hashrate of the network =h+h'. Proof-of-work: search for a nonce in Block Header such that Hash (Block Header) < Target. Set m=$\frac{2^{256}}{\text{Target}}$, we have

$$p = \frac{h}{h+h'}$$

$$q = \frac{\alpha}{\alpha+\alpha'}$$

$$(h+h')\,\phi = m$$

$$ht_0 = m$$

$$h't_0{}' = \mathrm{m} \qquad (2.12)$$

So, α, *h, p* are proportional.

3.2.4 Interpretation of Cost of Mining

Mining during *t* with hashing power *h* has a cost *C* (for honest miners) which is proportional to *t* and *h*: λ > 0 such that

$$C\,(h,\ t) = \lambda\, h\, t$$

Let *B* be the block reward. Parameter λ is adjusted so that

$$C\,(h + h', \phi\,) = \mathrm{B}$$

Which implies,

$$\lambda\,(h + h', \phi\,) = \mathrm{B}$$

and

$$C\,(h,\ t) = \frac{ht}{(h + h')\,\phi}\mathrm{B}$$

Similarly, for an attacker

$$C\,(h,\ t) = \frac{qt}{\phi}\,\mathrm{B}$$

Cost is a random variable Cost function at *T* =0 and is represented as:

$$C = \frac{q\tau}{\phi}\,\mathrm{B}$$

where τ is the stopping time:

$$\tau = \ \mathrm{Inf}\,\{t \geq \ S_z \,\middle|\, N'(t) \geq \mathrm{N(t)}\} \qquad (2.13)$$

Economic evaluation:

$$C = E[\frac{q\tau}{\phi}\,\mathrm{B}]$$

$$= \frac{qB}{\phi} \mathrm{E}\ [\tau]$$

$$= +\infty$$

Possible solution: In our assumption, the attacker will stop mining when he reaches $z + 1$ blocks on the fraudulent branch or when the honest miners reach z +1 blocks on the main branch, whichever happens first.

$$C = E[\frac{q\tau'}{\phi}\mathrm{B}]$$

$$= \frac{qB}{\phi} \mathrm{E}\ [S_{z+1} \wedge S'_{z+1}] \qquad (2.14)$$

where $S_{z+1}\ and\ S'_{z+1}$ are two independent random variables that has a Gamma distribution. It is the cost for mining *z* blocks. The security of a transaction increases with the number of confirmations that it receives, where an attacker benefits from the increasing goods at risk but is also throttled by the increasing proof of work required. Additionally, if a participant imposes a conservative confirmation deadline, the eclipse attack does not increase an attacker's profit when his share of the mining power is less than 35% or more than 10 confirmations are required.

3.2.5 Modelling of an attack prone network

Anonymous attack: A single output may not be used as an input to multiple transactions. At *T* =0, an agent N receives a transaction t_x from A (= attacker). A transaction t_x is issued from an UTXO t_{x0} and honest Miners start mining openly and transparently while attacker A starts mining secretly. As soon as the *z*-th block has been mined, A keeps on mining secretly and as soon as A has mined a blockchain with a length greater than the official one, A releases his blockchain to the network. Transaction t_x then disappears from the official blockchain. The attacker has a probability p of winning one unit and q =1- p of loosing one unit. We denote by *Xn* attacker's fortune at time *n*. Possible states are: {0}, {1},…..{N} and follows the behaviour of Markov's chain. The Transition probability $P_{k,l}$, given that k = {1, 2,… N-1} can be represented as:

$$P_{0,0} = 1$$

$$P_{N,N} = 1$$

$$P_{k,k+1} = \mathrm{p}$$

$$P_{k,k-1} = \mathrm{q}$$

Conditioning on the outcome of the initial play:

$$P_i = \mathrm{p}P_{i+1} + \mathrm{q}P_{i-1}$$

$$P_0 = 0$$

$$P_N = 1$$

$$P_{i+1} \text{ - } P_i = \frac{q}{p}\,(P_i) \text{ - } P_{i-1}$$

This gives:

$$P_i = \begin{cases} \dfrac{1-\left(\frac{q}{p}\right)^i}{1-(\frac{q}{p})^N} & if\ p = \dfrac{1}{2} \\ \dfrac{i}{N} & if\ p \neq \dfrac{1}{2} \end{cases}$$

Specific attack: When an attacker attacks keeping in mind a particular agent's address, at the beginning, gambler's fortune = banker's fortune minus *n* units. Gambler's fortune can be negative and a competition between attacker and agent starts. This competition ends if gambler's fortune =

banker's fortune at a certain time *t*. To determine the probability of success q_n, we have: q_0 = 1 and q_n tends to 0 when n tens to ∞. Also, by Markov's property,

$$q_n = q\ q_{n-1} + p\ q_n + 1$$

We have $q_n = (\frac{q}{p})^n$ when n> 0 and q_n = 1 when n ≤ 0 [103].

3.2.5.1 Approach 1

To detect the occurrence of an attack on the network the random variable **X**n is assigned which has a negative binomial distribution with parameters (n, p), i.e., for k ≥ 0 [104]. To determine the attacker's success probability let's reconsider the equation (2.9):

$$f_{Sn}(t) = \frac{(\alpha\ )^n}{(n-1)!} t^{n-1} e^{-\alpha t}$$

Now the probability of the random variable Xn can be given as:

$$P[Xn=k] = \int_0^{+\infty} P[N'(Sn) = k|Sn = t\ f_{Sn}(t)dt]$$

$$= \int_0^{+\infty} \frac{(\alpha' t)^{\ k}}{k!} e^{-\alpha'\ t} \frac{\alpha^n}{(n-1)!} t^{n-1} e^{-\alpha t} dt$$

$$= \frac{p^n q^k}{(n-1)!k!} \int_0^{+\infty} t^{k+n-1} dt$$

$$= \frac{p^n q^k}{(n-1)!k!} (k+n-1)! \qquad (2.15)$$

Thus, by introducing a negative binomial distribution the attacker's potential progress does not remain a Poisson distribution.

3.2.5.2 Approach 2

The agent waits for z blocks before making a transaction. Once it has been done, he knows how long it took and will denote this number by $\tau 1$. On an average, it should take E [z $\boldsymbol{T}$] = $z\frac{\tau 0}{p}$. Generally, the transition variable k is considered to be a dimensionless parameter and is set to 1 [105] but we will consider the dependency of k such that: k ≈ $\frac{p\tau 1}{z\tau 0}$. Hence, instead of computing the probability of z blocks, P(z) we will compute the concrete probability transition of z blocks P(z, k). Let the number of bocks mined by the attacker at $T = \tau 1$ be unknown to the merchant. By considering Poisson distribution parameter we get:

$$\lambda\,(\mathrm{z,k}) = \alpha'\tau 1$$

$$= \frac{q}{\tau 0}.\frac{zk\tau 0}{p}$$

$$= \frac{zq}{p}.\mathrm{k}$$

Thus equation (2.91) can be modified as:

$$\mathrm{P}[N'(\tau 1)=k] = \frac{(\frac{zq}{p}.\mathrm{k})^{k}}{k!}e^{-\frac{zq}{p}.\mathrm{k}t} \tag{2.16}$$

Hence, the risk of attacked is modelled more precisely and the occurrence can be detected by taking into account all the above considerations.

4 Input Analysis

The model comprises of 5 agent main types, and 4 agent sub-types. All the agent sub-type assumes all the characteristics from its main type. The 5 main agents include main, participant, transactions, blocks, and local records. The 4 sub-types are all inherited from the participant main type and include Blockchain manager, Administration, Professor and Student.

- **Main**: A function in the main agent randomly distributes the layout of the network before the initial setup. It decides the number of confirmed/unconfirmed transactions to be present in the memory pool, the number of links formed with the previous nodes based on the trust function and the more trusted nodes to be preferentially attached for every new node formation.

- **Participants:** All the participants have parameters for a public key (treated as a unique identifier for each participant) and a private key. Variables are initialized to store the number of blocks in the blockchain. The Blockchain Manager (BM) is responsible for managing all the transactions. BM develops the code for all services provided by the blockchain systems, smart contracts depicting the transfer of tokens and credits, verification of student's profile by the potential employers and interested parties that wish to provide direct internships and scholarships to the students. BM manages both the database services and Blockchain services simultaneously so as to explore the full potential of such systems. BM has 2-2 multi-signature private key to all the blockchain addresses and overviews any scenario of attack of hack of this key. The procedure of activities during any suck attack is discussed further in the report. The Administration comprises of all the current activities of any Higher Educational institute. It records the relevant information of all the current employees and students and checks the smooth execution of all the processes. In this model, the only processes being considered are the ones which involve crediting the student on a specific course and recording that information. All the other processes like registering of a new student, fee payment etc are not the part of this model but the model can surely be extended to include all such features. The educational institute develops student records that are indestructible and universal. This facilitates developing of a global standard of accreditation that will not need any verification or notarization thus eliminating the time to do such activities. It will expand the opportunities for the students on a global scale and if in any case a student loses his academic records, he can get it from his home university at any point of time within a matter of seconds unlike now when he has to go through formal procedures to go through any such situation. The professor verifies the results and publishes them after a student takes an exam. Other records related to every student like: attendance records, informal assessment, behaviour, remarks on leadership qualities etc can also be stored on the student's blockchain address. The proposed system focuses on the importance of formative assessment hence the student's say in evaluation is taken in account to avoid in future contradiction and to make sure that all the assessment is done in a fair manner. Before publishing the results, the students are informed to log into their accounts and check the manner of evaluation and are given a clear step by step protocol to refer to. Professor answers to any query the student might have regarding his evaluation and finally publishes the results. If there is a disagreement, the professor notifies the administration to step in and resolve the matter. In either case, the outcome is recorded in student's Blockchain address with his public key. Thus, results are stored in the central database only when professor is able to individually register completion of student's course obligations. The student is the pivoting participant in this model. He can always access his records using a private key but cannot change anything in them. He can approach any organization for the purposes of internship, scholarship and employment without the barrier of country, language or time. During any such situation, he can share his one-time usable private key with the interested institute. The employer will also save time in verifying if the records are authentic since it is present on student's university blockchain address with a timestamp and digital certificate. Each participant is only connected to two other participants in a ring-type fashion to reduce the total number of connections in the model. Each participant contains a population of blocks, transactions and local records.

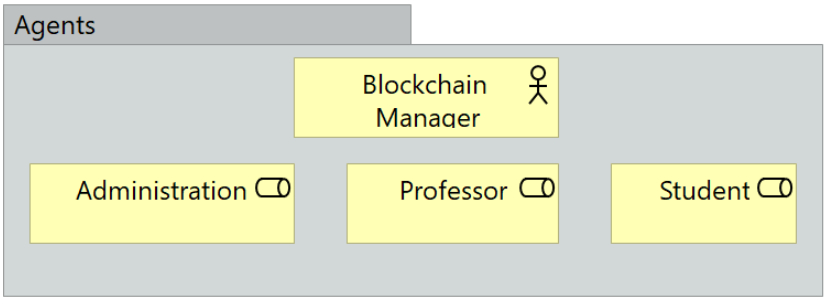


Figure 3-4: Participants of the proposed model

- **Transactions:** Transactions contain parameters to specify the time when the transaction was created, a unique identifier for that particular transaction and name of the sender and the receiver.

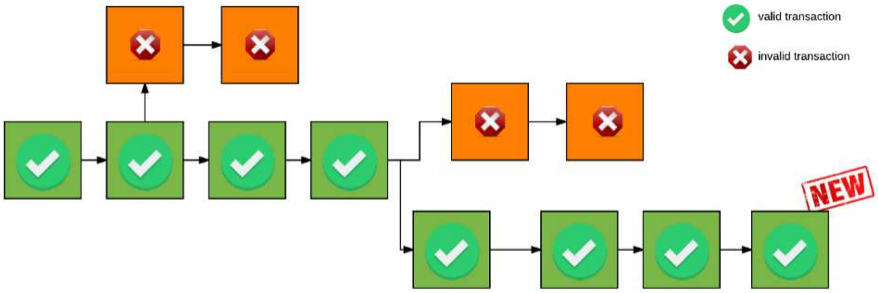


Figure 3-5: Process of Transaction formation [98]

- **Blocks:** Each block contains parameters to determine the hash string of the previous block, the number of transactions contained within the block, a timestamp for when the block was created, the total amount of toke transacted by all transactions within the block and the total number of tokens credited to that particular blockchain address.

- **Local records**: Local records contain information for the database service of the Educational Institute. It includes the names, student IDs and biometric information of students; names and identification number of Professors and Administration staff and the Blockchain Manager. Other parameters like the time the local record was created, the corresponding transaction ID on the blockchain addresses are also present.

3.3 Model design

At the initialization stage of the simulation every agent is equipped with several tokens and a trust (in digital currency) function. The number of different networks, the dimension and the density can be set independently. The simulation run can be initiated by “SETUP” and then begin by pressing the “GO” button. The model starts with a number of transactions laying around in the memory pool: some of them recent and the others which are yet unconfirmed. Theses transactions are represented in the model as nodes. Some of the nodes are shown to be connected with one or multiple links. The nodes arrange themselves in a scattered format thus inferring its de-centralized format. At each step, a new node randomly but with some bias, connects to the old node. Every new node only connects to the previous node if the previous node is verified and validated. More specifically, a node’s chance of being selected is directly proportional to the number of connections it already has, or its “trust”. The algorithm for initiating the model is shown below:

```
to setup
 clear-all
 [
 set-default-shape turtles "circle"
make-node nobody
make-node turtle 0
]

[ set-default-shape turtles "square"
create-turtles number-of-initial-transactions
   let num-links (number-of-initial-transactions) / 2
while [count links < num-links ]
[
  ask one-of turtles
  [
    let choice (min-one-of (other turtles with [not link-neighbor? myself])
                 [distance myself])
    if choice != nobody [ create-link-with choice ]
  ]
]

repeat 10
[
  layout-spring turtles links 0.3 (world-width / (sqrt number-of-initial-transactions)) 1
]
]
```

The code for making a connection is shown below:

```
to make-node [old-node]
 create-turtles 1
 [
   set color blue
   if old-node! = nobody
     [ create-link-with old-node [ set color gray]
       move-to old-node
       fd 8
     ]
 ]
end
```

The single GO button runs the simulation for one time-frame and will add one new node unlike the GO forever button which continuously and randomly links up the nodes. The code for simulation on GO button is as follows:

```
to go


 ask links [ set color yellow ]
 make-node find-partner
ask turtles

 [ ifelse fraud-identifier >= fraud-check-frequency

   [become-infected]

   [become-susceptible]



   set fraud-identifier fraud-identifier + 1

   if fraud-identifier >= fraud-check-frequency

   [ set fraud-identifier 0]

 ]



 tick

 layout

end



 reset-ticks

end
```

For the possibility of attack, detection of attack and prevention of attack on the network the following algorithm is followed:

```
to become-attack
  set infected? true
  set resistant? false
end
to become-susceptible
  set infected? false
  set resistant? false
end
to become-resistant
  set infected? false
  set resistant? true
  ask my-links [ set color gray - 2 ]
end

to spread-attack

  ask turtles with [infected?]

    [ ask link-neighbors with [not resistant?]

        [ if random-float 100 < attack-spread-chance

            [ become-infected ] ] ]
```

```
end

to do-attack-checks

 ask turtles with [infected? and attack-check-timer = 0]

 [

  if random 100 < recovery-chance

  [
   ifelse random 100 < gain-resistance-chance

    [ become-resistant ]

    [ become-susceptible ]
  ]

 ]
end
```

This procedure builds the network following preferential attachment algorithm. The procedure "setup" creates the network as a cluster of the connected nodes (referred to as "turtles") putting all of them close to each other. In this way a clearer graphical vision of hubs can be obtained.

- **UML diagram:**

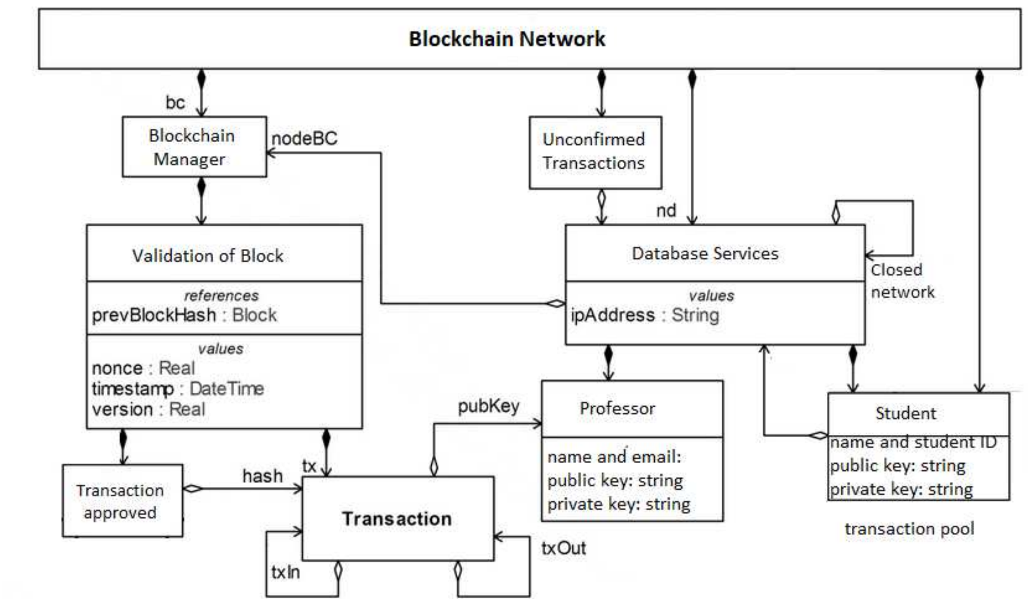
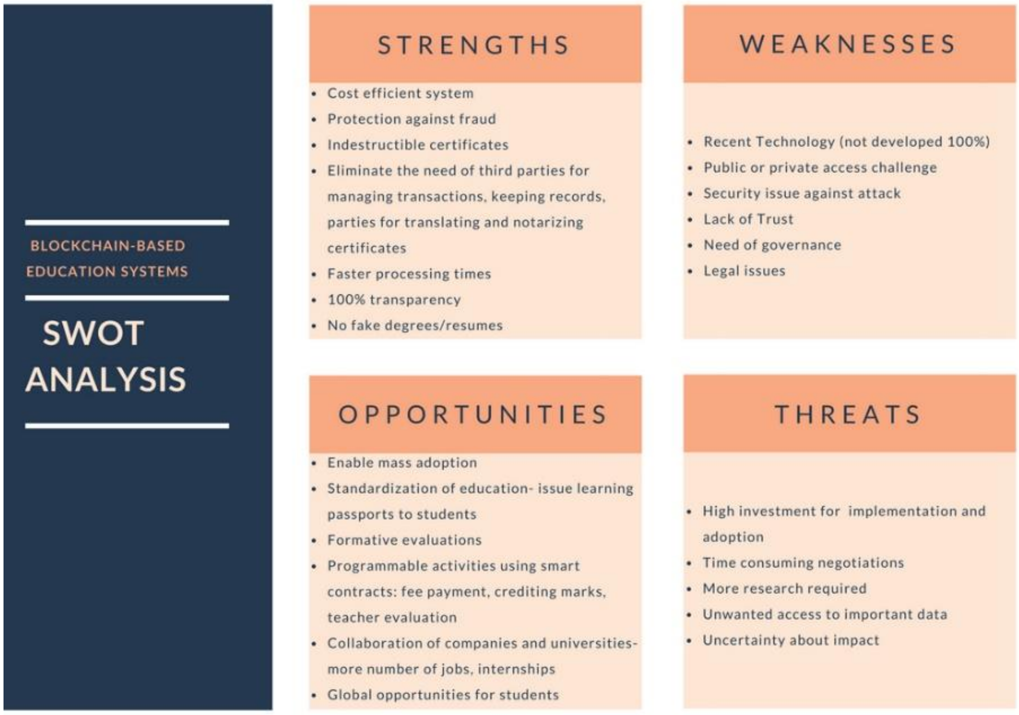


Figure 3-6: UML class diagram of Blockchain model

- **SWOT Analysis:**



BLOCKCHAIN-BASED EDUCATION SYSTEMS

SWOT ANALYSIS

STRENGTHS

- Cost efficient system
- Protection against fraud
- Indestructible certificates
- Eliminate the need of third parties for managing transactions, keeping records, parties for translating and notarizing certificates
- Faster processing times
- 100% transparency
- No fake degrees/resumes

WEAKNESSES

- Recent Technology (not developed 100%)
- Public or private access challenge
- Security issue against attack
- Lack of Trust
- Need of governance
- Legal issues

OPPORTUNITIES

- Enable mass adoption
- Standardization of education- issue learning passports to students
- Formative evaluations
- Programmable activities using smart contracts: fee payment, crediting marks, teacher evaluation
- Collaboration of companies and universities- more number of jobs, internships
- Global opportunities for students

THREATS

- High investment for implementation and adoption
- Time consuming negotiations
- More research required
- Unwanted access to important data
- Uncertainty about impact

Figure 3-7: SWOT analysis of the Blockchain based education system

3.4 Output analysis

The proposed model is envisioned for processing, managing and controlling tokens as academic credits and resting on a globally distributed Peer to Peer network, where peers of the blockchain network are Educational institutes and users of the platform are students and organizations (e.g. companies as potential employers). The tokens are an equivalent to student's credit value for completed courses. Each student will hold a dedicated blockchain address, where he will collect the corresponding tokens, i.e. the value of credits assigned by the Administration for his completed courses. Every time a student completes a course, his home educational institute will transfer the appropriate number of tokens to his blockchain address. The transfer information is stored on the blockchain address along with the following data: (1) the sender- presented as the related educational institute, (2) the receiver - student is anonymously identified, (3) token – course credit value, and (4) course identification. Now the student’s blockchain address will be able to globally prove his completed courses, without any administrative, script or language obstacles by simply presenting his blockchain address. For the sake of security, students will be assigned a 2-2 multi-signature address (student’s fingerprint and password) by home educational institute. Hence the student’s will not be able to transfer any of tokens to other addresses. The process of assigning students with tokens and institute’s ability to prove the possession of those will be handled by a blockchain manager assigned by the institute.

- **Blockchain services:** The basic services provided by the Blockchain depends upon the type of network it is being used in. as mentioned earlier, it a tool and not a solution. When employed in our system, it provides six basic services that can be used for improving the overall efficiency of the entire system.

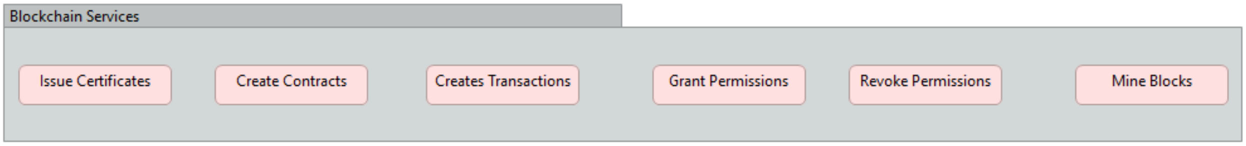


Figure 3-8: Different types of services provided by the Blockchain-based Education system

The most important service is Issuing certificates or Learning Passports to the students. Students will record proof of learning received from any source themselves, and a blockchain would be employed for instant verification of the authenticity of these documents. Apart from formal qualifications like degrees, this service can also hold and keep track of job experience, training courses volunteer work and certifications etc. Initially, two smart contracts are submitted to the blockchain by the administration. The first smart contract supports management of identities in the Blockchain for Education platform and the second one manages the lifecycle of certificates issued over the blockchain.

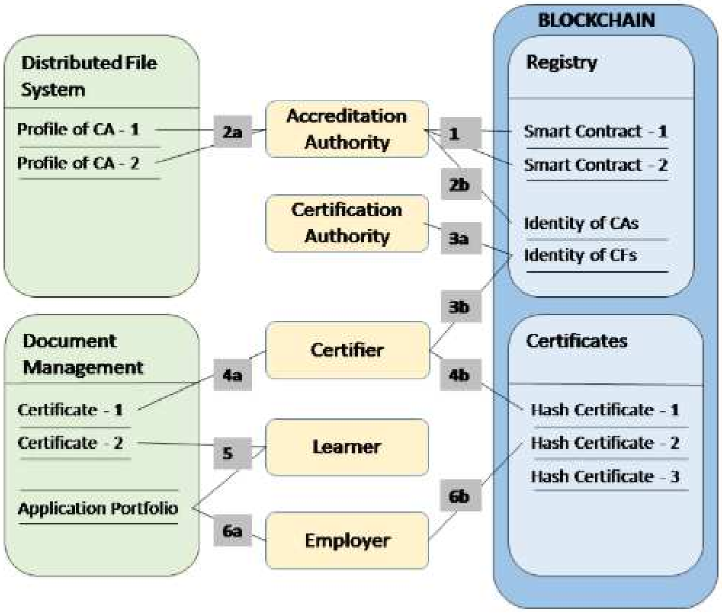


Figure 3-9: Certification in Blockchain [65]

The institute collects all information that a certificate consists of. The dataset comprises qualification or title, name and address of the certification authority, name of the certifier, name of the learner, and the date. Then the certificate is signed by the certifier and stored on the document management system and its fingerprint is written into the blockchain. Once the contracts are deployed, it is the Blockchain manager registers the public keys of administration as the legitimate issuer of certifiers in the contract and to submit public and non-personal profile information to the public storage. The profile information is read-only and publicly readable, i.e. it is not subject to the access control mechanisms of the smart contract. It contains only the long-term profiles of the institute like their name and country and not any personal information of certifiers or even students. The output analysis of system requirements along with blockchain features is shown below:

Blockchain features → **System requirements** ↓	**Transfer of value**	**Security**	**Auditability**	**Decentralization**
Reduction in process time	●		●	●
Cost reduction	●		●	●
Fraud detection		●	●	●
Fraud prevention		●	●	●
Record availability	●	●	●	●
Universality of records	●	●	●	●
Student satisfaction	●		●	
Teacher satisfaction	●		●	
Trust	●	●		●

Table 4: Output analysis of the proposed system

- **Connecting with Blockchain:** When a participant wishes to connect with the Blockchain for using its services, a request is made to the Blockchain manager. The participant is then providing with the specified Block Generator URL, network token and Blockchain address through which he wants to access the network. The Blockchain manager verifies the information provided by the participant and approve his request if it is authentic, if not the process is terminated. The participant then downloads the required data form the blockchain and connects to the services using his private key.

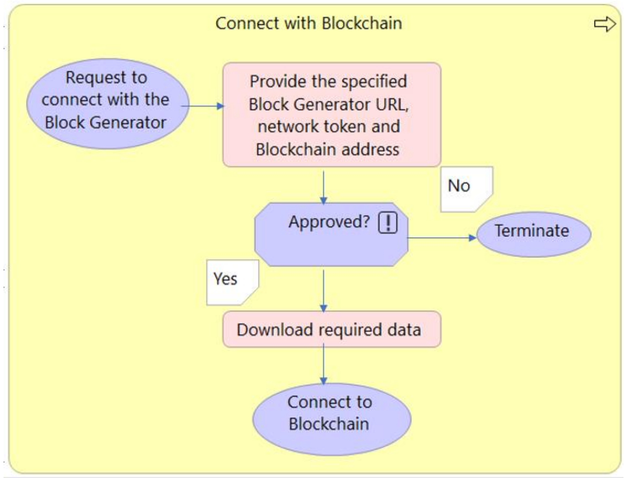

Connect with Blockchain
Request to connect with the Block Generator
Provide the specified Block Generator URL, network token and Blockchain address
No
Approved?
Terminate
Yes
Download required data
Connect to Blockchain

Figure 3-10: Process flow diagram of connecting with the Blockchain

- **Creating a Transaction:** The blockchain-based Education system is a publicly shared immutable ledger where transactions are contained in blocks which are linked together through a series of hash pointers. For creating a new transaction in the model, a request to do so is made by Administration, professor or the student. The Blockchain Manager receives the request and verifies the conditions under which the request is made. There are five different contexts under which the requests can be made: Regular Transaction, Issue new Asset, creating new Stream, Manage Permissions or Creating a Contract. For a regular transaction, the Blockchain manager asks to specify the name, quantity of transaction and receiver's address. Example of a regular transaction can be adding student's ID number on his personal profile. The transaction name and quantity need to be set for issuing a new asset like crediting the student's blockchain address with tokens after every successful course completion. For creating a new stream like starting a payroll for the student with a new scholarship, the stream name and details must be specified. For managing all the permissions related to any regular activity, the permission is checked for its nature and validity. Lastly, to create a new smart contract if requested by the administration, the contract code, address and input data is particularized. The next step for any of the above five requests is to sign the transaction with a unique hash and timestamp and send it to the associated Blockchain address. This results in creation and addition of a new transaction. The process flow of the entire procedure is shown in the figure below:

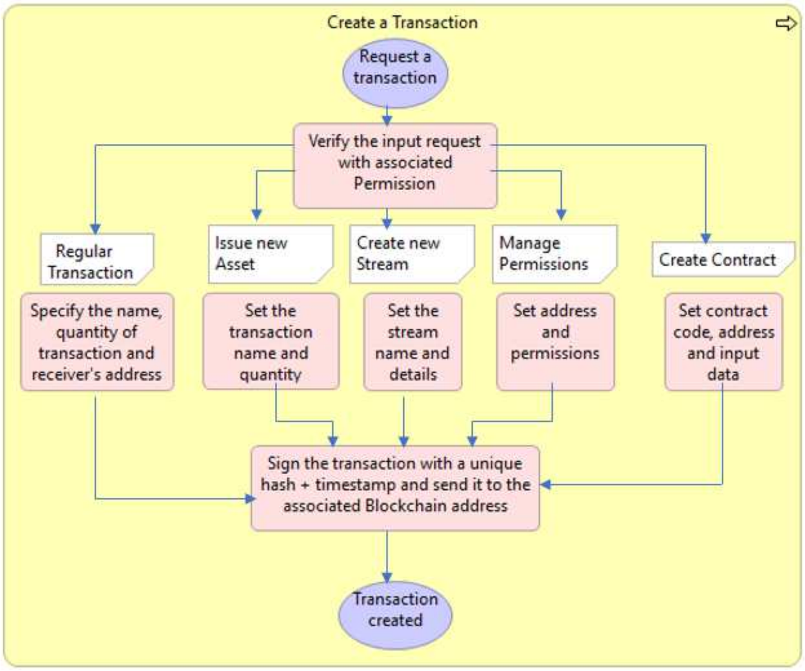

Create a Transaction
Request a transaction
Verify the input request with associated Permission
Regular Transaction
Issue new Asset
Create new Stream
Manage Permissions
Create Contract
Specify the name, quantity of transaction and receiver's address
Set the transaction name and quantity
Set the stream name and details
Set address and permissions
Set contract code, address and input data
Sign the transaction with a unique hash + timestamp and send it to the associated Blockchain address
Transaction created

Figure 3-11: Process flow diagram of creating a transaction

- **Generating a new Block:** The participants make transactions which sit pending in the memory pool. When they start making a new block and requesting transactions, the transactions become "verified" with 1 confirmation from all nodes. The process starts with receiving the previous block from the network. The unverified transaction is added to the block followed by attaching hash of the previous block and completing valid transaction generation. The proof of work is then calculated, and the new block is submitted to the network.

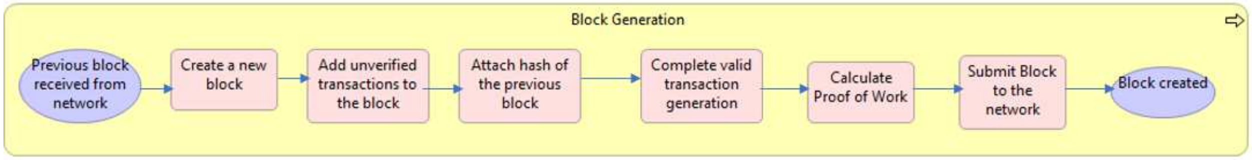

Block Generation
Previous block received from network
Create a new block
Add unverified transactions to the block
Attach hash of the previous block
Complete valid transaction generation
Calculate Proof of Work
Submit Block to the network
Block created

Figure 3-12: Process flow diagram of generating a new block

- **Validating the Block:** New transactions are broadcast to all nodes and as each node collects new transactions into a block and works on finding a difficult proof-of-work for its block, it finds a proof-of-work, it broadcasts the block to all nodes. Once the block is received and validated, the participant uses his private key sends it to the Blockchain manager for verification. Only if all the transactions are present in the block will a node accept that block. Nodes accept the block by creating the next block in the chain, using the hash of the accepted block as the previous hash. Always the longest chain will be considered the correct one by nodes and the nodes will keep working on extending it.

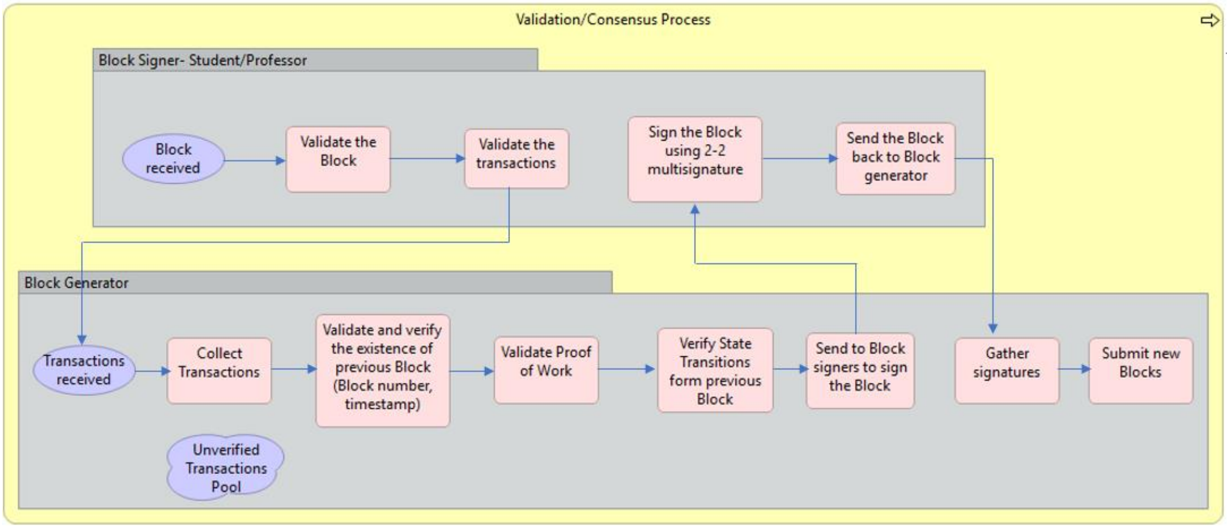

Validation/Consensus Process
Block Signer- Student/Professor
Block received
Validate the Block
Validate the transactions
Sign the Block using 2-2 multisignature
Send the Block back to Block generator
Block Generator
Transactions received
Collect Transactions
Validate and verify the existence of previous Block (Block number, timestamp)
Validate Proof of Work
Verify State Transitions form previous Block
Send to Block signers to sign the Block
Gather signatures
Submit new Blocks
Unverified Transactions Pool

Figure 3-13: Process flow diagram of consensus mechanism

3.6 Concepts and assumptions

The assumptions made during the construction of this blockchain protocol are stated below:

- All participants have an equal chance at mining the next block.
- All transactions are of the same size ie. 1 kilobyte.
- Any participant who will initiate the transaction will also store the corresponding local record of that transaction.
- All the blocks are of the same size.
- It is very difficult to calculate the initial setup cost of the system since it depends upon Database management system costs: 5% to 10%, Infrastructure costs: 10% to 20%, Software costs: 15% to 30% and Human resources costs: 40% to 60% [106]. As a result, we take that the initial cost of setting up our proposed system is $1 million if it is adopted for a large university.

3.7 Model Verification and Validation

The total number of transactions, total size of the blockchain, and network efficiency were plotted over time, to validate the behavior of the model relative to the real Bitcoin network historically. The general direction of all the parameters also coincided with the real Bitcoin network.

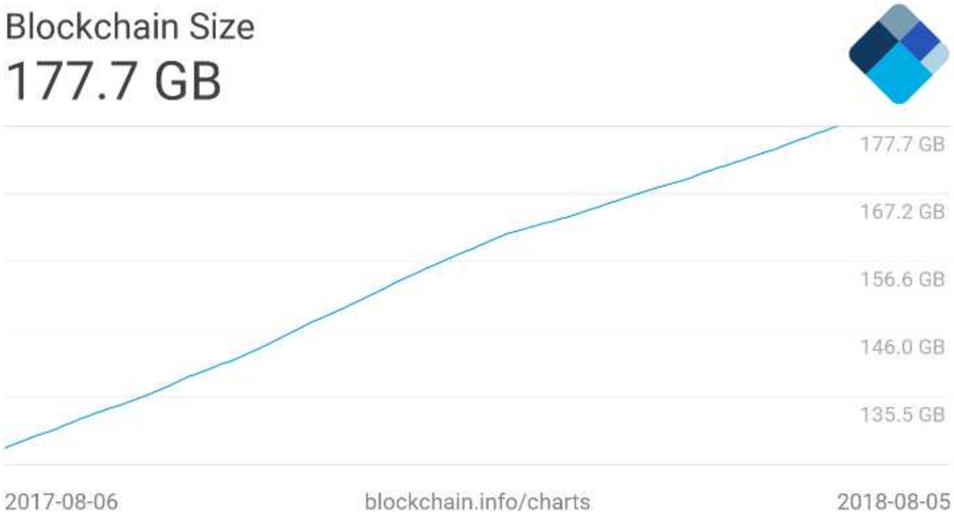


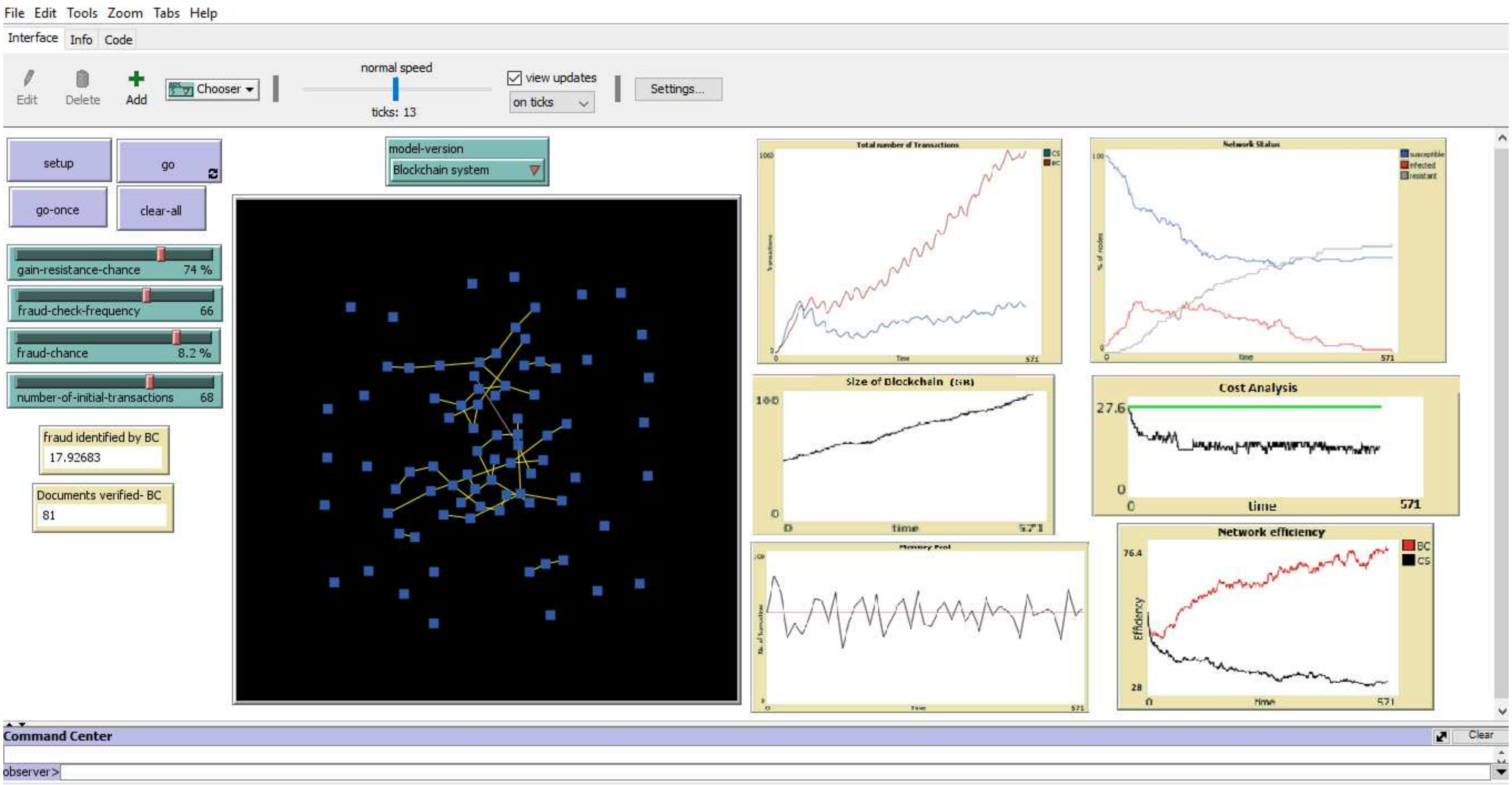
Figure 3-14: Growth of Blockchain from 2017 to 2018 [110]

When viewing the total number of transactions seen in Figure 3.8a, the final number of transactions in the simulation is 106,0045,000, while the real value is 128,612,806 [111], creating a difference of 21.3%. This difference was never more than 21.7% in the rate of transactions throughout the simulation. The resulting size of a blockchain is directly related to the amount of transaction data contained within it. The source of collection of data for the network efficiency of the real Bitcoin network is from one particular Bitcoin node. The data is highly variable, as the number of connected peers may vary at any given time [112]; however, in general, the average bandwidth consumption in the simulation coincided with the direction of the real Bitcoin network. Based on the performance of the mentioned parameters, it seems to be a reasonable conclusion that one can use the proposed model to replicate specific behaviors of blockchain-based networks.

Chapter 4

Results and Discussion

As a single run of the simulation is performed, the confirmed transactions in the memory pool start connecting through links in a decentralized manner. The unconfirmed transactions float around in the memory pool until they are confirmed. Once the transaction has waited for a time limit of T_n it automatically gets removed from the memory pool and the participant who initiated that transaction is notified. 16 unique runs were performed and the graphs were collected for the most valid run. A screenshot of the model simulation in progress in Netlogo is shown below:



model-version: Blockchain system

gain-resistance-chance 74 %

fraud-check-frequency 66

fraud-chance 8.2 %

number-of-initial-transactions 68

fraud identified by BC: 17.92683

Documents verified- BC: 81

Figure 4-1: Screenshot of the model simulation in progress

It is observed that the number of transactions of a blockchain system increases with the passage of time following the power-law while the number of transactions of a traditional system increases following the normal exponential distribution. The curve is a fluctuating ascending graph by taking into considerations factors like number of participants and possibility of attack. While on the other hand, the curve for a traditional system follows the same path as that of the blockchain system at the initial stage of transactions but the number of transactions starts to decrease after the peak because a greater number of participants results in congestion on the network with decreased efficiency. The network efficiency of the proposed system corresponds to the number of transactions processed, time taken to process each transaction and the cost analysis of the system. Unlike the blockchain network, the traditional network follows an exponential distribution. It was observed that both the systems show and initial rise in total number of transactions irrespective of the number of pending or initial transactions in the system. But with increase in the initial transactions both the systems start behaving differently. While the curve for blockchain network do not vary much, the peak for the traditional system's curve is achieved much later if the initial transactions in the system are more. The behaviour of both the systems with a random of 68 initial number of transactions is shown in Figure 4-2.

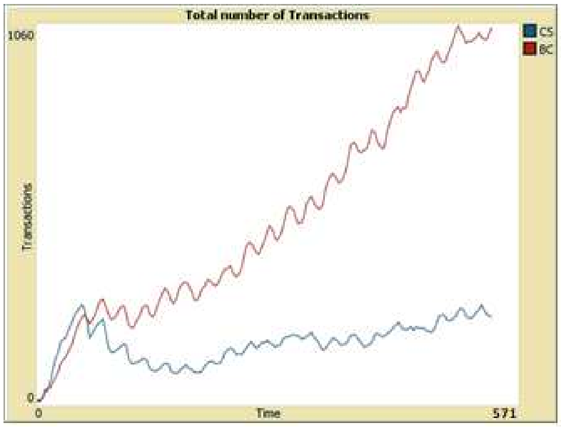


Figure 4-2: Number of transactions on a blockchain based network vs on a traditional network

A comparison between network efficiencies of blockchain system and the traditional education system is made. The efficiency is computed by considering the following parameter: total time for the transaction to complete, average number of participants, average number of transactions and tolerance to possible attack. The network efficiency of the blockchain based system increases with every tick (time unit) while on the other hand it decreases for the traditional system. An observation is made at this point that the network efficiency of the traditional system will keep on decreasing with time even if the average number of participants and average number of transactions do not vary. This implies that the traditional education system is always in a constant need of checks, data storage clearance and restarts which results in service disruption and further decrease in efficiency. With increase in the occurrence of an attack on the network, network efficiency of both the systems decrease but the overall efficiency of the blockchain network still remains higher than that of the traditional system. The network efficiency of the blockchain network increases with the increase in number of attack-check frequency but that of the traditional system remains almost the same. When chance of both the networks to become resistant to attack increases, they show an increase in network efficiency. The network efficiency of both the systems with resistance-chance = 71%, attack check frequency = 66%, chance of occurrence of attack = 82% and initial number of transactions = 68 is shown in Figure 39. Under this circumstance, the efficiency of the blockchain system is around 76% while that of a traditional network is around 32%. Hence it can be inferred that the efficiency of the educational system increases by almost twice on a blockchain network under the above said circumstances.

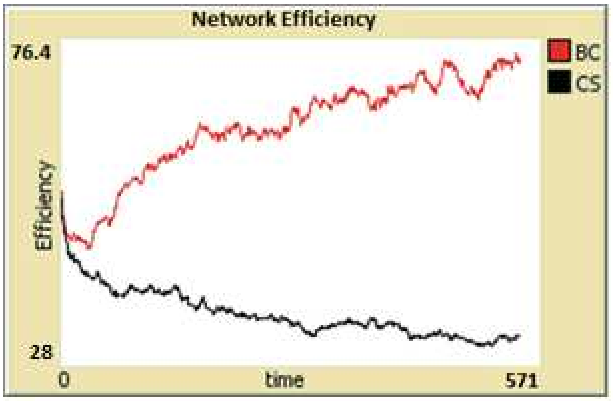


Figure 4-3: Network efficiency of a blockchain based network vs of a traditional network

To ensure that the proposed system is working as anticipated and to examine all the transactions ever happened on the blockchain it is important to calculate the total size of the blockchain during the simulation runs. For our simulation run, the size of blockchain becomes 100 GB in time = 571 days. With the variations in resistance-chance, attack check frequency, chance of occurrence of attack and initial number of transactions there is less to no variation in the size of Blockchain and can be seen in Figure 4-5.

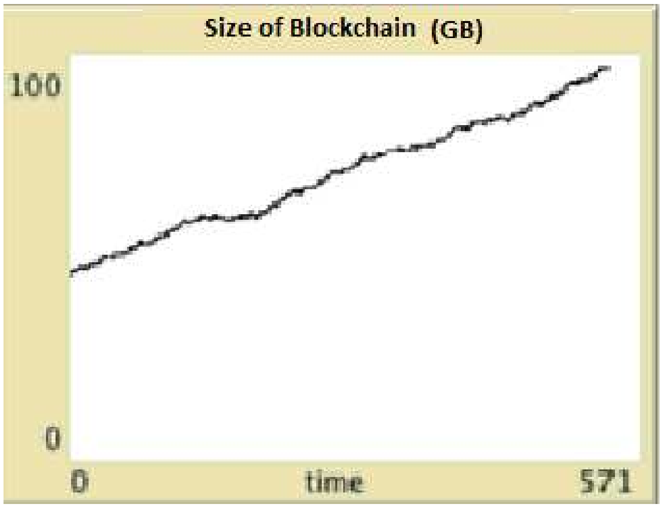


Figure 4-4: Total size of blockchain in GB

The number of transactions in the memory pool of the system is important to determine because it reflects the possible number of transactions the system will work with. A number of 68 transactions in the memory pool at any given moment is considered as a threshold as the proposed model responds best to this number. This results in a fluctuating graph inferring that the number of transactions in the memory pool remain close to the initial number of transactions without any affect of resistance-chance, attack check frequency and chance of occurrence of attack because these transactions make new for new transaction requests once they are confirmed or deleted from the memory pool due to lack of validation. The graphical result of this inference is shown in Figure 4-6.

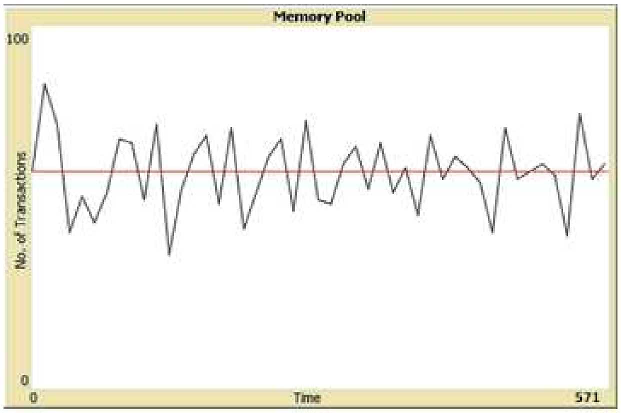


Figure 4-5: Number of transactions in memory pool

As mentioned in the previous chapter it is extremely difficult to estimate the initial cost of setting up a new system hence an assumption is made of $ 1 million. It is observed that the cost of running and managing a blockchain system reduces with time. After the initial setup cost, it does not require any maintenance cost as long as the blockchain system works with the same activities that it was set up with and no additional activates are added into the system.. There is no affect of resistance-chance, attack check frequency, chance of occurrence of attack and initial number of transactions on the cost of Blockchain. It decreases visibly after the setup and becomes almost constant with time as shown in the Figure 4-7.

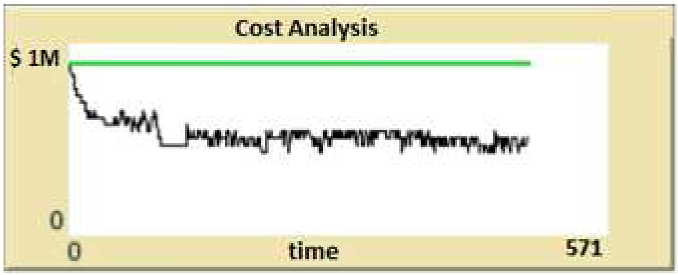


Figure 4-6: Cost analysis of the blockchain based education system

Under the condition of an attack on the blockchain network, the nodes of the network get prone to this attack become infected. The proposed system detects the infected node and tries to remove it. This is done by increasing the number of confirmations required for each transaction to occur along with increasing the waiting time for every transaction. This means that the transaction requests will be received and viewed by the system but not verified instantly even if they appear to be valid transactions. This will decrease the probability of attack on the system. Also, the system will become susceptible to such attacks and wait for such an attack to occur so that it can boycott the attacker by deactivating the infected node. If the attack is still consistent, re-programming of the system can be done so as to make the system resistant to such attacks. The behaviour of the system under attack is shown in the Figure 4-8. As depicted in the figure, 100% of the nodes are assumed to be infected as the simulation starts and its curve declines with time. On the other hand, the number of infected nodes increase when the simulation starts because the system becomes aware and starts detecting them. Once past this stage, the number of infected nodes decrease and does not peak again. The system becomes more and more resistant to the attack with time as seen from the figure below. The following observation is made by setting the system parameters at resistance-chance = 71%, attack check frequency = 66%, chance of occurrence of attack = 8.2% and initial number of transactions = 68.

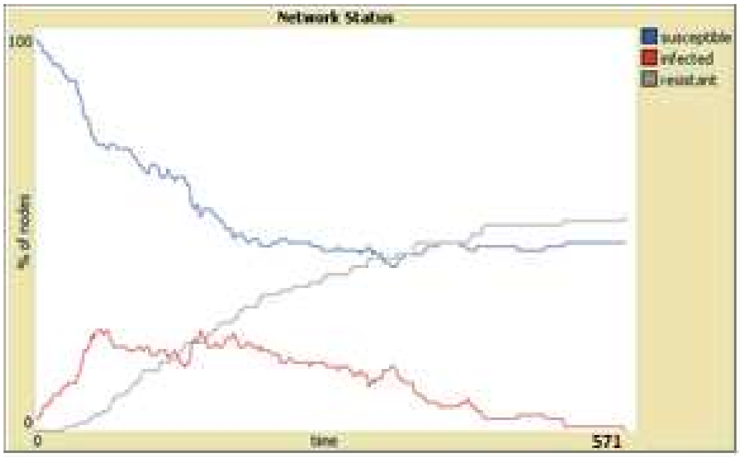


Figure 4-7: System behaviour under attack, scenario 1: at attack check frequency = 66%, chance of occurrence of attack = 82%, initial number of transactions = 68

With all the other parameters to be same, if we reduce the attack-check frequency to 20 % from 66% following graph is obtained shown in Figure 4-9. It shows that if there are fewer checks for the attack on the system the number of susceptible nodes will decrease but the number of infected nodes will surge up. The number of resistant nodes will show a dramatic increase, but it will not improve the efficiency of the system since only the suspected nodes are becoming resistant. Less the number of suspected nodes, more is the overall number of resistant nodes. The system behaviours of reducing the initial number of transactions and reducing the chance of attack are shown in Figures 4-10 and 4-11 respectively.

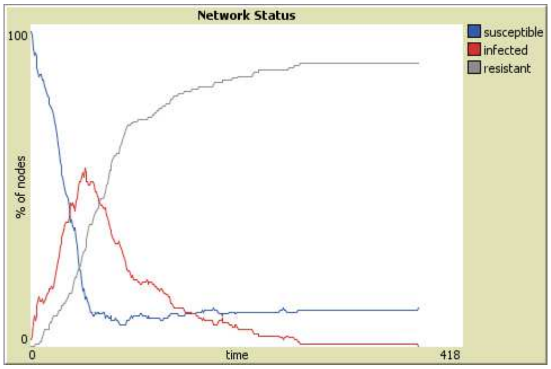


Figure 4-8: System behaviour under attack, scenario 2: at attack check frequency = 20%, chance of occurrence of attack = 82%, initial number of transactions = 68

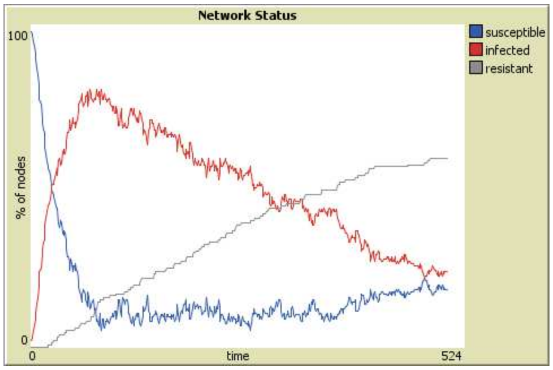


Figure 4-9: System behaviour under attack, scenario 3: at attack check frequency = 66%, chance of occurrence of attack = 35%, initial number of transactions = 68

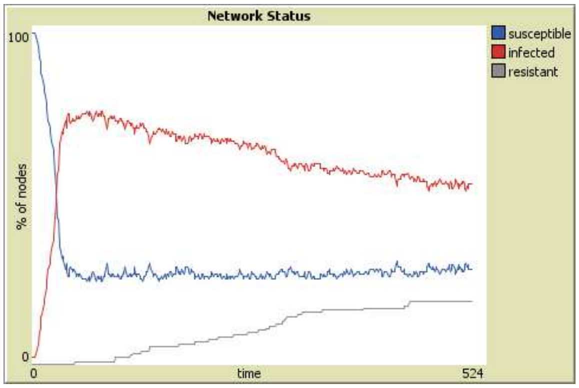


Figure 4-10: System behaviour under attack, scenario 4: at attack check frequency = 66%, chance of occurrence of attack = 35%, initial number of transactions = 20

Chapter 5:

Conclusion and Future Work

5.1. Conclusion

Blockchains have the potential to revolutionise various industries besides finance. In this thesis, an agent-based model was developed in Netlogo modeling software to study blockchain and proposed a hypothetical blockchain-based Education System. The first objective of our work was met by successful implementation of this model. Since distributed ledger systems like Blockchain and Education systems (where the activities and working can never be completely predicted or generalized) are both complex systems, their modelling and simulation is extremely challenging. The work provides a comprehensive review of blockchain-based Education systems and demonstrates how such a system is constructed and is used to further facilitate discussion surrounding effective design of such a system. The model is formed using Gresham's Law and Trust function associated with Bitcoin and blockchain. Overall efficiency of the system is analysed by determining the total number of transactions happening during the simulation, memory pool size of the blockchain, total size of the blockchain and by analysis cost of the system. It is found out that the total number of transactions of the system is 106,0045,000 for the simulative run for 571 days and varies by 21.3% from the real Bitcoin values. After initial setup cost of the blockchain, the overall cost of the system declines and remains constant unlike traditional systems which require regular maintenance. The total size of the blockchain system over this time period becomes around 100 GB which is also close to the size of an actual blockchain if observed over same amount of time. The third objective of our work is met by examining the behaviour of system under attack by varying the input parameters of the system. The model shows best behaviour when the attack check frequency of the system is set to 66%, chance of occurrence of attack is 82%, initial number of transactions in the memory pool are 68. Under these circumstances, the system quickly becomes aware of infected or attacked nodes and increases its resistance towards them. This resistive nature can be obtained by increasing the number of nodes, increasing the number of confirmations required for each transaction and by boycotting the infected node altogether. Demonstrating the requirements of a blockchain-based education system with a basic simulation must be emphasised to the education industry as it introduces new challenges in addition to demonstrating the underlying operational capabilities and technical features offered by blockchain. Varying design decisions can be made when constructing a blockchain-based education system that affect the ability of certain requirements to be met. Blockchains may be used as a valuable tool for the transfer and auditing of information within an educational ecosystem, but further research remains to be done that explores the performance trade offs involved when moving from legacy systems to the integration of more decentralized blockchain-based systems. Blockchains and cryptocurrency technologies are still in their infancy, and it may take several years until they can be used in commercial production environments, but their potential remains promising.

5.2. Strengths and Limitations

The strengths offered by our model are:

- The objectives of our study were completely met as the simulation model behaved like a real blockchain network and the satisfactory results were obtained.

- The most important feature of a decentralized network: trust function is taken into account while performing mathematical modelling to increase the security of such a system and avoiding attack.
- Different parameters of the system like cost, time and system behaviour under attack are modelled.

Limitations of our work is as following:

- Though the hype of Blockchain technology has been there for a while now but still there are not many real-world implementations to look at and for proper understanding. This results in a very narrow section of research and work which has been done so far. With a limited number of literatures to work with, this work faced a scarcity to reference. Secondly, Blockchain-based systems are still in their infancy as industries find it difficult to trust a new technology for its full implementation and recording its confidential data on a globally accessible network. Our work also comes with these two limitations, but they can be eventually removed once more and more research is done in this area and Blockchain-based systems start proving themselves to be trustworthy and reliable. The limitations of our model are:
- The model is built on predictive equations based on power-laws that were initially used to build Bitcoin, Blockchain and other cryptocurrencies and have not been updated or improved since then.

5.3 Future scope

While our model demonstrates the efficiency and feasibility of a blockchain-based educational

System, the model can be extended to explore complete optimal design and architecture. These topics may include:

- Simulation and modeling of varying token incentive structures like: a) modifications to the mining and initial distribution of the tokens associated with using the blockchain network, b) models with an increased number of system participants and agents, c) models can be created with interaction of the potential employees with the university for the intent of providing internships, scholarships and jobs and d) payment of student fee using blockchain.
- Simulating and estimating resource requirements for system participants. These requirements will limit the amount of data and number of participants that can use such a system. Simulation tools have already been used to predict latency of blockchain-based systems.
- Internal processes could be added to model the execution of smart contracts. Mathematical modelling of introduction of Smart contracts in the simulation model should be made.
- More research and solutions can be formed for the privacy and security concerns for data stored, shared or secured in a blockchain.

References

1. Chen G., Xu B., Lu M., Chen N. S. (2018). Exploring blockchain technology and its potential applications for education. Smart Learning Environments, 5(1), 1
2. Turkanović M., Hölbl K., Heričko M., Kamišalić A. (2018) eductx: A Blockchain-Based Higher Education Credit Platform, in IEEE Access, 6, 5112-5127, DOI: 10.1109/ACCESS.2018.2789929
3. https://www.theguardian.com/higher-education-network/blog/2012/jul/18/degree-fraud-hedd checking-service (accessed on July 26, 2018)
4. Andreev R. A., Andreev, P. A., Krotov L. N., Krotova E. L. (2018). Review of Blockchain Technology: Types of Blockchain and Their Application. Intellekt. Sist. Proizv., 16(1), 11-14.
5. Djafri K., (2018). Blockchain as a service in Education. Edgecoin - The future of education is smart and built on blockchain. https://www.edgecoin.io/ (assessed on July 26,2018)
6. Grech A., Camilleri, A. F. (2017). Blockchain in education.
7. Heath B. L., (2010). The history, philosophy, and practice of agent-based modeling and the development of the conceptual model for simulation diagram.
8. Paul (2014)., Column. Available via https://www.portofrotterdam.com/en/news-and-press-releases/without-datano-logistics (assessed on July 26,2018)
9. Liedel D. A., (2018). The taxation of bitcoin: How the IRS views cryptocurrencies. Drake Law Review 66(1), 107-146.
10. Ballou R. H., (2007). Business logistics/supply chain management: planning, organizing, and controlling the supply chain. Pearson Education India.
11. Glaser F., (2017). Pervasive Decentralisation of Digital Infrastructures: A Framework for

Blockchain enabled System and Use Case Analysis. In Proceedings of the 50th International Conference on System Sciences. https://aisel.aisnet.org/hicss-50/da/open_digital_services/4/.

12. Brenig C., Schwarz J., Rückeshäuser N., (2016). Value of Decentralized consensus Systems-Evaluation Framework. In ECIS (p. ResearchPaper75).
13. McGinnis J. O., Roche K. (2017). Bitcoin: order without law in the digital age. https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2929133.
14. Nakamoto S. (2009). Bitcoin: A Peer-to-Peer Electronic Cash System. http://bitcoin.org/bitcoin.pdf (assessed on July 26,2018)
15. Notheisen B., Hawlitschek F., Weinhardt C. (2017). Breaking down the blockchain hype–towards a blockchain market engineering approach.
16. Chuen D. K., Deng R. H., (2017). Handbook of Blockchain, Digital Finance, and Inclusion: Cryptocurrency, FinTech, InsurTech, Regulation, ChinaTech, Mobile Security, and Distributed Ledger. Academic Press.
17. Buterin V. (2014). A next-generation smart contract and decentralized application platform. white paper.
18. Zheng Z., Xie S., Dai, H. N., Wang, H. (2016). Blockchain challenges and opportunities: A survey. Work Pap. –2016.
19. Morabito V. (2017). Business Innovation Through Blockchain. Https://doi.org/10.1007/978-3-31948478-5 (accessed on July 26, 2018)
20. Froystad P., Holm, J. (2016). Blockchain: powering the internet of value. Evry Labs.
21. Xu J. J., (2016). Are blockchains immune to all malicious attacks? Financial Innovation, 2(1), 25. https://doi.org/10.1186/s40854-016-0046-5 (accessed on July 26, 2018)

22. Notheisen B., Hawlitschek F., Weinhardt C. (2017). Breaking down the blockchain hype– towards a blockchain market engineering approach.

23. Swan M., (2015). Blockchain: Blueprint for a new economy. " O'Reilly Media, Inc.".

24. Cheliotis G., (2009). From open source to open content: Organization, licensing and decision processes in open cultural production, Decision Support Systems, 47(3), 229–244

25. Grewal R., Gary L., Mallapragada G., (2006). Location, Location, Location: How Network Embeddedness Affects Project Success in Open Source Systems. Management Science 52(7):1043-1056. http://dx.doi.org/10.1287/ mnsc.1060.0550

26. Lindman J., Kinnari T., Rossi M. (2016). Business Roles in the Emerging Open-Data Ecosystem, IEEE Software, 99

27. Midha V., Palvia P., (2012). Factors affecting the success of Open Source Software, Journal of Systems and Software, 85(4) 895–905. DOI: 10.1016/j.jss.2011.11010

28. Glaser, F. (2017). Pervasive decentralisation of digital infrastructures: a framework for blockchain enabled system and use case analysis.

29. Bogart, S., Rice, K. (2015). The blockchain report: welcome to the internet of value. Needham Insights.

30. V. Buterin, (2014). A next-generation smart contract and decentralized application platform, Etherum, no. January 1–36.

31. Crosby M., Pattanayak P., Verma S., Kalyanaraman V. (2016). Blockchain technology: Beyond bitcoin. Applied Innovation, 2, 6-10.

32. Iansiti M., Lakhani K. R. (2017). The truth about blockchain. Harvard Business Review, 95(1), 118-127.

33. Szabo N. (1997). Formalizing and securing relationships on public networks. First Monday, 2(9).

34. Buterin V. (2014). A next-generation smart contract and decentralized application platform. white paper.

35. Fairfield J. (2014). Smart contracts, Bitcoin bots, and consumer protection, Washington and Lee Law Review Online, 71(2):35-50.

36. Omohundro S. (2014). Cryptocurrencies, smart contracts, and artificial intelligence. AI matters, 1(2), 19-21.

37. https://www.pcmag.com/article/350088/blockchain-in-2017-the-year-of-smart-contracts (accessed on July 27, 2018)

38. https://whitepaperdatabase.com/ethereum-eth-whitepaper/ (accessed on July 26, 2018)

39. Wood G. (2014). Ethereum: a secure decentralised generalised transaction ledger https://github.com/ethereum/yellowpaper, Yellow paper 151 (accessed on July 26, 2018)

40. Idelberger F., Governatori G., Riveret R., Sartor G. (2016). Evaluation of logic-based smart contracts for blockchain systems. In International Symposium on Rules and Rule Markup Languages for the Semantic Web (167-183), Springer International Publishing.

41. Troy S. (2018). What is a smart contract and what's it good for?, Available online at: http://searchcio. Techtarget.com/feature/What-is-a-smart-contract-and-whats-it-good-for. (accessed on July 26, 2018)

42. Hoskinson C, A brief introduction to smart contracts. Available online at: https://www. Youtube.com/watch?V=3by66zgr8cs. (accessed on July 26, 2018)

43. Xu X., Pautasso C., Zhu L. et al (2016). The Blockchain as a software connector. 2016 13th Working IEEE/IFIP Conference on Software Architecture (WICSA 2016), Venice, 2016, pp. 182–191

44. Wood G, Devcon1: Ethereum. Available online at: https://www.youtube.com/watch?V=U_ LK0t_qapo. (accessed on July 26, 2018)

45. Koulu R., (2016). Blockchains and online dispute resolution: smart contracts as an alternative to enforcement. SCRIPTed, 13, 40.

46. Cuomo J., (2016) how businesses and governments can capitalize on blockchain. Available online at: https://www.ibm.com/blogs/think/2016/03/16/how-businesses-and-governments-cancapitalize-on-blockchain/. (accessed on July 26, 2018)

47. Lim C., Saw T., Sargeant C., (2018) Smart contracts: bridging the gap between expectation and reality. Available online at: https://www.law.ox.ac.uk/business-law-blog/blog/2016/07/smartcontracts-bridging-gap-between-expectation-and-reality. (accessed on July 26, 2018)

48. Levine M., (2018) Herbalife deals and blockchain dreams. Available online at: https://www. Bloomberg.com/view/articles/2016-08-26/herbalife-deals-and-blockchain-dreams. (accessed on July 26, 2018)

49. Coy P., Kharif O., (2018). This is your company on blockchain. Available online at: http://www. Bloomberg.com/news/articles/2016-08-25/this-is-your-company-on-blockchain. (accessed on July 26, 2018)

50. http://about.smartcontract.com (accessed on July 26, 2018)

51. Stark J., (2018) Making sense of blockchain smart contracts. Available online at: http://www. Coindesk.com/making-sense-smart-contracts/. (accessed on July 27, 2018)

52. Wall L., (2018). Smart contracts in a complex world. Available online at: https://www.frbatlanta. Org/cenfis/publications/notesfromthevault/1607. (accessed on July 27, 2018)

53. Heires, K. (2014). Preparing for the Internet of Things. Risk Management. 61(1),28.

54. Rowland, C., Goodman, E., Charlier, M., Light, A., Lui, A. (2015). Designing connected products: UX for the consumer internet of things. " O'Reilly Media, Inc.".

55. Burkitt, F. (2014). A strategist's guide to the Internet of Things (No. 77). Strategy+ Business.

56. Christidis, K., Devetsikiotis, M. (2016). Blockchains and Smart Contracts for the Internet of Things. IEEE Access, 4, 2292-2303

57. Dorri, A., Kanhere, S. S., Jurdak, R. (2017). Towards an optimized blockchain for IoT. In Proceedings of the Second International Conference on Internet-of-Things Design and Implementation (173-178). ACM.

58. Wang P., Valerdi R., Zhou S., Li L., (2015). Introduction: Advances in IOT research and applications. Information Systems Frontier, 17(2),239-241.

59. Perera C., Liu C., Jayawardena S. (2015). The emerging internet of things marketplace from an industrial perspective: a survey. IEEE Transactions on Emerging Topics in Computing. Doi:10.1109/ TETC.2015.2390034.

60. Whitmore A., Agarwal A., Xu L. (2015). The internet of things-a survey of topics and trends. Information Systems Frontiers, 17(2). Doi:10.1007/s10796-014-9489-2

61. Xu L., He W., Li S. (2014). Internet of things in industries: a survey. IEEE Transactions on Industrial Informatics, 10(4), 2233–2243.

62. Bi Z., Cochran D. (2014). Big data analytics with applications. Journal of Management Analytics, 1(4), 249–265.

63. Zeinab, K. A. M., Elmustafa, S. A. A. (2017). Internet of Things applications, challenges and related future technologies. World Scientific News, 2(67), 126-148.

64. Gubbia J., Buyyab R., Marusic S., Palaniswami M. (2013). Internet of Things (IOT): A vision, architectural elements, and future directions. Future Generation Computer Systems 29 1645-1660

65. https://dupress.deloitte.com/dup-us-en/focus/internet-of-things/iot-commercial-realestate-intelligent-building-systems.html (accessed on July 26, 2018)

66. Grandinetti L. (Ed.). (2013). Pervasive Cloud Computing Technologies: Future Outlooks and Interdisciplinary Perspectives: Future Outlooks and Interdisciplinary Perspectives. IGI Global.

67. http://standardsinsight.com/iot/iotworkshop (accessed on July 26, 2018)

68. Bandyopadhya D., Sen J. (2011). Internet of things: Applications and challenges in technology and standardization. Wireless Personal Communications, 58(1), 49-69.

69. http://www.academia.edu/3276195/Internet_of_Things_Applications_and_Challenges_in_Technology_and_Standardization (accessed on July 26, 2018)

70. Thierer A. D., (2015). The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation.

71. Shekhar S., (2015), Blockchain Revolution in Supply Chain. International journal of engineering science and computing, 7(6).

72. Gockel B., Acar T., Forster M. (2018), Perspectives on the upcoming impact of blockchain technology and use cases for the logistics industry, “Blockchain in logistics”

73. Britchenko I., Cherniavska T., Cherniavskyi B. (2018). Blockchain technology into the logistics supply.

74. http://thinkers50.com/biographies/don-tapscott/ (accessed on July 26, 2018)

75. http://www.ics-shipping.org/shipping-facts/shipping-and-world-trade (accessed on July 26, 2018)

76. http://www3.weforum.org/docs/WEF_SCT_enablingtrade_Report_2013.pdf (accessed on July 26, 2018)

77. https://www-03.ibm.com/press/us/en/pressrelease/51712.wss (accessed on July 26, 2018)

78. Manuj I., Mentzer J. T. (2008). Global supply chain risk management. Journal of Business Logistics, 29(1), 133–155.

79. Baird I. S., Thomas H. (1991). What is risk anyway? Using and measuring risk in strategic management. In R. A. Bettis, & H. Thomas (Vol. Eds.), Risk, strategy and management: 24. Connecticut: Jai Press Inc.

80. Svensson G. (2000). A conceptual framework for the analysis of vulnerability in supply chains. International Journal of Physical Distribution and Logistics Management, 30(9), 731–749.

81. Kshetri N. (2018). Blockchain's roles in meeting key supply chain management objectives. International Journal of Information Management, 39, 80-89.

82. Francisco K., Swanson D. (2018). The supply chain has no clothes: technology adoption of blockchain for supply chain transparency. Logistics, 2(1), 2.

83. Provenance Has a Big Year Ahead Delivering Supply Chain Transparency with Bitcoin and Ethereum. International business times. Available online:

http://www.ibtimes.co.uk/provenance-has-big-year-aheaddelivering-supply-chain-transparency-bitcoin-ethereum-1537237 (accessed on July 26, 2018).

84. Roberts J. J. (2017). The diamond industry is obsessed with the blockchain. Fortune. Available online: http://fortune. com/2017/09/12/diamond-blockchain-everledger/ (accessed on 13 September 2017).

85. Burgess K., Singh P. J., Koroglu R. (2006). Supply chain management: a structured literature review and implications for future research. International Journal of Operations & Production Management, 26(7), 703-729.

86. https://www.inttra.com/assets/documents/ced97146-272c-436e-8c54-131313915625.pdf (accessed on July 26, 2018)

87. https://www.accenture.com/us-en/blogs/blogs-blockchain-can-drive-saving (accessed on July 26, 2018)

88. IBM, (2017). Maersk and IBM Unveil Supply Chain Solution on Blockchain. I. Available at: https://www03.ibm.com/press/us/en/pressrelease/51712.wss (accessed November 13, 2017).

89. Bajpai P., (2017). How IBM And Maersk Will Use the Blockchain To Change the Shipping Industry. NASDAQ.com. Available at: http://www.nasdaq.com/article/how-ibm-and-maersk-will-use-theblockchain-to-change-the-shipping-industry-cm756797 (accessed on July 26, 2018).

90. Fürstenberg S., (2017). Fleet Transformation: What blockchain can really do -. Fathom News. Available at: http://www.fathom-news.com/fleet-transformation-blockchain-can-really-2/ (accessed on July 26, 2018).

91. Seebacher S., Schüritz R. (2017). Blockchain technology as an enabler of service systems: A structured literature review. In International Conference on Exploring Services Science (pp. 12-23). Springer, Cham.

92. World Bank, (2002). Transport services: Reducing barriers to trade. Global Economic Prospects. Available at: http://siteresources.worldbank.org/INTGEP/Resources/3353151257200370513/04--Ch4--96-127.pdf (accessed on January 14, 2018).

93. Zeng X., (2017). HMM completes first blockchain pilot voyage. Fairplay IHS Markit. Available at: https://fairplay.ihs.com/container/article/4291331/hmm-completes-first-blockchain-pilot-voyage (accessed on January 15, 2018).

94. https://lloydslist.maritimeintelligence.informa.com/LL111275/HMM-completespilot-blockchain-voyage-with-reeferladen-boxship (accessed on January 15, 2018).

95. Di Gregorio R., Nustad S. S., Constantiou I. (2016). Blockchain adoption in the shipping industry.

96. Terna P., Maggiora M., Battistoni L. (2016). Emerging cryptocurrency trust in an agent–based model."

97. Jones, H. (2016). Broker ICAP says first to use blockchain for trading data. Reuters, London, 15 March 2016. Http://uk.reuters.com/article/us-icap-markets-blockchain-idukkcn0wh2j7

98. Valenzuela J., Arcade City (2016), Ethereum's Big Test Drive to Kill Uber. The Cointelegraph. Http://cointelegraph.com/news/arcade-city-ethereums-big-test-drive-to-kill-uber

99. Heath B. L., (2010). The history, philosophy, and practice of agent-based modeling and the development of the conceptual model for simulation diagram.

100. Wilensky U., Rand W. (2015). Introduction to Agent-Based Modeling: Modeling Natural, Social and Engineered Complex Systems with NetLogo. Cambridge, MA. MIT Press.

101. Resnick M., Wilensky U. (1993). Beyond the deterministic, centralized mindsets: New thinking for new sciences. In annual meeting of the American Educational Research Association, Atlanta, GA.

102. Merkle R. C., (1987). A digital signature based on a conventional encryption function. In Conference on the theory and application of cryptographic techniques (369-378). Springer, Berlin, Heidelberg.

103. Bayer D., Haber S., Stornetta W. S., (1993). Improving the efficiency and reliability of digital time-stamping. In Sequences II (pp. 329-334). Springer, New York, NY.

104. Feller W. (2008). An introduction to probability theory and its applications (Vol. 2). John Wiley & Sons.

105. Rosenfeld M. (2012)., Analysis of hashrate-based double-spending URL: https://bitcoil. co. il. Doublespend. pdf.

106. Decker C., Chapter 8. (2016). On the Scalability and Security of Bitcoin. Available on: https://www.researchcollection.ethz.ch/bitstream/handle/20.500.11850/114732/eth-48881-02.pdf

107. http://blog.clientsfirst-ax.com/blog-1/how-much-is-erp (accessed on July 26, 2018)

108. http://esotera.eu/clients-explorers/ (accessed on July 26, 2018)

109. Grunspan C., (2017). The Mathematics Behind Bitcoin, Double Spend Race Available online on: http://freeofread.com/download/haber-and-stornetta-at-at-t-bell-labs-anf-autoridad-de/ (accessed on July 26,2018).

110. Johoe's mempool size statistics - 9/1/17 to 9/14/17, 2017. URL https://jochenhoenicke.de/queue/#all (accessed on July 26,2018).

111. Bitcoin charts & graphs - blockchain, (2017). URL https://blockchain.info/charts (accessed on July 26,2018).

112. Mubaslat J. S., (2018). Demonstrating the Functionality and Efficacy of Blockchain-based System in Healthcare Using Simulation Tools (Doctoral dissertation, Wright State University).

113. Tremblay K., Lalancette D., Roseveare D. (2012). Assessment of higher education learning outcomes. Feasibility study report, 1.