Modernization of Land Registry
by Adapting Blockchain with Proof-of-Work (PoW)

by

Sabrina Israt Mostofa
16101057
Tasin Mahmud
16101290
Bivor Faruque Adrito
16101306
Tridiv Roy
17101260

A thesis submitted to the Department of Computer Science and Engineering
in partial fulfillment of the requirements for the degree of
B.Sc. in Computer Science

Department of Computer Science and Engineering
Brac University
December 2019

Declaration

It is hereby declared that

1. The thesis submitted is my/our own original work while completing degree at Brac University.
2. The thesis does not contain material previously published or written by a third party, except where this is appropriately cited through full and accurate referencing.
3. The thesis does not contain material which has been accepted, or submitted, for any other degree or diploma at a university or other institution.
4. We have acknowledged all main sources of help.

Student's Full Name & Signature:

Sabrina Israt Mostofa
16101057

Tasin Mahmud
16101290

Bivor Faruque Adrito
16101306

Tridiv Roy
17101260

Approval

The thesis/project titled “Modernization of Land Registry by Adapting Blockchain with Proof-of-Work (PoW)” submitted by

1. Tridiv Roy (17101260)
2. Sabrina Israt Mostofa (16101057)
3. Tasin Mahmud (16101290)
4. Bivor Faruque Adrito (16101306)

Of Fall, 2019 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science on December 24, 2019.

Examining Committee:

Supervisor:
(Member)

Mahbubul Alam Majumdar, PhD
Professor and Chairperson(CSE), Interim Dean, School of Sciences
Department of Computer Science and Engineering
BRAC University

Program Coordinator:
(Member)

Md. Golam Rabiul Alam, PhD
Associate Professor
Department of Computer Science and Engineering
Brac University

Head of Department:
(Chair)

Mahbubul Alam Majumdar, PhD
Professor and Chairperson(CSE), Interim Dean, School of Sciences
Department of Computer Science and Engineering
Brac University

0.1 Abstract

All over the world land registry is a big problem which needs to be addressed. In order to bring this process in a more secured and trusted state, a systematic way has to be implemented. To eradicate the issue, blockchain can play a vital role. Blockchain is a revolutionary technology which has emerged recently. It is well known for its broad implication for securing and authenticating data at a unique way. In this paper a new system has been proposed which will bring the land registry system in a process where every transaction will be recorded within a new block. This block will be created through a selected miner. The miner selection will be done through a consensus algorithm known as Proof-of-Work. All the blocks will be connected with each other with the help of the hash of previous block. This will not only make the connection between two blocks but also make the system more secure and reliable. This hash code will be generated using SHA256 hashing algorithm with the help of Elliptic Curve Digital Signature Algorithm. This distributed ledger will keep track of land ownership. The system will keep track of any ownership changes in the ledger. There will be option for purchasing of land directly in the system so that no need of any third party transection. When all the requirement is met, the transaction will be enlisted and new chain will get distributed among all the nodes. As long as digital signature of a chain of the nodes matches with more than 50% of other chains of other nodes, it is accepted and kept. Whenever a version of the chain with different digital signature emerged in the system, it will be rejected after the checking is completed. This will prevent any manipulation and fraud attempt by unauthorized entity. Based on these, the paper will show a demonstration of a modernized system which can solve existing problems in land registry sector with the help of blockchain technology.

0.2 Keywords

Blockchain, Hybrid, Proof of Work, ECDSA, SHA256, Land registry

Table of Contents

Declaration **i**

Approval **ii**

Abstract **iii**

0.1 Abstract . . . iii

0.2 Keywords . . . iii

Table of Contents **iv**

List of Figures **vii**

Nomenclature **vii**

1 Introduction **1**

2 Literature Review **3**

3 Blockchain Technology **8**

3.1 What is bloackchain? . . . 8

3.2 Characterstics of Blockchain . . . 9

3.2.1 Shared databases . . . 9

3.2.2 Multiple writers . . . 9

3.2.3 Distributed trust . . . 9

3.2.4 Disinter mediation . . . 9

3.2.5 Transaction dependency . . . 9

3.2.6 stamping of time . . . 10

3.2.7 Rules of Transaction . . . 10

3.2.8 Validation . . . 10

3.2.9 Scalability . . . 10

3.3 types of blockchain . . . 10

3.3.1 Public blockchain . . . 10

3.3.2 Private blockchain . . . 12

3.3.3 Hybrid blockchain . . . 14

3.4 Process of transaction . . . 15

3.5 Hashing in blockchain . . . 20

4 Consensus Algorithm 24
4.1 Proof of Work 25
4.2 Proof of Stakes 26
4.3 Practical byzantine fault tolerance 27

5 Elliptic Curve Digital Signature Algorithm 28
5.0.1 Key generation 29
5.0.2 Signature generation 29
5.0.3 Signature verification 29

6 Land Registration principles 30
6.1 principle of specialty 30
6.2 Principle of booking 30
6.3 Agreement principle 30
6.4 Publicity 30

7 Functionality of proposed model 32
7.1 used libraries 32
7.1.1 Python Flask Library 32
7.1.2 Hash lib library 33
7.1.3 The json library 34
7.1.4 URL parsing library 34
7.1.5 Request library 35
7.1.6 ECDSA library 35
7.2 Code Description 35
7.2.1 __init__ (self) 36
7.2.2 create_block() 36
7.2.3 create_land_block() 37
7.2.4 mine_block() 37
7.2.5 add_transaction() 37
7.2.6 get_previous_block() 37
7.2.7 proof_of_work() 37
7.2.8 hash() 38
7.2.9 id_chain_valid() 38
7.2.10 add_node() 38
7.2.11 replace _chain() 38
7.2.12 search_land_hole() 39

8 Methodology and Novelty 40
8.1 workflow 40
8.1.1 Blockchain and attributes 40
8.1.2 User Land registration Process 41
8.1.3 Land Buying process 41
8.1.4 Signature key generation and verification 42
8.1.5 Miner selection process 42
8.1.6 Block generation 43
8.2 Outcome 43
8.2.1 Computational power of miners 45
8.2.2 Outputs of the system 45

8.3 Comparative Analysis 49
8.3.1 RSA vs ECDSA 49
8.3.2 Proof-of-Work (PoW) vs other consensus algorithm 50
8.4 Distinctive Feature 51

9 Future work and Conclusion 52
9.1 Future Work 52
9.2 Conclusion 52

Bibliography 55

List of Figures

3.1 representation of public blockchain 11
3.2 representation of private blockchain 13
3.3 representation of hybrid blockchain 15
3.4 initial block of the process 16
3.5 Hash generation of a single block 17
3.6 Hash of second block 17
3.7 Hash of consecutive block 18
3.8 Altered Hash of a block 19
3.9 Altered Hash of another block 20
3.10 Storing hash for each consecutive blocks 21
3.11 Creation of nonce by the miners 22
3.12 Generation of blocks one after another 23

4.1 types of consensus algorithm in blockchain 24
4.2 Proof of Work block diagram 26

5.1 Arithmetic operations in Elliptic Curve Cryptography (ECC) Hierarchy 28

7.1 Difference in data before and after hashing procedure 34

8.1 Blockchain and attributes 40
8.2 Land registration process 41
8.3 User registration process 41
8.4 Land buying process 42
8.5 Sign key generation and verification from ECDSA 42
8.6 Miner selection process 43
8.7 Blockchain formation process 43
8.8 Block generation graph 44
8.9 Miner computational power 45
8.10 Transaction blockchain 46
8.11 Miner blockchain 47
8.12 Registered land blockchain 48
8.13 Main chain List 49
8.14 Elliptic Curve for Digital Signature Algorithm 50

Chapter 1

Introduction

The land management system follows ancient and outdated guidelines. Maximum of these rules were in vogue from the ancient time. There are a number of flaws, corruptions and loopholes. Because of land officers, revenue collectors and surveyors on whom these old traditional method relies, are responsible for the exploitation. There are many loopholes which give opportunity to create false data thus making the land owners vulnerable to bribe the authority in order to keep proper records of their lands. Other than this, many of the registrars, revenue workers and surveyors covertly cajole squatters to snatch the land of weak, helpless owners. With the proper modification of the fundamental structure of land supervision, appropriate handling of land ownership, registration, relocation and other lawful paper work can be possible. For this reason this paper came up with a solution to reduce land management issues with the help of blockchain technology.

Blockchain technology – that cryptographically secures documentation of transactions, is an excellent type of distributed ledger. It is renovating the making and storing of data. From time to time, same type of alterations of records, data creation, recordkeeping and applications have in the practice of storing records, for the reason that these variations required contrasting methods to preservation. Blockchain is basically one sort of distributed ledger system that authorized sets of transaction storage which teamed into blocks, which are then linked together cryptographically, authenticated and broadcasted via a p2p mesh network [1]. These set of operation and structural design is said to give accuracy of transaction data, which answers a vital issue: the trust issue. Trust is required to start any communication. Cryptographic security of datasets and dispensing copies that might be matched, it is likely to validate, secure and protect the reliability of data as a vital features required to make us believe the system. Reliable information is a significant basis for different types of believe, like the faith between public and nation, communicating system or corporate deals. This aptitude to offer a basis for faith is what makes blockchain technology different from all other technologies and stands out as a unique invention Clearly, the Blockchain technology is suitable for the management of land registry. Blockchain's functionality possibly be termed as a distributed ledger. This has the similar purpose by way of a good property registry method: this identifies who is the owner of what at a particular time. It can say when a particular transaction happened. It is not impossible to' track back' and hence the title is guaranteed. Blockchain may even provide some extra clarity compared to a' typical land registration system.' Because of the shared servers, back-ups are secure. Added by cryptographic evidence and a decentralized database trust. It may also be used as a substitute to the conventional Land Registry methods. Due to its transaction dependence, it is impossible for someone who is not owner to exchange ownership in the Blockchain. Ownership checks are spontaneously performed by means of the laws of transaction dependence also the transfers. While the Registrar carries out ownership searches in the present Land Registry schemes, mostly by matching this data to the land registry material in person and scrutinizing the deed. This means that in most situations the seller's information listed in the contract is matched in person with the current owner's information in the land registry.[1]

Chapter 2

Literature Review

Current land registry system in our country is not transparent at all. The general people hardly have any access to it. As a result, many people are becoming subjected to fraud. Moreover, if a person wants to gather information while buying or renting a land in the country, he has to go through a lot of complex and complicated processes. When a consumer wants to access any information he has to go from person to person and table to table in land registry office just to get even a minimalistic data regarding a land such as who is the actual owner of that land. Sometimes this information has to be collected through third party agent for which one needs to spend more money than he should. Apart from this, the amount of time usually being wasted in the process knows no bound. In the current system of land registry there is also problem of redundancy. Same information has to be kept in many file in the land registry office.

In a study, it states that counterfeit of property papers is a key difficulties encountered by a administration for the land registration method. Albeit the information at present are protected inside the database but because of lack of security and time-stamping in the database system these data can be altered. To come out from the situation, Blockchain can organized the use case. As a distributed method, everyone can avail the information in the network in the blockchain. The block which are new in the system are time stamped, making the documents very rigid to be changed since to add new block proof-of-work is essential. In that article, the use-case of land registry entails copying the records into a blockchain and validating them with the one held in an electronic locker, thus, the falsification of documents. [2]

Another paper suggested, they need to take into consideration that the Bitcoin blockchain space is a scarce and precious resource, thus it cannot be used for issuing random information. Instead of that, information will be hashed and embed those hashes into transactions. Data itself can be attained from a party which generated it, i.e. the registry. This way we still get a consensus over what data was published, but only as long as registry is available and can provide information.[3]

The developers of the blockchain technology have asserted on two main advantages. They are- Since it is a decentralized system each node holds all the information and anybody can view the data at anytime and maintain a copy of the blockchain by downloading the protocol. It is said that this form of blockchain is transparent because it is available to all, not because of any interaction or government involvement. But private blockchains are likely to be established with restricted access and the number of miners restricted. The technological solution to some challenges could be this new opportunity. These are: First, with the aim of becoming a miner, the amount of nodes possibly will become restricted and a special requirement may be required. We execute their role as the blockchain's registrars. Second, mining would not be a computational quest, but another method that would include thorough and functional transaction analysis. Third, the nodes do not need to collect all the data. As it would be scattered and dispersed in separate locations, data will not be consolidated. Lastly, according to the fundamental law of each country, the right to use all the material could be limited. For example, information under German law62 would be restricted for everyone except for the person who has a genuine reason to search for data. Whereas the process will be available in compliance with Austrian law61, and anyone can obtain information. In any case, the name recording devices are both.[4]

This paper inspired by the a paper that states that ,Blockchain has been titled as the future of land registration. Documents delivered at the World Bank Conference on Land and Poverty held in Washington D.C. in early 2016 endorsed the idea as permitting for "distributed" registries, righteous, most importantly, removing the middleman out of the transaction, allowing "peer-to-peer" direct transactions. That papers promote such a system would enable important savings in transactional charges.[5] To make land registration system in Kenya digital, Kenya's government spent a lot. It is because to face challenges in the registration system and promote an economic balance throughout the country by handling transaction and management.[6]

The Sweden government's estimations are that the land registry using blockchain project can save over $106 million USD of tax payers per year through eradicating paper-work, decreasing scam, and rapid the process.[7] Statistics shows that, in India more than twenty million rural families do not own and have legal ownership of the land that they live in.[8] Blockchain suggests a wide range of common technological works which includes interchange data also transaction of digital properties in distributed systems.[9]Blockchain technology is a remarkable method to offer a joint basis in order to transact data of transmitting value.[10] There are some aspects which form a blockchain technology that contain: trusting the system than middleman; public key and cryptography; an absolute feature of trusting the ledger and decentralization that ensure information is secured even when one node goes down.[11] The blockchain is known as a distributed ledger and is consists of several data "blocks," individually represents a definite amount of transactions. Hence creating a digital storehouse of each transaction that accomplished in that system.[12] It can be said that the most of the core countries of the world are getting benefitted from the blockchain technology using it in multiple sectors.[13] After researches Blockchain technology is helpful to be used to eradicate issues which includes data reliability at recent times and near future, with its appropriate architecture and infrastructure management.[14] Blockchain has been titled as the future of land registration. Documents delivered at the World Bank Conference on Land and Poverty held in Washington D.C. in early 2016 endorsed the idea as permitting for "distributed" registries, righteous, most importantly, removing the middleman out of the transaction, allowing "peer-to-peer" direct transactions. That papers promote such a system would enable important savings in transactional charges. The blockchain technology proposes an exceptional method of distributed authentication that does not count on a fundamental authority. They contemplate this system against outdated governance methods. They validate their argument by paying distinguishing attention to blockchain based authentication functions in the domain of land registry systems all over the world. From the discussions with legislatures from organizations installing blockchain, they maintain traditional governance ideal sorts against what the rivalry that blockchains and cryptocurrencies bring to digital settings. After declaring to hierarchy, market, network they undertake outlining the predictions of a blockchain associated governance approach called 'tribal' that states the closeness that contention initiated.

A country in West Africa, the blockchain set up is a component of a general state digitisation initiative that targets at creating a completely unique eco-system, linking notaries, investors, and voters. Land records uncertainty and exploitation have encouraged this initiative. Their execution partner is dynamic in further than five countries and keeps further than one thousand land records and transaction at the time of writing. This blockchain-based resolution is quite innovative: it validates transactions with proof-of-stake that is faster and cheap than Bitcoin's mining-intensive proof-of work. It additionally links its own tokens to each permissioned and permission less blockchains to influence their completely different properties. In reality, to ensure the system's elasticity against interfering, every token is connected to Bitcoin blockchain, whose scale guaranties proof-of-existence and a storage chain, whenever to except authentic records. Responsible for data entering is a partnership between state authorities and notaries, who can also modify claimed argumentative information and therefore acts as a sole point of truth. The verification of records therefore partly depends both on open infrastructures and native actors (both state and private). [15]

Land registries wide-reaching are fascinated by blockchain technology, as it can manage governing requirements, asset allocations and financial dealings and it has the ability to transform land allocation. Blockchain can be said as the future of land registries because of the significant profits it proposes which are- blockchain increases transparency, offers accurate, precise and trusted property records, safeguards the proprietorship of all registered assets, decreases cost, quick processes , instead of taking months and weeks, the process only take few hours, delivers solid auditability, provides a dispersed system to support disaster retrieval, permits public to trade properties distantly, shrinks paperwork, helps to build smart process, removes potential deception, make easier, quicker and cheaper land registry facilities.[16]

Blockchain technology assure to face security trials in IoT supported facilities for example allowing protected information distribution and records reliability.[17]

This paper emphasize more on using blockchain for land registry after the Honduras situation. Some researcher researched over the situation of Honduras and suggested using blockchain for their land registry. They stated the property rights safety system in Honduras did not pass. The judicial system and state Property Institute has proved their incompetent to provide a protected and crystal clear land registry, to inspect and accurately prosecute crimes containing land, offer an efficient, fair and autonomous court process, and to protect arbitrary and unlawful invasions or property burglary. Assigning a blockchain backbone to the facility Honduran public institutions provide, will help reinforce each one of the weaknesses they have or facing. Firstly, it will offer an absolute and protected software for the registration of land property and other activities. Next, to boost the governments capabilities to investigate criminal invasions against property, the "Proof of Process" and "Proof of Existence" structures of Factoms decentralized blockchain based system will give an accurate, confirmable, and absolute audit trail . Third, the rulings of the judiciary will become more reliable. The Honduran legitimate system, all public papers (those emitted by public institutions), gets a presumption of good faith; which is, they should be documented as honest by the judiciary, except one of the sides can efficiently validate they are not. The difficulty is that, as they detailed earlier, a lot of the exploitation about land registries essentially comes from inside the offices of the Property Institute. The same thing occurs with Notary papers that have been one of the significant tools used to change the divisionary lines of private land properties and which are illicitly recorded in the Property Institute. Due to the great trustworthiness of the blockchain technology, the "Proof of Existence" and "Proof of Process" will made up with scientific proof which can expose and lawfully surpass any deceitful and deployed land titles in court.[18]

According to The World Bank (2014), 63 percent of the population in Honduras is existing under poverty. In rural zones, approximately 6 out of 10 families living under excessive poverty or on less than US dollar 2.50 per day. Per se, those in extreme poverty and those said to be in the rural deprived in Honduras, are mainly struggling farmers and agricultural workforces. The lack of human and few agricultural production, financial property and capital have been steadily marked as the core causes for rural poverty in Honduras. Researches on the land market and rural poverty in Honduras directed by the United States government have marked that with insecure contact to land, the poor will not be capable of increasing productivity and receive bigger profits or it can be said earn some profits of unblemished property rights comprising: a decrease in clash, amplified entree to credit, reduced land market transaction prices and better investments on the land property. Those consequences, would convey more and more effective distribution of land property, a reduction in poverty and a better productivity. They mention, private property land lease in Honduras is acomes with a great significant amount of insecurity, threat and uncertainty. As a consequence, there are solid reasons in contradiction of investing or permitting credit to plans in rural areas; that in fact styles it stiffer to interrupt the poverty cycle. Fundación Eléutera will carry on operating carefully with blockchain companies to apply the blockchain technology in Honduras, either inside ZEDE establishment or on the nationwide system, as it has been precisely planned for a solution for the earlier stated issues. Only a trustworthy, unchangeable, protected and translucent, easy to use and little priced property registry system can offer the basis for a gigantic labelling and registration for land ownership. Such a method will significantly diminish the uncertainty of proprietorship and risk of land burglary by the changing or modifying of public records. It is to assume that an enhancement of assurance in the property rights safety system of cities and rural land will also convey out a boost of really desired investment in Honduras. Land naming and larger entree to credit have been acknowledged as crucial components to enable citizen in developing countries. Peruvian economist Hernando de Soto has enlightened us for several years, that land naming reforms help the poor in a significant manner, allowing such chances as access to credit, the formation of systems of documentation, the formation of systems for insurance and credit data, the provision for housing, infrastructure and other establishment, the issue of stocks, the mortgage of land and a host of additional economic deeds that initiate a up-to-date market economy. In his 1999 research, Development as Freedom, Nobel laureate Amartya

Sen highlighted that one of the most vital features of development is freedom of opportunity, a crucial section of which is access to credit and capital. Since property rights are protected, and therefore grander contact to capital and credit gets accessible, market situations will permit for bigger investment in capital properties, that by the way will increase agricultural productivity and consequence greater pay for the public who required it best. Thus poverty decreases in rural areas.[18]
Blockchain is not only for record keeping of land transaction at all. It is also used for health records, different type of government records securely.[19] On the other hand, another paper is against the the thought of using blockchain in land registry system. Their point is discussed below- Blockchain systems are said to be unsuitable for use in real property rights transaction, that is on a traditional law structure. The blockchain concept may consider to be a helpful for vehicle, helpful for allocation of lawful title to small worth properties, or resources with a narrow shelf life, none of that has an exceptional feature.
Nevertheless, actual property transactions do not fit within this features. Later presenting what all understand the mechanisms of a blockchain system to be, thought is asserted to its practice for the transaction of lawful designation to both tangible and intangible properties. This empowers people to well frame and realize the problems that then appear when people pursue to operate blockchain methods for real property rights transaction process, they become tangible or intangible in nature. The unsettled concerns that appear from this, make it compulsory to create who conveys the threat if a transfer does not go right. These varieties seem to be the users or the controllers of the system. If a familiarized system has to completely leave from the life of people who recognize to be main indicia of a blockchain with the intention of securely operate in a reliable method, it will not be called a blockchain system. If such leavings are unavoidable one should leave the descriptor of the method being ‘blockchain’ in nature. Constant use of this word is deceptive and will only result in greater misconception about what is the meaning of the term blockchain system. This paper understand their thought but will refute their thinking with proper discussion and proof. [20]

Chapter 3

Blockchain Technology

3.1 What is bloackchain?

Blockchain refers to a digital registry or log of economic transactions, a list of continuous records in blocks. It is continuously updated many people and also fully public. It is considered as impossible to corrupt by many people. It is one of the most controversial and also most popular topic among the technology leaders. Blockchain, similar to the Internet, which is an exposed, open and also a global structure that lets corporations as well as persons manufacture businesses to leave out the distributor, decreasing the rate of dealings and the period delay from being occupied by middle parties. This equipment is centered on a distributed record as well as consensus procedure. This equipment permits a digital record book of dealings (in this case land dealings) to be formed and also communal concerning all the nodes on a system. The record is never maintained nor organized by one central consultant and it can also be verified by every entities of the framework. If any operator needs to record a deal to the record book, when any operation is occurred it is encoded as well as finalized by other nodes by means of cryptographic algorithms. When there exists harmony among most of the nodes or users that the operation is legal then one fresh block of entry is included into the chain of blocks which is public to all the nodes of the system. Deals or the transactions are protected, confidential and auditable. There are two types of records containing in a blockchain database transaction and blocks. There is also a possibility of programming a blockchain to record the transaction automatically. Blocks are always time stamped and linked to the upcoming and previous blocks. Each block holds transaction batches. The transaction cannot be altered with.[21]

Whenever any two members of the network (nodes) transact they give an announcement of their transaction to all the nodes of the network. The transaction then recorded in a limited capacity block. Once a block completes its necessary credentials it starts preforming Proof-of-Work that are combination of hard to decipher mathematical operations. This operations are hard to decipher but easy to verify the correct solution. These mathematical operations force the verification of nodes. The nodes verification will be dissipated if it includes illegal dealings. The part, which prospers in deciphering Proof-of-Work, it announce the answer among through the transaction blocks, to every nodes. This is the essence of bitcoin in blockchain solution.

The distributed blockchain operations are completely based the deciphering of the

Proof-of-Work. By using this mechanism, Bitcoin has accurately recorded in almost 8 years more than 140 million transactions occurred.
Through 2013, more than a few suggestions along with a few firms were encouraging the impression of trying blockchain technology devoid of a digital crypto exchange behind it. Fashionable those ‘permitted blockchains’ solitary approved participants may obligate information from the blockchain, which is a common record among altogether contributing parties. Still, there is no existence of commercially established blockchains, nevertheless there are numerous well-publicized models as well as proposals.[[22]

3.2 Characterstics of Blockchain

The wonder called blockchain some characteristics:

3.2.1 Shared databases

: In the world of blockchain and also land registry system it is a good practice to use one and only source and one database with some back-up data. A blockchain is a collective record, copied on numerous files which are all linked with each other.

3.2.2 Multiple writers

: There can be multiple writers working on a chain simultaneously. All the operation in a blockchain could be put in respective versions of the folders. This case of Land Registry and Registers of Land, this operation can be modernized in one process. However, a replica of the operation could be kept in the database of the back-up arrangements.

3.2.3 Distributed trust

Blockchain can be defined as ‘shared single source of truth’. Dissimilar to the existing systems for Registry of Land where only the manager is reliable, we won‘t want to rely upon the management of a copy folder. As it was already backed up.

3.2.4 Disinter mediation

: In the current Land Registry systems we always have to put our trust in a third party that can only updates the registration. That is probable for anybody to retain replica of the folders and implement a operation on that folder

3.2.5 Transaction dependency

Blockchain is likely to generate the reliance on transactions, an operation can be completed if and only if all the dependencies are met

3.2.6 stamping of time

Blockchain has a possibility to firmly save the path of the modification also creation period of a transaction otherwise a document. Including the landlord of the land, no one is capable to alterating the components of the operation when it is kept, providing that, reliability of stamping of time is not ever bargained.

3.2.7 Rules of Transaction

From the traditional Registry system of Land structures the middleman or Land Register observe the validity of the transaction following some rules. However, in that structure human error can take place. To prevent any objectionable transactions taking place, by following some certain transaction rules block chain could be checked if the operation is legit.

3.2.8 Validation

As blockchain is a public register and unalterable and therefore incontrovertible. Blockchain logs all validate the transactions always in a sequence. In existing registry systems of land all the trades, part of a record also can be noticeable by means of some kind of authentication.

3.2.9 Scalability

Everybody who wants to keep or put his or her record to the chain of blocks could also do so. Which makes blockchain expandable simply.
From the above discussion it seems that, blockchain is an ideal and uniquely functioning system.[23]

3.3 types of blockchain

Whether, that could be certain whether blockchain could also be the finest option to preserve the system of land registry, there are several queries that needs to also be responded concerning to maintainance of such structure. However, firstly we have to answer the query that is whom will have to plan and also maintain the blockchain of land registry. Furthermore, the following question would be which format of blockchain to follow. Whether the blockchain would be public blockchain, private blockchain or a hybrid format blockchain [24]. In case of a public blockchain for Land Registry System, everybody should be able to connect the blocks also apply in the software. The max dependable claim of this blockchain technology is the security and safety obtainable by using the large number of computers. For the reason that it's globally obtainable to the public record keeper where the data is kept in the blockchain, it could be neither manipulated nor removed by anybody or any computer.

3.3.1 Public blockchain

If the private system of land registry could be substituted by a public system of blockchain any person will be able to learn about the data and learn the transactions of the blockchain[25]. That is in agreement from the existing condition in Bangladesh respecting the current systems of registry as anyone can gain knowledge concerning of a certain land and its transactions as well as the information of the current owner, nevertheless it is most likely not to match the systems of registry of land of various other countries. Furthermore, there is also potentials to not provide each data, every agreements, and actions are accessible for everyone. There was also possibility to generate privileges for every precise persons including so that only related information can be public. Furthermore, it is also possible to use a system which is privately administrated like. Moreover, there also exists the choice of generating the cross chain interchange between public as well as private blockchains for providing extra security and to make the user experience more convenient. By using these combinations as well as other combinations of public and private blockchains diverse types of hybrid blockchain arrangements could be created and released. Into open blockchain there is a scope participation in the consensus process by anyone in the world. It is possible to add to regulate what blocks get added to the chain and therefore which transactions is to add can also be regulated.

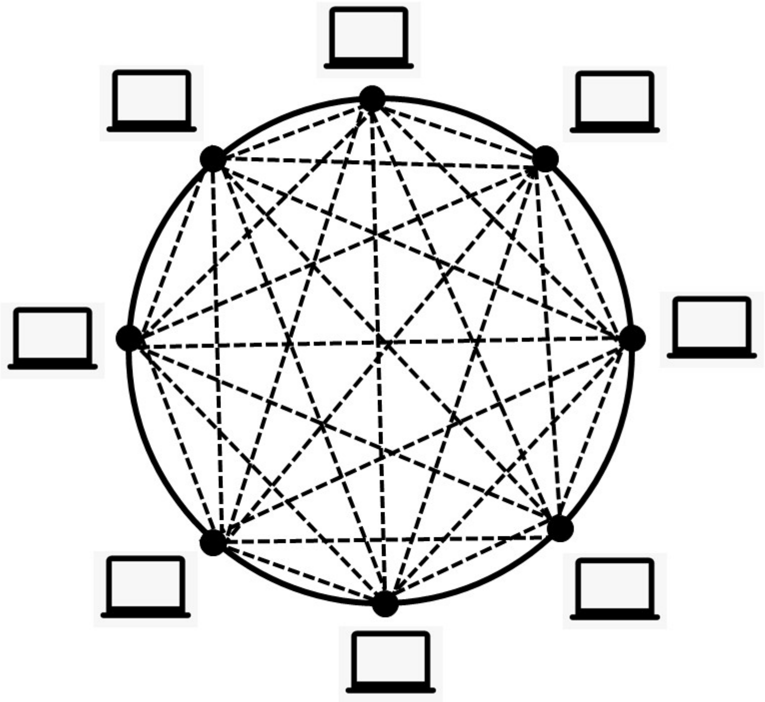


Figure 3.1: representation of public blockchain

The present position of possession of any land or plan is consequently a concern of the open as it is unrestricted. That provides a firm level of reliance to the users of the blockchain as the strongest point of the open system is the hopeless for the developers to create certain modifications in the chain. A deficiency of procedures associate unbiased privileges, high costs to validate properties, inefficiency of the bureaucracies taking years to accomplish basic tasks also general issues with poor authority could be the motives to conduct research on the possibility of blockchain for the establishment of a Land Registry system. It is certainly a question whether these modern techniques will actually help constructing a dependable and trustworty Land Registry system. It seems very alluring to use blockchain technology in less developed also developing countries where there might be a chance of having dishonest governmental parties, perhaps also conveyancers, surveyors and registrars. It is always likely to upload every first entry or the transaction directly into the blockchain once it is created. But then again the actual encounter on the nations appears to be the preliminary documentation of correct owners, details concerning their privileges, boundaries besides accountabilities. Additionally, determining also authenticating the geographic limitations must be comprehended in several cases. For these reasons many other possible resolutions may be more appropriate. Generally less developed countries has cheap land registry system, however it is firm and intended to encounter the needs of people. This expertise cannot always provide an explanation for any unavoidable party-political weaknesses also corruption, nonetheless by beginning to keep each stage like review and drawn from the tap titles in the blockchain, it could come in our advantage. When the blocks themselves are recorded, confirmable possession is recognized. As per mentioned, that could also be completed by applying diverse procedures, dependent on the situations.

3.3.2 Private blockchain

In case of a private Land Registry system using Blockchain, one unit uses the blockchain technology to record the transactions, overriding the fundamental principle of blockchain of the creation of distributed trust by using shared and common databases. In contrast, because of the less number of nodes, the validation rules can be adjusted easily. As being the only entity using the blockchain technology, consensus is met in an instance. This makes the system easy to use and very flexible. In the case of a private blockchain, there remains no fully public as well as controlled network that is secured by crypto economics (eg. Proof of work, Proof of stake).However, it is possible to create a system with more firmly controlled access permissions, alteration rights and permission to read. In the case of a private blockchain, permissions writing is kept centralized to mainly one organization. Reading permissions can be either restricted or public.

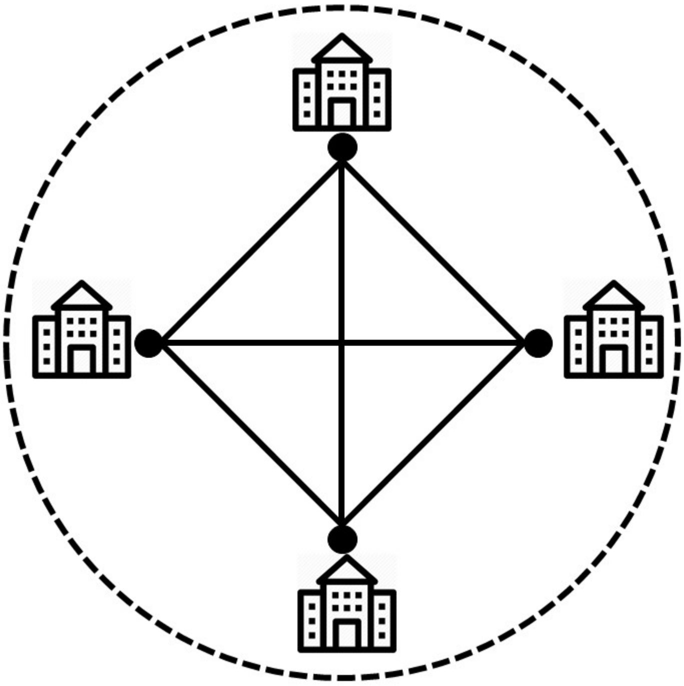


Figure 3.2: representation of private blockchain

Meanwhile the Land Registry system is kept totally open and available, in the case of the Bangladesh permissions would not need to be implemented. One of the benefits of a private blockchain is the possibility of reserving the transaction or changing the rules of the blockchain with comfort. This could be the case of great importance if, when a ruling of court would mean possession has to be transferred again or in case of the apartment rights do no longer exist and the plot or land itself has to 'revive' from an administrative point of view. The application of a private blockchain in the purposes of keeping the Land Registry system does not seem to have any added value. A new way of registration would have to be constructed and implemented. Furthermore, with regard to the number of transactions that has to be uploaded and verified on a daily basis, substantial computing power to mine has to be installed. Next to it, there is the similar risk of being hacked as in a traditional land registry system. Matching the transactions with a public blockchain, transactions are very low-cost in a private blockchain since they only need to be verified and confirmed by a few nodes that can be trusted. It is not completely certain that these costs are actually lower than the computing costs of a traditional Land Registry system. The only added value is the step of cryptographic auditability, though that can also be implemented in another way. A well-functioning Land Registry system comprises of a system of checking the balances. In general the documents are being checked by the registrars as they receive the documents from conveyancers in addition these conveyancers are checking the contents of the Land Registry system after updating. In fact, in Bangladesh, the registrars of the lands have to go through a process containing many stages to verify the land.

3.3.3 Hybrid blockchain

When Land Registry system is created using a hybrid Blockchain, the amount of units and peoples are part of the chain is limited. At this moment, Banks appear to working for a fusion(hybrid) form of Blockchain system where groups of banks will put their transactions into the blockchain to resolve inter-payment facilities. Similarity can possibly work for the blockchain for handovering property possession: verified registers would also work along with the administrators in registry system of land using this technology. It means that licensed or confirmed conveyancer can upload a record then the administrator will approve it. After it is approved plus the transaction is also checked, the record is reflected as complete. Similarly, the private blockchain system of land registry code for dispersed belief could be disheartened; consequently the chain isn't fully exposed for everybody. On the other hand, the registrars could make an distinguishable set also for that reason can make altercation over the directions for formating the record authenticity. Similar to this case every entities regarding chain implementing also applying fresh instructions in the same procedure. If traditional system for registry of land be swapped by using of a mix system blockchain, that is used by the fresh peoples concerning this blockchain for the transfer of the real estate, a part for the notaries also registrar, even parties that are providing the authorized dataset to record it to the registry folder. It is necessary that only the licensed registrars could verified by ID of concerned persons related to the business also by providing an electric ID by means of it uploading of transaction like, possession or a mortgage deed. The role of these entities should be measured. In such cases the position or role of the registrars could be down from a lawful expert in all kinds of facts, datas, figures and deed as well as any other sanctioned data to a expert with the IDs. Such cases registrars have to be contingent upon the capabilities as well as skill of the concerning peoples whom are including the record by themselves. An option might be the condition in which the conveyancers will be able to upload the record to the chain and the registrars will accept the certain record in the system. Furthermore, another way could also be the situation where the concerning people altogether the registrars will be able to make an association which tracks the chain. Conveyancers should be able put the concerning record along with registrars, both could also validate it. All of them together could control the system furthermore, definite number of entities must validate and sign each and every block so that the blocks are valid. There are also danger of an attack rising from some other entity in such a case collusion will not apply, as all managers are known to all, without this network of registrars will be endangered also the meachines could also be taken over by another entity of hackers however, they would be banned from watching the real lengthiest blocks. There is a chance of more risk if there are fewer nodes. There is a possibility to alter a block if there are more power of computation be able to used. The right to see or go through the chain might be open following the legal system. In many countries, this blockchain would be publically accessible, since the Land registers are open for everybody.

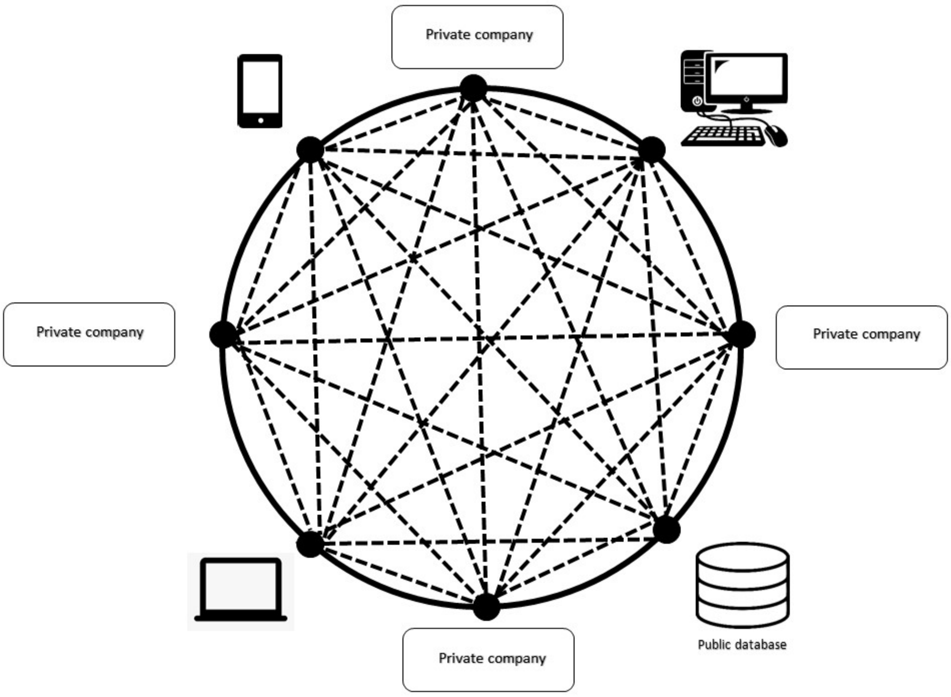


Figure 3.3: representation of hybrid blockchain

3.4 Process of transaction

Exactly when a block of data is associated to various blocks, its data can never be changed again. It will be straightforwardly open to any person who needs to see it once more, in absolutely the way where it was once added to the blockchain. That is exceptionally dynamic, since it empowers us to keep track records of basically anything we can consider (to give some examples: property rights, characters, money changes, therapeutic records), without being at risk for someone disturbing those records. For instance if an individual buy a house at the present time and incorporate a photo of the property rights to a blockchain, The individual will reliably and everlastingly have the alternative to show that he/she guaranteed those rights by at that point. It's impractical for anybody to change that piece of information when it is on a blockchain.

An exchange procedure of bitcoin blockchain is talked about beneath to see how an exchange occur in a blockchain framework:

The Bitcoin blockchain is the older blockchain in nearness. The blocks on the Bitcoin blockchain contain around 1 MB of data each. At the hour of creating it counts around 5 lac blocks, which implies roughly a total of 500,000 MB has been taken care of on this blockchain. The data on the Bitcoin blockchain just exists out of trade data concerning Bitcoin trades. It is a massive reputation of all the Bitcoin exchanges that have ever happened, right back to the absolute first Bitcoin exchange. In later part we shall get to know how a blockchain stores and exchange information, much the same as the Bitcoin blockchain

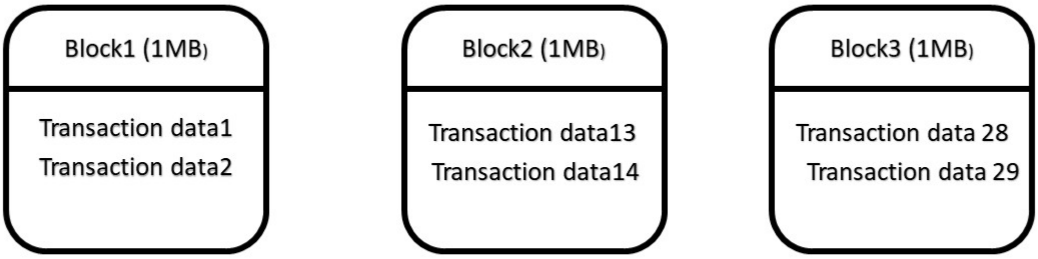


Figure 3.4: initial block of the process

In the above, there are three blocks, all containing some exchange information. Not exactly unique yet. We can balance it with some self-directed word reports or blocks that clarifies what trades have occurred and how these have influenced certain changes. In the block 1 would then consecutively clarify the principal trades that have occurred up to 1 MB, where after the upcoming trades would be represented in block 2 up to another megabytes (MB), and so on. These files are the blocks of data. These blocks are presently being associated (also called joined) together. To do this, each block gets a one of a kind mark that identifies with correct string of data in that block. In case anything inside a block changes, even just a sole digit change, the block will get new signature.

Assume block 1 registers two trades, trade 1 and trade 2. Imagine that these trades make up a total of 1 megabytes (MB) (when in doubt this would be significantly more trades). This block of data presently gets a mark for this specific string of data. Assume the imprint is 'X32'. Here is the thing that this looks like.

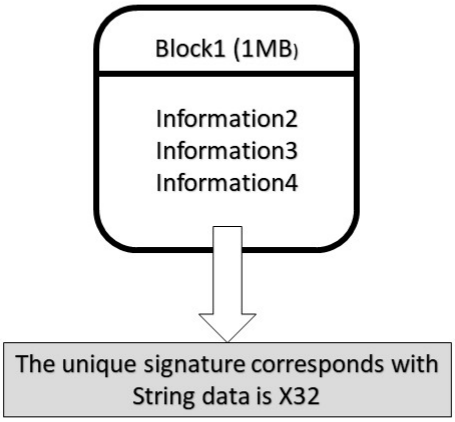


Figure 3.5: Hash generation of a single block

A single digit change of the data in block 1 would now cause it to get an absolutely uncommon mark. The data in block 1 is at present associated with block 2 by including the sign of block 1 to the data of block 2. The sign of block 2 is presently a degree to the characteristics of block 1, since it is recalled for the string of data in block 2. It looks like the figure given below.

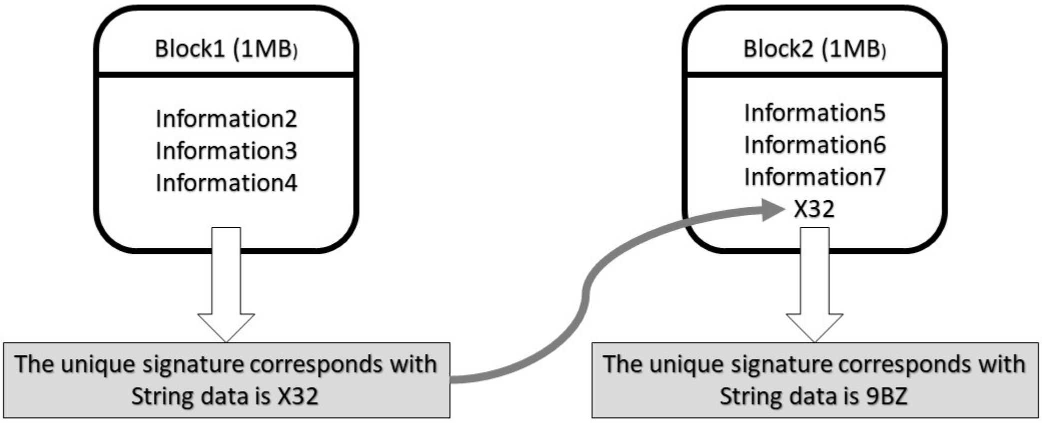

Block1 (1MB)
Information2
Information3
Information4
The unique signature corresponds with String data is X32
Block2 (1MB)
Information5
Information6
Information7
X32
The unique signature corresponds with String data is 9BZ

Figure 3.6: Hash of second block

The mark interface the blocks to each other, making them a chain of blocks. We picture adding another block to this chain of block 3.

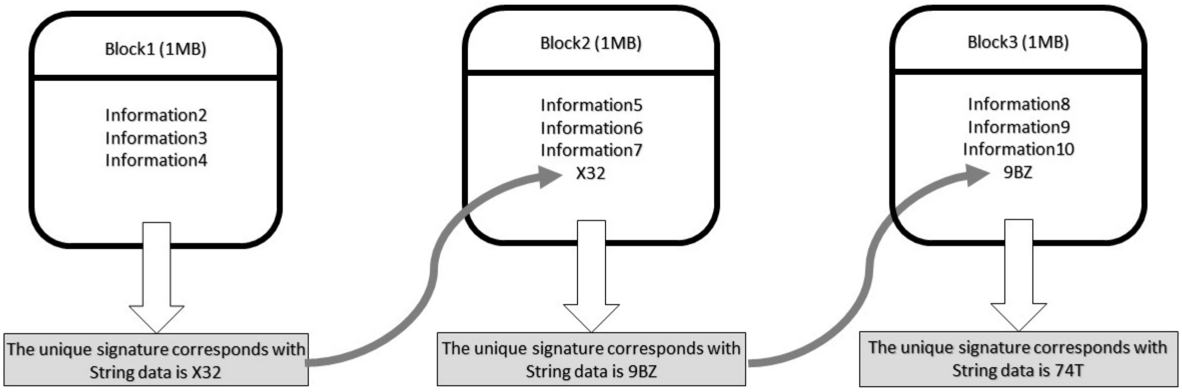

Block1 (1MB)
Information2
Information3
Information4
The unique signature corresponds with String data is X32
Block2 (1MB)
Information5
Information6
Information7
X32
The unique signature corresponds with String data is 9BZ
Block3 (1MB)
Information8
Information9
Information10
9BZ
The unique signature corresponds with String data is 74T

Figure 3.7: Hash of consecutive block

Now if the information in block 1 is modified. Suppose that the exchange among Person1 and Person2 is adjusted and Person1 gave 500 Bitcoin in place of 100 Bitcoin. The data of information in block 1 then gets changed, which means the block additionally gets another signature. The signature that relates with this new arrangement of information is no longer X32. Suppose it is currently 'W10.

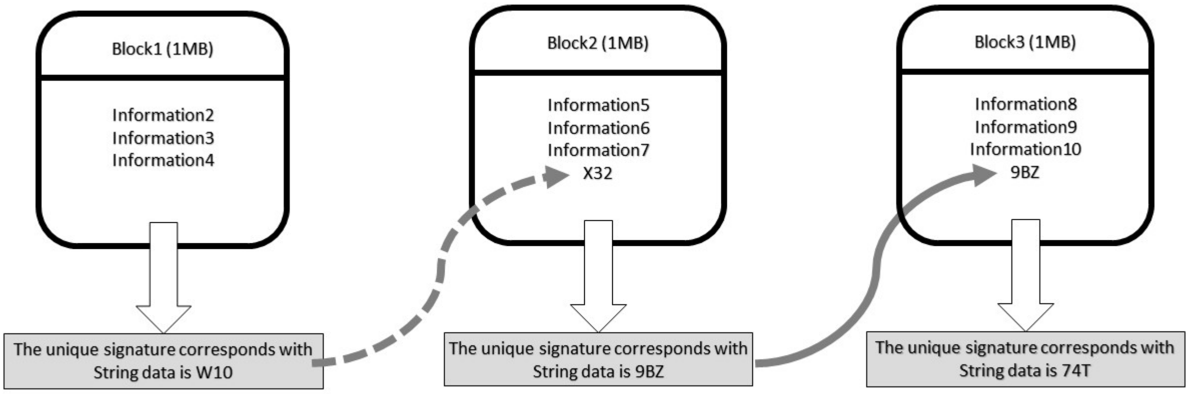

Block1 (1MB)
Information2
Information3
Information4
The unique signature corresponds with String data is W10
Block2 (1MB)
Information5
Information6
Information7
X32
The unique signature corresponds with String data is 9BZ
Block3 (1MB)
Information8
Information9
Information10
9BZ
The unique signature corresponds with String data is 74T

Figure 3.8: Altered Hash of a block

The mark W10 does not facilitate the mark that was recently summed to block 2 any longer. Block 1 and 2 are directly seen as never again secured to each other. This exhibits to various customers of this blockchain that a couple of data in block 1 was balanced, and considering the way that the blockchain should be everlasting, they discard this alteration by moving back to their previous record of the blockchain where all of the blocks are securely chained together. However the primary way that a change can stay undetected, is if all of the blocks remain secured to each other. This suggests for the change to go hidden, the new mark of block 1 must replace the previous one in the data of block 2. If in any case the data of block 2 is detected different, this will cause block 2 to have a substitute mark too. Assume the sign of block 2 is by and by 'PP4' as opposed to 9BZ. Then the block 2 and the other block 3 will never get attached together.

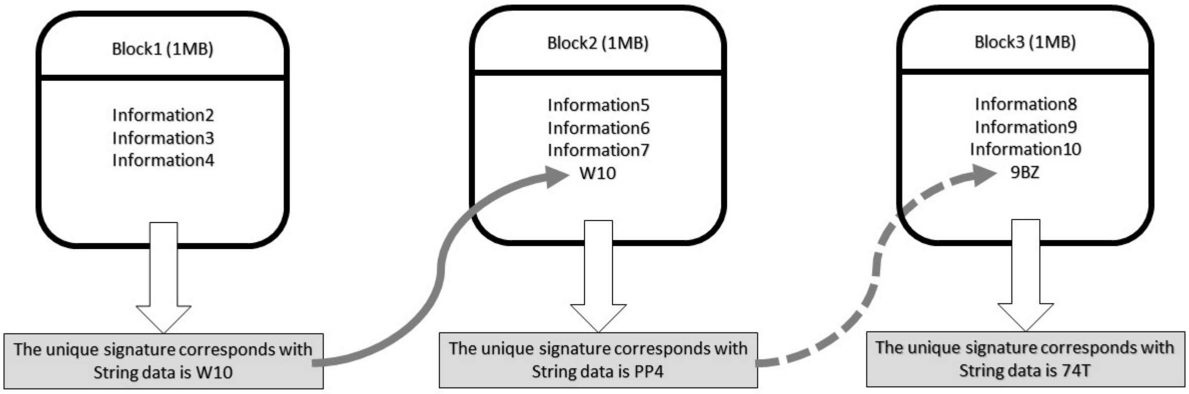

Block1 (1MB)
Information2
Information3
Information4
The unique signature corresponds with String data is W10
Block2 (1MB)
Information5
Information6
Information7
W10
The unique signature corresponds with String data is PP4
Block3 (1MB)
Information8
Information9
Information10
9BZ
The unique signature corresponds with String data is 74T

Figure 3.9: Altered Hash of another block

The blocks on a blockchain are openly accessible to anybody. Along these lines, if a modification should remain hidden inside the blockchain, every one of the blocks is supposed to remain appropriately tied (generally individuals can express that specific blocks do not appropriately connection to one another). This implies modifying a solitary block requires another mark for each other block that comes after it right to the finish of the chain. This is viewed as close to unimaginable. So as to get why, you should see how the marks are made.

3.5 Hashing in blockchain

A cryptographic hash work is an extremely complex way that takes any string of data and transforms it into an exceptional 64-digit string of yield. For every new input a new hash will get generated. In the following we can see a hash of block 1 is generated and it is saved in the block2.

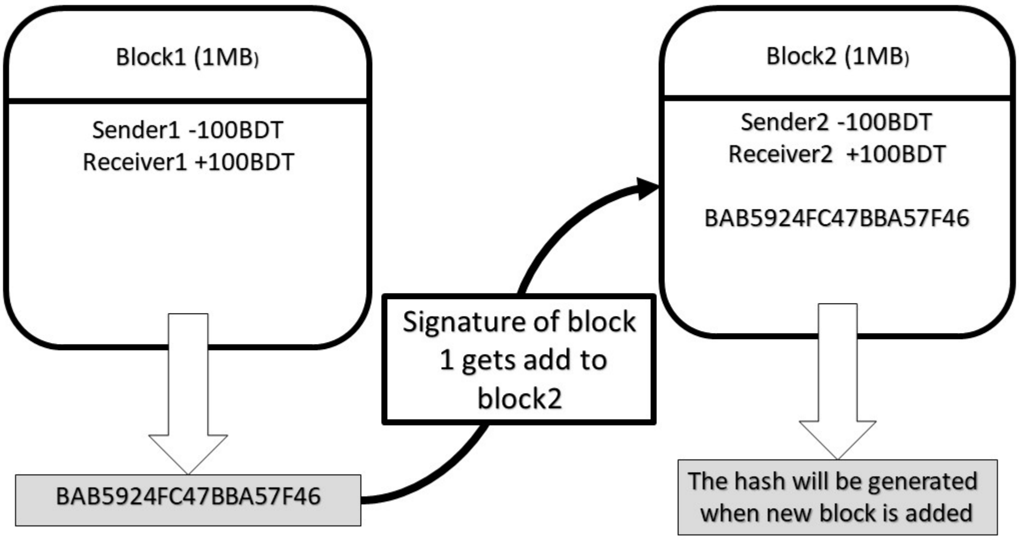


Figure 3.10: Storing hash for each consecutive blocks

A mark or signature does not generally eligible. A block may be acknowledged in the blockchain on the chance that its computerized mark begins with — for instance — a back to back number of zeroes. For instance; the blocks with a mark beginning with at any rate four continuous zeros meet all requirements to be added to the blockchain. Apart from this, as clarified already, every string of information has just a single remarkable hash bound to it. Eventually if there a situation comes of not having four zeros then the activity of mark age will happen over and over.
Since the exchange information and metadata need to remain the manner in which they are, a small data is added to each block that has no reason aside from being changed continuously qualified signature or mark. This bit of information is known as the nonce of a block. The nonce is a totally arbitrary series of . To recapitulate, a block now contains; transaction information, the mark or signature of the past block and a nonce. The procedure continuous changing of the nonce and hashing the block's information to discover a qualified mark is called mining and is the thing that diggers do. Excavators spend power as computational power by continually changing the block combination (nonce) and hashing it until they locate a qualified mark (signature). The more computational power they have, the quicker they can hash distinctive block combinations and eventually they are to locate a qualified mark (signature) quicker. It is a kind of trial and error.

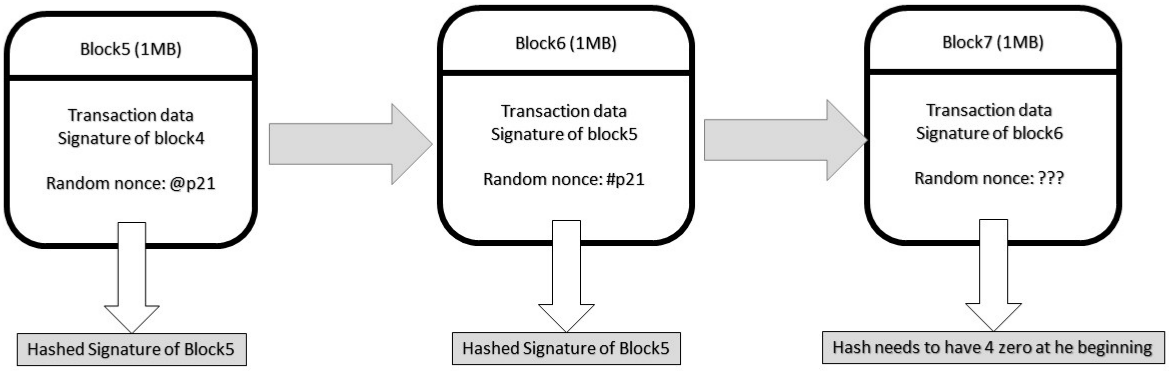


Figure 3.11: Creation of nonce by the miners

In this system of blockchain any of the user can take part in this procedure by downloading and beginning the agreeing digging programming for that particular blockchain. When any user does this, they will basically take care of their computer based calculation capacity to make the nonce for a block.

If anything gets modified then the blocks will get detached. All together for an adjusted block to be acknowledged by the remainder of the system, it should be fastened to the resulting blocks once more. It was recently clarified this requires each block that comes after it to get another mark. Also, that mark needs to meet the necessities. Giving these obstructs another mark will be exorbitant and tedious, in spite of the fact that it doesn't appear to be inconceivable.

A big number of miners are mining on the Bitcoin blockchain, and along these lines it tends to be expected that a solitary awful entertainer or substance on the system shall not be able to have more computer based arithmetical power than the remainder of the system joined, which means the system will never acknowledge any progressions in the system of blockchain, making the system unchangeable. When information is summed to the blockchain system, it can never be truly replaced again. There is an exemption however. Imagine a scenario where a terrible entertainer has more computational power than the remainder of the system joined. Hypothetically truly, this is conceivable. It is known as a nearly 50 percent attack has happened on different blockchain systems previously. However, this kind of attack on the blockchain would be clearly more unreasonable to execute than it would return consequently. It would not simply require a massive measure of equipment, cooling hardware and extra room for the mathematical power, yet in addition includes the danger of arraignment and, all the more critically, would extremely hurt the natural system of the agreeing blockchain , rendering the potential returns in Bitcoin to drop in a general sense in regard. Endeavoring a nearly 50 percent assault is for all intents and purposes attempting to battle the various 28 clients on a blockchain just without anyone else. This is additionally the explanation that the more clients or miners take part in the mining procedure the more the system of blockchain becomes secure.

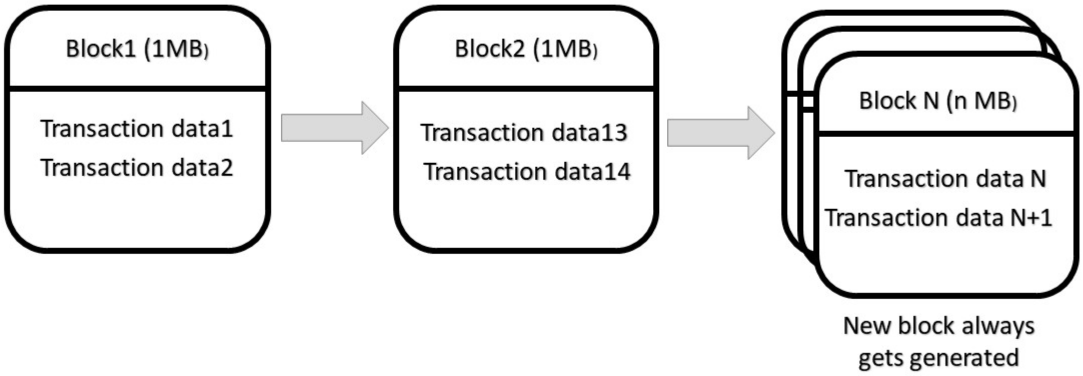


Figure 3.12: Generation of blocks one after another

The Bitcoin blockchain pursues an administration model of governance, and hence refreshes its record of exchanges (and therefore the Bitcoin adjusts) as per what most of its clients state is reality. The blockchain convention does this consequently by continually following information of the longest chain in the blockchain , in light of the fact that it accept that this chain is spoken to by the dominant part. All things considered, it requires most of the computational capacity to make the longest form of the blockchain. Additionally, this is how an adjusted block is naturally dismissed by most of the system. Most of the system dismisses a changed block consequently on the grounds that it is never again tied to the longest chain.

Chapter 4

Consensus Algorithm

In the blockchain real applications, there are two problems that need to be solved. - twice spending and Byzantine Generals Problem. [1]. Twice the problem of investment notes by reusing the same ownership of land at exactly the same time in two transactions. The issue of double spending can also be solved by Internet transactions and the central reliable organizations. Blockchain solves this problem with the system of validating the transactions by many decentralized nodes together. The issue within the decentralized approach is the Byzantine Generals issue. The data can be shared by peer-to-peer networks between several nodes. Nevertheless, there are few nodes that can be cruelly targeted, turning communication issues. Current nodes had to discern the altered information and obtain the steady outcomes with other current nodes. This also includes the parallel consensus algorithm's approach. The consensus algorithm has been studied in decentralized system for several years. There are various algorithms used in blockchain for transplantation of consensus. The definitions of some of these consensus algorithms are explained in detail below.

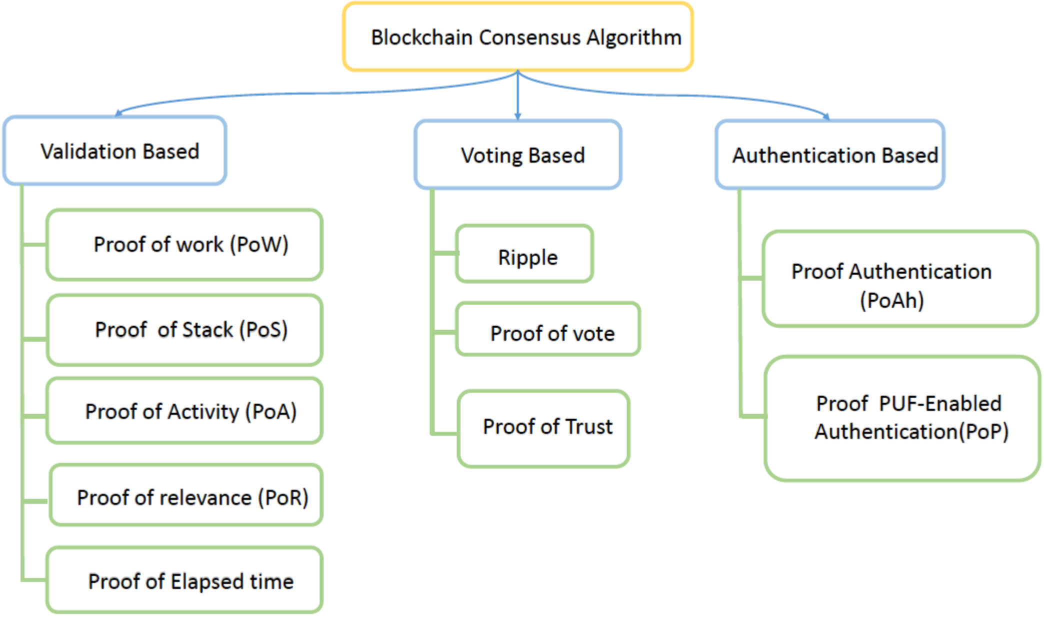


Figure 4.1: types of consensus algorithm in blockchain

4.1 Proof of Work

Proof of work used in the Bitcoin network is a consensus algorithm. In a decentralized system, somebody has to be nominated to note the transfers. The simplest method is arbitrary choice. Nevertheless, arbitrary choice is weak to defend attacks. So when one node requests to distribute a block of transactions, a large proportion of task has to finish to verify that the node is not going to be a threat to the network. Usually computer calculations is actually the real work. In Proof of Work, to count or calculate the hash value of the header one node of the network is needed or can be said it is the work of each node. To get diverse hash results, the block header holds a nonce and miners keep altering the nonce repeatedly. The consensus needs that the intended number must be smaller or equal to a definite given number. When one node extents the anticipated value, it would transmit the block to other nodes and all of the nodes commonly need to approve the accurateness of the hash value. Miners will join the new block to their own blockchains if they find the block is validated. Nodes which compute the hash numbers are termed as miners and the Proof of Work technique is known as mining. In the setup which is not centralized, legal blocks can be made instantaneously when numerous nodes discover the appropriate nonce approximately at the identical time. Consequently, divisions can be made. On the other hand, it is improbable that two opposing forks will create following block concurrently. In Proof of Work practice, a sequence that turn out to be lengthier subsequently is refereed as the accurate one. To diminish the damage, few Proof of Work methods where works can have few cross implementations have been planned. For example, Primecoin [26] explores for distinct prime number sequences which can be used for mathematical studies. [27]

Proof of Work is protected by the value of work. The block that has been freshly generated is linked to the blocks before it. The chain dimension is proportional to the amount of work done. The longest chain is believed by all nodes. If someone wishes to mess with blockchain, they must require to regulate more than half of the world's hashing dominance and confirm that they are able to grow into the first to create the new block and rule the lengthiest string. The benefits from altering could be far greater than the price. So the Proof of Work gives the security assurance of the blockchain.[28]

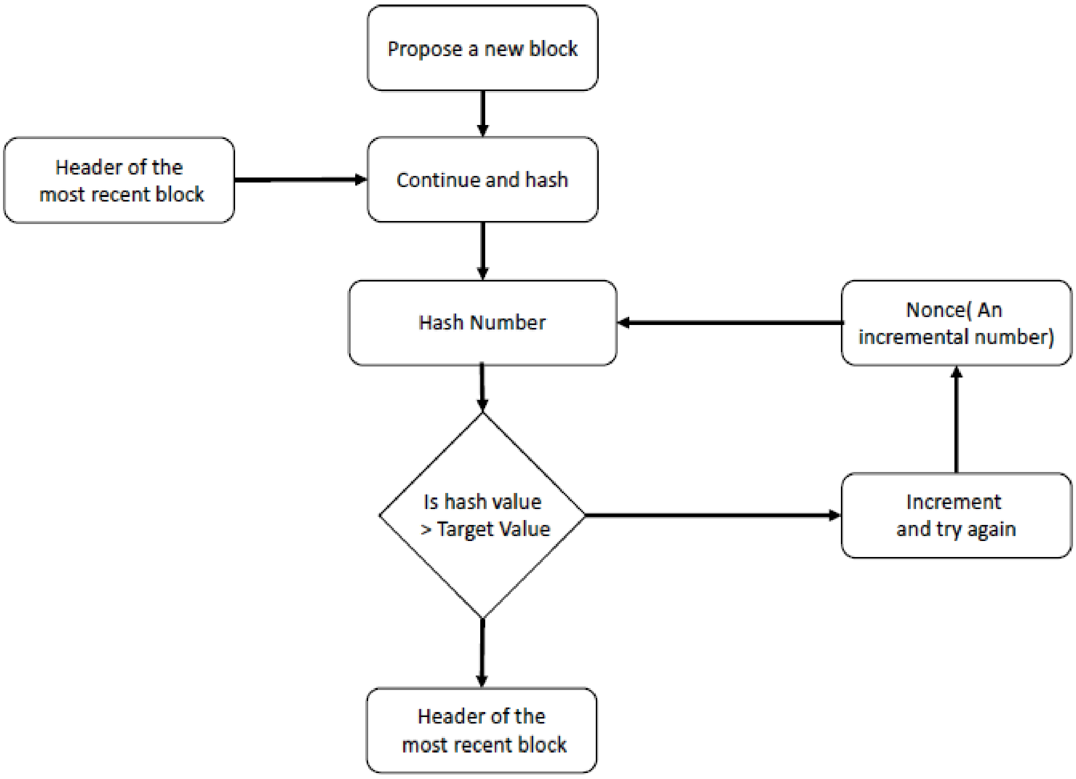

Propose a new block
Header of the most recent block
Continue and hash
Hash Number
Nonce(An incremental number)
Is hash value > Target Value
Increment and try again
Header of the most recent block

Figure 4.2: Proof of Work block diagram

4.2 Proof of Stakes

Proof of Stake was cited in the very initial task of bitcoin, but it was not implemented due to strength as well as different causes. PPCoin is the most basic implementation of Proof of Stake . The transaction in proof of stake has the idea of coin age. The transaction in Coin age is its cost multiplied by the time period later it has been produced. The lengthier every single node grips the transaction, the more rights it is able to acquire from system. Containers from the transactions would get a definite prize as stated by the coin age. In the strategy of PPCoin, to acquire the accounting privileges mining is necessary. The principle is-

$$proofhash < coinage \times target \tag{4.1}$$

The proofhash is consists of hash value of the weight factor, the non-spent result and the uncertain amount of recent period. Proof of Stake restricts the hashing ability of each single node. Coin age is inversely proportional to the trouble of mining. Proof of Stake empowers the coins owners to rise the allotment period. Moreover the PPCoin, there are similarly various type of coins using Proof of Stakes for instance the Nxt and BlackCion. However it thinks through the privileges of the nodes as well as practice an arbitrary algorithm to assign accounting rights.[28]

4.3 Practical byzantine fault tolerance

Practical byzantine fault tolerance is a duplication algorithm to bear byzantine faults. Hyperledger Fabric uses the Practical byzantine fault tolerance by means of its consensus algorithm since Practical byzantine fault tolerance could hold up to 1/3 malevolent byzantine copies. A new block is decided in a segment. In each segment, a key would be chosen along with some guidelines and it is responsible for organizing the transaction. The complete procedure can be distributed into three segment: pre-prepared, prepared and commit. In each segment, a node would arrive following segment if it gets votes from above 2/3 of total nodes. So Practical byzantine fault tolerance needs that every single node is identified to the network. Similar to Practical byzantine fault tolerance, Stellar Consensus Protocol (SCP) is likewise a Byzantine agreement protocol. In Practical byzantine fault tolerance, every node has to request other nodes while Stellar Consensus Protocol offers contributors the right to select which set of other contributors to trust. Based on Practical byzantine fault tolerance, Antshares has executed their dBFT (delegated byzantine fault tolerance). In dBFT, some specialized nodes are chosen to save the transactions.[27]
Thus, these are some significant consensus algorithm. The algorithm we are using is Proof of Work. Detailed discussion will be given later in this paper.

Chapter 5

Elliptic Curve Digital Signature Algorithm

The ECDSA (Elliptic Curve Digital Signature Algorithm) is utilized for authorizing integrity of data to stop from tempering of data. It was projected in 1992 by Scott Vanstone. Data reliability of a message or information is significant in the proposed network because the invader may try to alter data at the time of transferring to destination from source. Many organizations such as ISO (1998), ANSI (1999), IEEE and NIST (2000) use it as standard [29]. This algorithm is somewhat similar to the Digital Signature Algorithm (DSA), because this algorithms rely on DPL (Discrete Logarithm Problem). Here is a diagram for showing arithmetic operations through this curve,

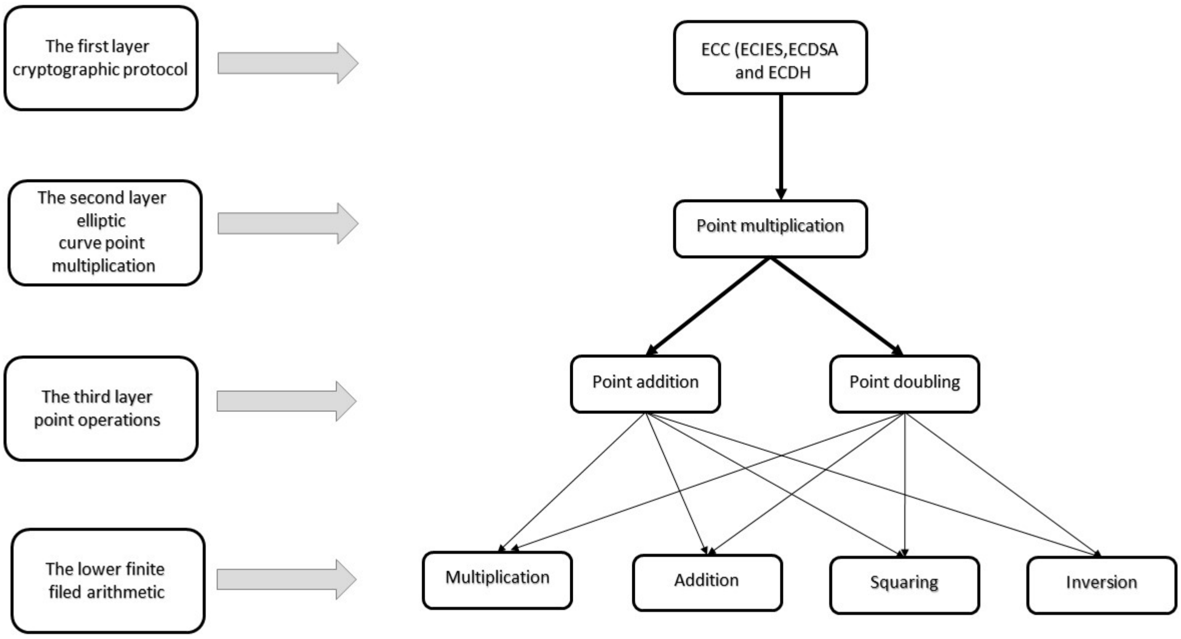

The first layer cryptographic protocol
The second layer elliptic curve point multiplication
The third layer point operations
The lower finite filed arithmetic
ECC (ECIES,ECDSA and ECDH
Point multiplication
Point addition
Point doubling
Multiplication
Addition
Squaring
Inversion

Figure 5.1: Arithmetic operations in Elliptic Curve Cryptography (ECC) Hierarchy

ECDSA algorithm utilizes a set of points on curve for generating the keys. Moreover, the generated keys are small in size. This algorithm having key length of 160-bit can provides the equivalent on behalf of symmetric cryptography with key length of 80-bit [30]. Apart from this, ECDSA is very convenient for constrained source devices since it generates small keys and also provides speed in computation work in the signature [31].]. Additionally, in ECDSA algorithm four point multiplication execution has been used, two for signature verification, one for signature generation and one is in public key generation [32]. Apart from this, the algorithm mostly constructed of three operations. They are signature verification, signature generation and key generation. These operation are described in below,

5.0.1 Key generation

- Selecting a random or pseudo random integer d in the interval [1, n- 1]
- Computing Q = dG
- Public key is set Q, private key is set d

5.0.2 Signature generation

- Selecting a random or pseudo random integer k, $1 \leq k \leq 1$
- Computing kG = (x1, y1) and convert x1 to an integer $\overline{x1}$
- Computing r = x1 mod n. If r = 0 then go to the step number 1
- Computing k-1 mod n
- Computing SHA-1(m) and convert this bit string to an integer e
- Computing s= k-1(e + dr)mod n. If s = 0 then go to the step number 1
- Signature for the message m such that (r, s)

5.0.3 Signature verification

- Verifying r and s are in the interval [1, n- 1]
- Computing SHA-1(m) and convert this bit string to an integer e
- Computing w = s-1 mod n
- Computing u1 = ew mod n and u2 = rw mod n
- Computing X = u1G + u2Q
- If X = θ then reject the signature. Otherwise, convert the x-coordinate x1 of X to an integer x1, and compute v = x1 mod n

Chapter 6

Land Registration principles

Usually the land registry principle are divided into four parts

6.1 principle of specialty

The involved property and the owner behind the entity must be unmistakably known to the system of land registration also accordingly within these data that are given for record keeping. Within this chain, the id and the tracking of any individual is troublesome work. This system was designed to not reveal this information to the users within the chain.

6.2 Principle of booking

Till amendment, the predictable facts are recorded, set-aside otherwise listed into the registry, the amendment in actual privileges on a fixed possessions isn't lawfully effected. The chain records all binding communications through a arrangement. This shows the process is suitable for payments on ownership, owners. That indicates chain will be in 'harmony with this principle.

6.3 Agreement principle

The norm suggests that the actual permitted individual whom reserved as per such within the registry should provide agreement for the alteration of the writing in the registry. This code will be fulfilled subsequently the landlord of the plot will have to mark all business dealing within the chain, beforehand it is registered to the net and place in a registry.

6.4 Publicity

System along with its data is open meant for review of general people. Moreover, there exists safety for the middle-man, for their integrity. A chain could be a common file that keep track, in a sequence of all valid transactions. Similar to a open registry keeper which is to never be meddled so, indubitable. It represents a 'sole collective drive of truth', consistent to the people, however there is no security for the other party.

Chapter 7

Functionality of proposed model

Usually the land registry principle are divided into four parts
In the proposed model, there are two categories of account. First one is administrator and the second one is user type account. Since the proposed model is a hybrid blockchain model, administrator account will have different functionality from the user accounts. In the user category, there are also two different types of users. One is owner of the land and another one is the person show wants to buy a land. The owner type user will have properties such as his land details, information about remaining amount in account. Additionally, an owner get to choose whether he wants to give his land on sale or not. A buyer account will have properties such as his account information, searching functionality for an available land, and available currency amount in his account. A buyer can only buy the lands which are available for sale. There will be a fixed value for a land. When a buyer wants to buy a suitable asset, he will issue for a transection request. In the very first stage, a checking will ensure if the buyer has enough currency to buy that specific land. Another checking will be done to ensure if there is such land which the buyer requested to buy. After all the checking is done, the requested transection will be withheld in a queue. Then a miner will try to mine a block by solving a mathematical puzzle. This block will consist of the transection information waiting in the queue. If the miner can successfully mine the block, a transaction will be recorded and the block will be added to the transection chain. For doing all the process correctly, multiple chain is used in the model.

7.1 used libraries

To conduct the model properly some of well-known libraries are used. List of the libraries with description is attached below,

7.1.1 Python Flask Library

This is a very popular and well known python library. It is a web framework. Basically, a web framework is an assemble of packages or modules that helps to create, manipulate and control web applications or more likely the services without needing to handle low level details as protocols sockets or process or might be the thread management. Flask is a tool which is used here to make the web development more flexible so that the model can be developed properly. It is part of the micro-framework categories. Micro-frameworks are normally type of framework with little to no dependencies to exterior libraries. This has some good sides and some bad sides. The main pros are that the framework is light, very less dependencies to update and watch for security bugs. Whereas main con is that sometimes dependencies are increased due to adding new plugins. Dependencies of the flask are:

- Werkzeug a WSGI utility library
- Jinja2 which is the template engine

We have used a template engine here for developing the model easily. Because, sometimes it becomes difficult to keep the consistency of design style in web based designs and need to change again and again. If the project contains only few pages, then changing its style might not take up a huge chunk of time. However, if there are a lot of pages this can become tiresome and troublesome work. So, to solve all these issues, flask is very helpful for this block-chain based land registry system.

7.1.2 Hash lib library

The main use of this library is to secure messages by hashing. Many different hashing algorithm is implemented in this library. FIPS secure hashing algorithm such as SHA1, SHA224, SHA256, SHA384 and SHA512 together with RSA's MD algorithm is defined in this library. The MD5 is a very commonly used Message-Digest algorithm. The record depicts the MD5 message-digest calculation.The calculation takes a message of discretionary length and generates a message of 128-piece "message digest" or "unique finger impression" of the information. Usually, it is impossible to deliver multiple messages which will have a same message digest, or to deliver any message having a given specific target message digest. The MD5 is projected to be used for computerized signature applications, there a huge document has to be compacted in protected technique before scrambling with a private key depending on an open key based cryptosystem for example RSA.

There is a constructor method named specifically for every type of hash available in the library. All return an object with hash having same simple type of interface. For example, sha256() constructor is used to generate a SHA256 hash object. This object then will be fed with by the help of update() method. It can be asked anytime for the digest of the concatenated data which has been fed to that so far using the methods like hexdigest() or digest(). Sha1(), sha224(), sha256(), sha384(), sha512(), blake2b(), and blake2s() are the constructors of hashing algorithms which are existing in the module. Aprt from these, md5() is also available as well, though it may be missing if rare "FIPS compliant" build of Python is used. Depending upon OpenSSL library, additional algorithms may also be available for the used platform. On most of the platforms, usually sha3_224(), sha3_256(), sha3_384(), sha3_512(), shake_128(), shake_256() are available.

In this system of land registry, SHA256 hash object has been used. This hashing library is used for increasing the security of the network by the creation of checksum. This checksum is proposed to represent private information. The process works by passing information as the input parameter in the hash function. It then returns a string of hashed characters. A diagram is given below for better understanding the whole procedure.

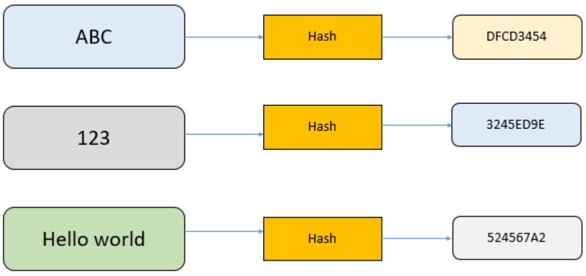


Figure 7.1: Difference in data before and after hashing procedure

So, every time the function generates a different hash. There will be no replication and no repetition of any hash generation. As the message become bigger, the system will generate stronger hash. Hence, it will be more difficult to decode the hash for any attacker.

7.1.3 The json library

Full form of JSON is JavaScript Object Notation. It is the de facto standard for many type information exchange system. It can make the transection of data faster and easier. JSON works by gathering information through an API (Application Program Interface) or sorting data in a database. Remote application can connect to a public system with the help of API. It works like a key for storing any data or information to a system. For example, if an application in a device wants to connect to an online database for storing the data and accessing it all the time from any place then using API is the way to go. The API works like a key here for entering into database from the system and also extracting the data when it is needed. Example of a JSON array is enlisted below,

$''chain'' : [$

$\{$

$''index'' : 1,$

$''previous\_hash'' : 0,$

$''proof'' : 1,$

$''timestamp'' :'' 2019-11-2920:15:29.707588'',$

$''transaction''[]$

$\}$

$]$

$''length'' : 1,$

$\}$

7.1.4 URL parsing library

This library gives a standard interface for breaking URL (Uniform Resource Locator) strings into segments. It is also used to join the segments once again into a URL string. This library has the capacity to change over a ”relative URL” to a flat out URL given a ”base URL.” In the system, urlparse() method parses URL into six parts by restoring a 6-tuple. This compares with the general structure of a URL. Each of this tuple is a string. The generated segments are not separated into smaller parts. For example, the system area is a solitary string and percent escapes are not extended.

7.1.5 Request library

The request library holds the de facto characteristics which makes HTTP (HyperText Transfer Protocol) applications in the Python. It extracts the difficulties of creating applications of an easy API so user can emphasis more on interacting with facilities in the application. An overview of the library is,

- Making requests by utilizing the HTTP methods
- Customizing request headers and data with the use of query string and message body
- Inspecting data of all the responses and requests
- Making request with are authenticated
- • Configuring applications for preventing application from slow down issue

7.1.6 ECDSA library

In the system, a very easy application of ECDSA (Elliptic Curve Digital Signature Algorithm) cryptography has been showed. It is implemented completely in the Python environment. This version is released underneath the license of MIT. With the help of the library, key pairs (signing key and verifying key) and sign messages can be created along with verification can be done easily. The keys and signatures are short and precise in length, making it relaxed for handling and incorporating into different protocols too. The library also offers the functionality of signing, key generation and verification for popular five NIST "Suite B" GF (p) (prime field) curves, with lengths of the key having 192, 224, 256, 384, and 521 bits. These curves are mostly recognized by the OpenSSL tool as, prime192v1, secp224r1, prime256v1, secp384r1, and secp521r1. Among them, bitcoin uses the 256-bit curve named as secp256k1 [33].]. In the library, there is also assist for the usual verities of Brainpool curves which ranges 160 upto 512 bits. Those curves are better known as: brainpoolP160r1, brainpoolP192r1, brainpoolP224r1, brainpoolP256r1, brainpoolP320r1, brainpoolP384r1, brainpoolP512r1. Although, more curves are not included in the library, still it is very easy to put on support for other curves of primary fields.

7.2 Code Description

All the methods used in the model is present in the main blockchain class. A short description and working principle of the methods used in the system is given below:

7.2.1 __init__ (self)

Here the “self” input in the method represents the instance of the object itself. In most of the object orientated languages it is passed as a hidden parameter to the methods and it is defined on an object. Here, an object of the class is created and then the methods is called with the help of object of that class. In python it does not process in that way. So it has to be declared explicitly. These are some methods which are used in __init__ method,

Chain list

For testing the first ever block-chain we have initialized the chain list

Transactions list

This list is to add the transactions block in the chain

Create blocks

It is the block of the land owners. Transaction and other information are processed here

Add transaction

For checking whether the land in available or not

7.2.2 create_block()

In this method, two very crucial parameters have to be given. One is proof and another is previous_hash. This method will create a dictionary type block.
List of all the parameters for this method is given below:

- index [adding one block will increment the length of the index]
- timestamp [time of the data entry]
- proof [it is a given parameter]
- previous_hash [given parameter]
- transactions [the whole list of transaction list]

After giving all the parameters, transaction list is again created from the “init” method. Finally, it appends the created block with the previous block. Before any of the block is created, a sample block can be generated from the __init__ method like this:
$\{ ''chain'' : [$
$\{$
$''index'' : 1,$
$''previous\_hash'' : 0,$
$''proof'' : 1,$
$''timestamp'' :'' 2019 - 11 - 2920 : 15 : 29.707588,'' ,$

$''transaction''[]$
}
] $''length'' : 1,$
}
Since it is a sample block, the proof is sent 1 and previous hash is assigned as 0.

7.2.3 create_land_block()

It is a flask module's method. It is used to create a land block. Information like land details, owner of the land, contact details of owner are dealt with in this method.

7.2.4 mine_block()

This method retracts previous block from the chain by calling previous_block method. Initially when there is no record to hold on, it will just call the initial block from the chain. After that, it deals with the previous proof from that previously generated block. Combining all of these, and the new information which has to be stored, a block is mined.

7.2.5 add_transaction()

Input parameters in the add transaction method are sender, receiver, amount. The sender is preset according to name. After calling the method it adds a block to the transaction chain with the input parameters. Eventually, it will increase the index of the main chain. So, after the add_transaction() method is called, a new block (by calling create_block method) is created in the main chain.
While doing that, it requires the proof that is the previous proof from the current block and the previous hash that is the hash of the previous block.

7.2.6 get_previous_block()

This method returns the block of the previous index and the system will not give any error. Because as the program is started a sample or initial block gets created every time to avoid error.

7.2.7 proof_of_work()

The input parameters of this method are previous proof that is sent from the mine_block method. Here a proof is generated as a random number. At first, it creates a hash from the SHA256 and then encodes it. After that it will convert it to a hexadecimal string and then generate the proof by incrementing it following a check in the string hash. The condition of this checking is that the proof will get incremented until it finds '0000' at the starting position of the string. After it successfully finds the desired string, it returns the value. So, now the question might come then what is the work of the previous proof that was sent as the parameter in the method. The previous proof is needed because it uses this previous proof for generating the new hash. The equation used for this process,

$$hashlib.sha256(str(new\_proof^2 - previous\_proof^2)encode()).hexdigest() \tag{7.1}$$

After generating the new proof, it is then passed through.

7.2.8 hash()

This is another very important method for working with the hashing mechanism. Pseudo code for this method is given below for better understading.

- Encoded_block: encoded json of the input given block
- Returning the SHA256 encoded hexadecimal string

Using Python's context manager, a file called data_file.json is created and it is opened in write mode. The dump() method takes two positional arguments, they are

- the data object to be serialized
- the file-like object in which the bytes will be written

Here sort_key function is also used to sort these in an alphanumeric way. The input parameter is the block which is sent by the mine_block method and the hash is then generated. Then it finally returns the sha256 encoded hexadecimal string.

7.2.9 id_chain_valid()

Main concern here is to make the chain of blocks more and more secure. That is why this method is used for checking purpose. It checks if any variables of the chain is compromised or not. In this method, from the starting each index of the chain is taken to check the hash of previous block and the previous hash variable saved in the current block is matched with it.

- previous_block = chain[0]
- block_index = 1 (this is regarded as the current index of the chain)

This matching makes the chain validation way more secure than the one way validation of hash.

7.2.10 add_node()

This method is used for taking the URL address for adding a new node for to the chain.

7.2.11 replace _chain()

Through this method, the chain of nodes that are actually connected to the system can be modified automatically. A variable named "longest_chain" as null value and another variable "max_length" which represents the length of the main chain is compared. For each network a get request is sent and the response is saved. Then it checks if the response status is 200. The HTTP 200 OK success status response code indicates that the request has successfully passed. This response is cacheable by default. From the response the JSON length and the JSON chain is extracted. All the files are also extracted in JSON format. Then a checking is done to see if the main value of the main chain is larger than the chain of the other existing nodes and also if the chain is valid or not with the help of the chain_is_valid method.

7.2.12 search_land_hole()

This is a normal method where all the users can search for desired land by giving input of the land number. If the method does not find any kind of land with the given input the method will return zero.

Chapter 8

Methodology and Novelty

8.1 workflow

8.1.1 Blockchain and attributes

In our system we have a few number of blockchains. In the main blockchain all the transactional, land and mining information will be stored . Other than that in the transaction block there will be the nonce, sender, receiver and miner's name.In the miner's block there will be nonce and in the land block present and past owner name, land number.

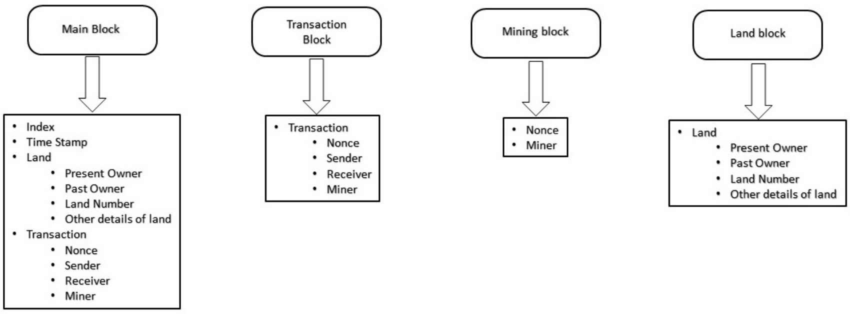


Figure 8.1: Blockchain and attributes

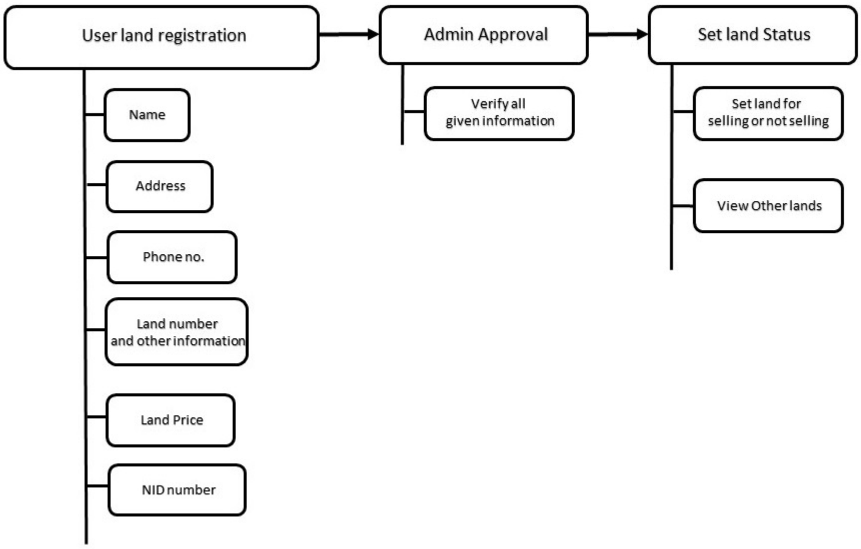


Figure 8.2: Land registration process

8.1.2 User Land registration Process

If a user wants to register his/her land. Then after giving the required information , the information will be under admin approval. After the admin approves the documents the land will be added to the system. The same thing will occur when any user will want to buy land. They need to give their bank account and other personal information and will be verified by the admin .

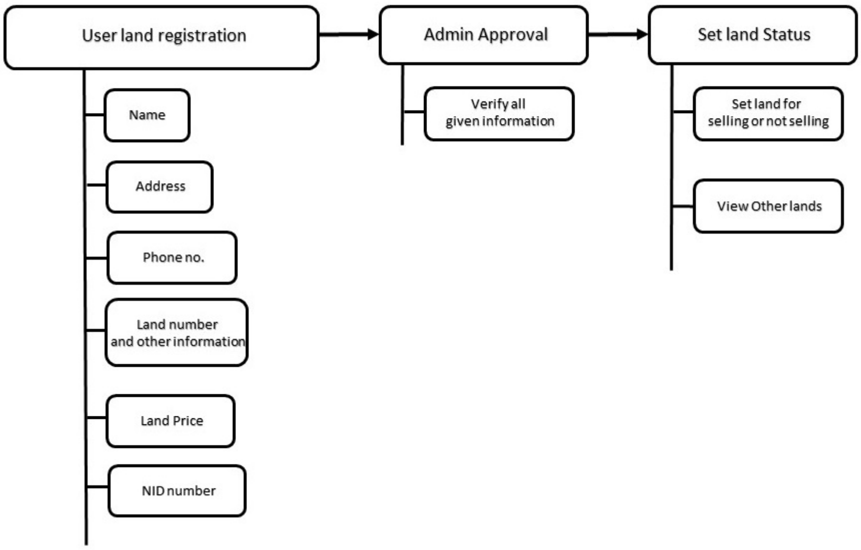


Figure 8.3: User registration process

8.1.3 Land Buying process

If any user wants to buy any selected land then our system will check if he/she has enough amount in the bank account verified by the admin and the land is verified by its signature then the transaction will withhold to get mined.

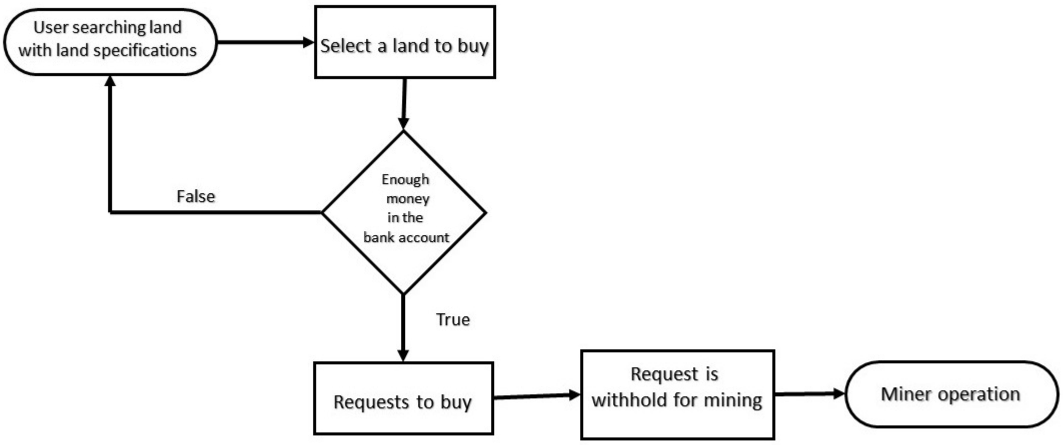

User searching land with land specifications
Select a land to buy
Enough money in the bank account
False
True
Requests to buy
Request is withhold for mining
Miner operation

Figure 8.4: Land buying process

8.1.4 Signature key generation and verification

Whenever a user will register a land for selling then a digital signature will get generated and saved with the land attribute in binary form. If the land is selected by any user for buying then the signature will go through a verification process . The process will be like the diagram shown below.

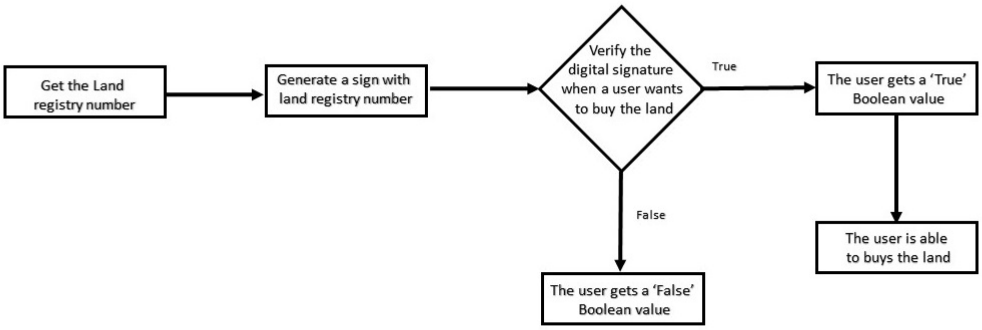

Get the Land registry number
Generate a sign with land registry number
Verify the digital signature when a user wants to buy the land
True
The user gets a 'True' Boolean value
The user is able to buys the land
False
The user gets a 'False' Boolean value

Figure 8.5: Sign key generation and verification from ECDSA

8.1.5 Miner selection process

As we have a selected number miner in our system. They will all be notified when there is a withhold transaction. A difficulty hash will get generated our given equation and mining hash will get generated by the existing blocks. With the cpu computational values miners list will get shuffelled. The check until the mining hash smaller than the difficulty hash.

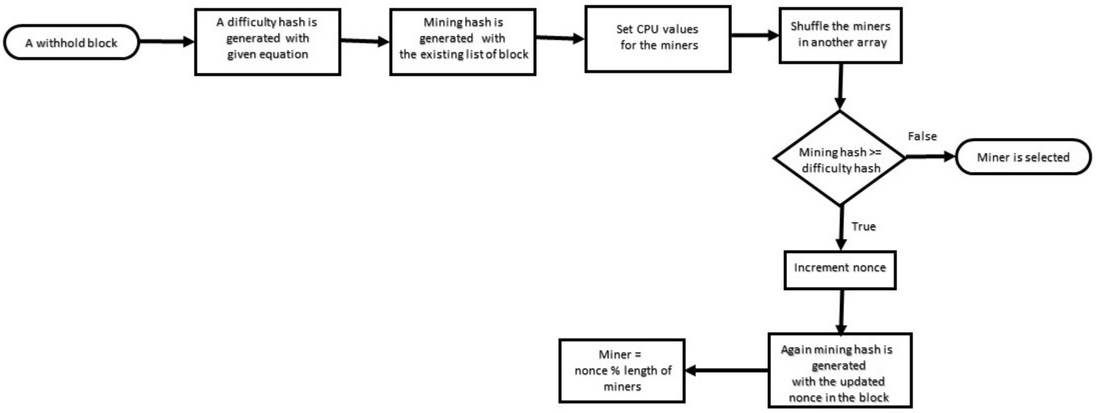

A withhold block
A difficulty hash is generated with given equation
Mining hash is generated with the existing list of block
Set CPU values for the miners
Shuffle the miners in another array
Mining hash >= difficulty hash
False
Miner is selected
True
Increment nonce
Again mining hash is generated with the updated nonce in the block
Miner = nonce % length of miners

Figure 8.6: Miner selection process

8.1.6 Block generation

Initially a block will be generated because of getting previous hash. For any kind of transaction a new block will get generated with a proof and hash of the previous block.

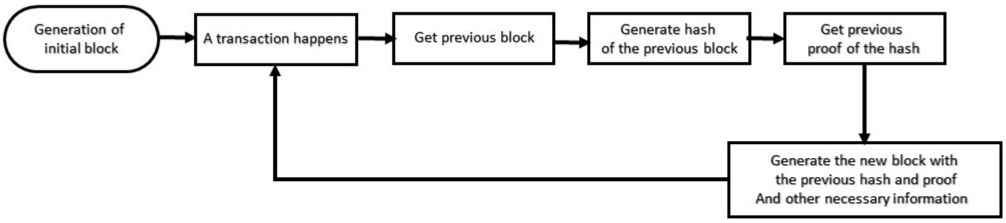
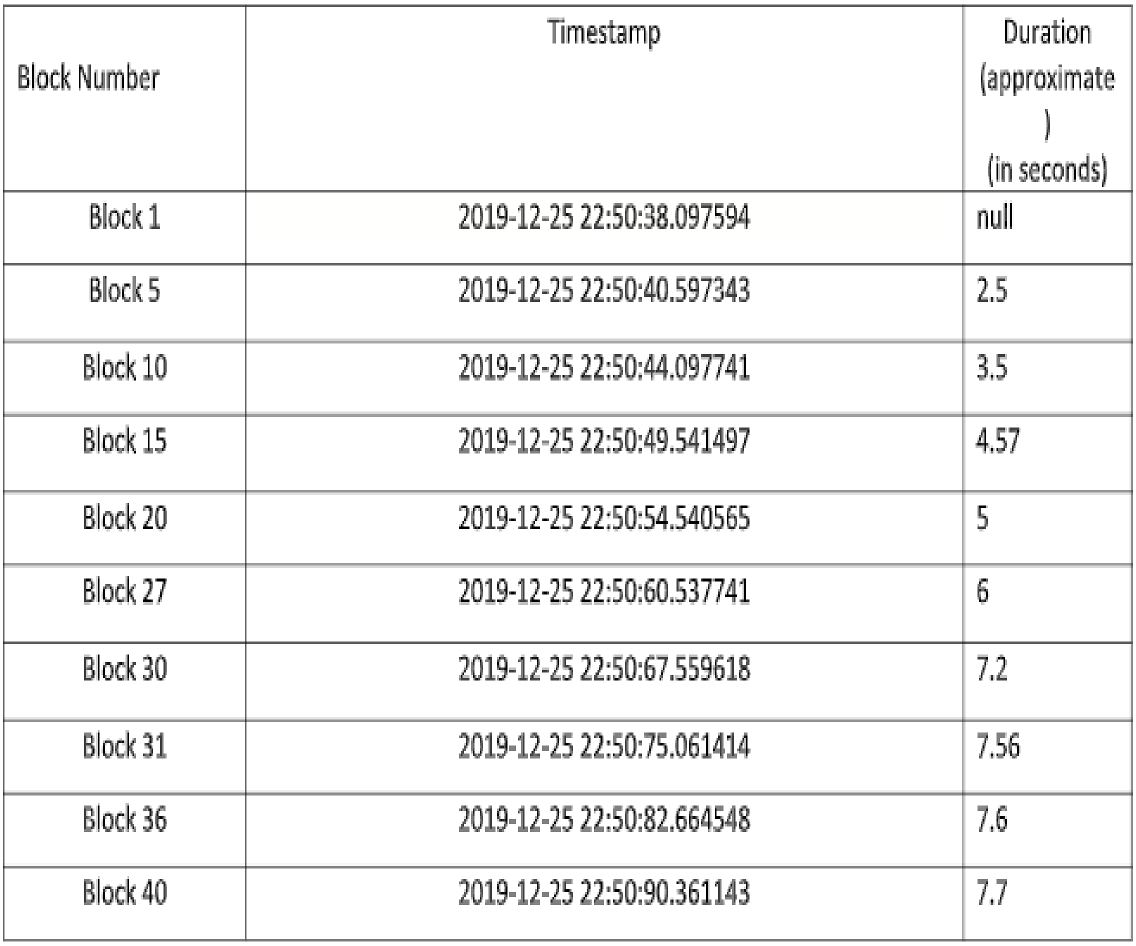

Generation of initial block
A transaction happens
Get previous block
Generate hash of the previous block
Get previous proof of the hash
Generate the new block with the previous hash and proof And other necessary information

Figure 8.7: Blockchain formation process

8.2 Outcome

In our system we have taken some time stamp for the block generation in the chain. Here the initial is given null time because it gets generated at the time the system starts. According to our proposed model we have seen that at the beginning the time of the block generation gets incremented



Block Number	Timestamp	Duration (approximate) (in seconds)
Block 1	2019-12-25 22:50:38.097594	null
Block 5	2019-12-25 22:50:40.597343	2.5
Block 10	2019-12-25 22:50:44.097741	3.5
Block 15	2019-12-25 22:50:49.541497	4.57
Block 20	2019-12-25 22:50:54.540565	5
Block 27	2019-12-25 22:50:60.537741	6
Block 30	2019-12-25 22:50:67.559618	7.2
Block 31	2019-12-25 22:50:75.061414	7.56
Block 36	2019-12-25 22:50:82.664548	7.6
Block 40	2019-12-25 22:50:90.361143	7.7

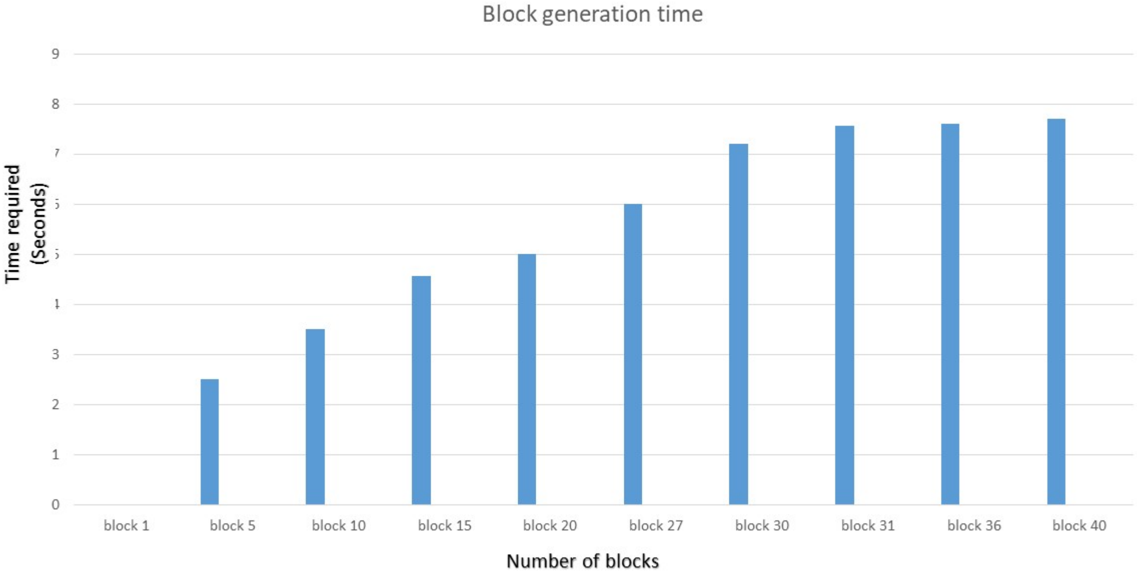


Figure 8.8: Block generation graph

8.2.1 Computational power of miners

As this is the proposed we have taken some arbitrary value for the computational power.

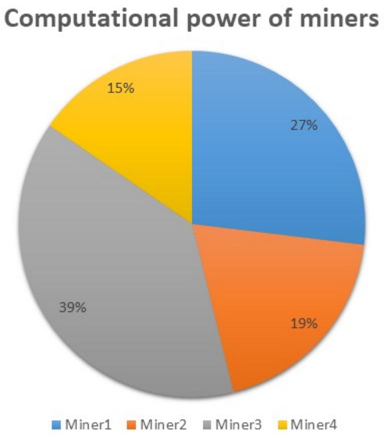
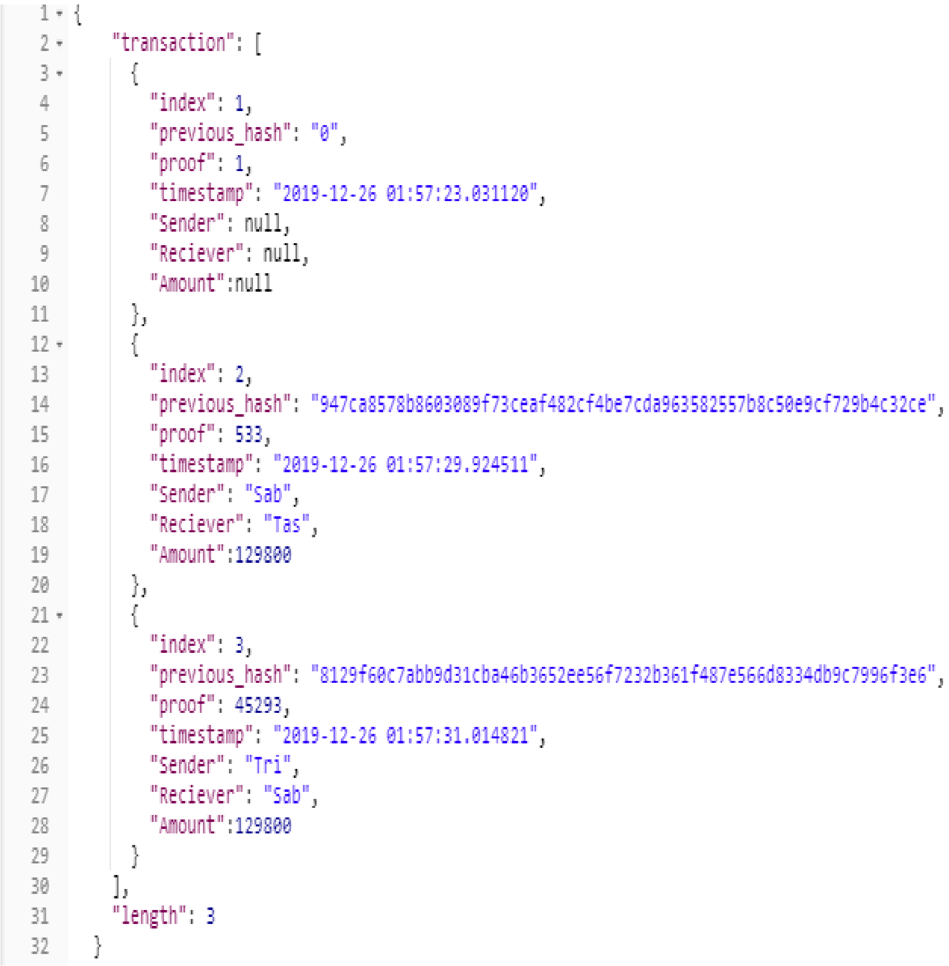


Figure 8.9: Miner computational power

8.2.2 Outputs of the system

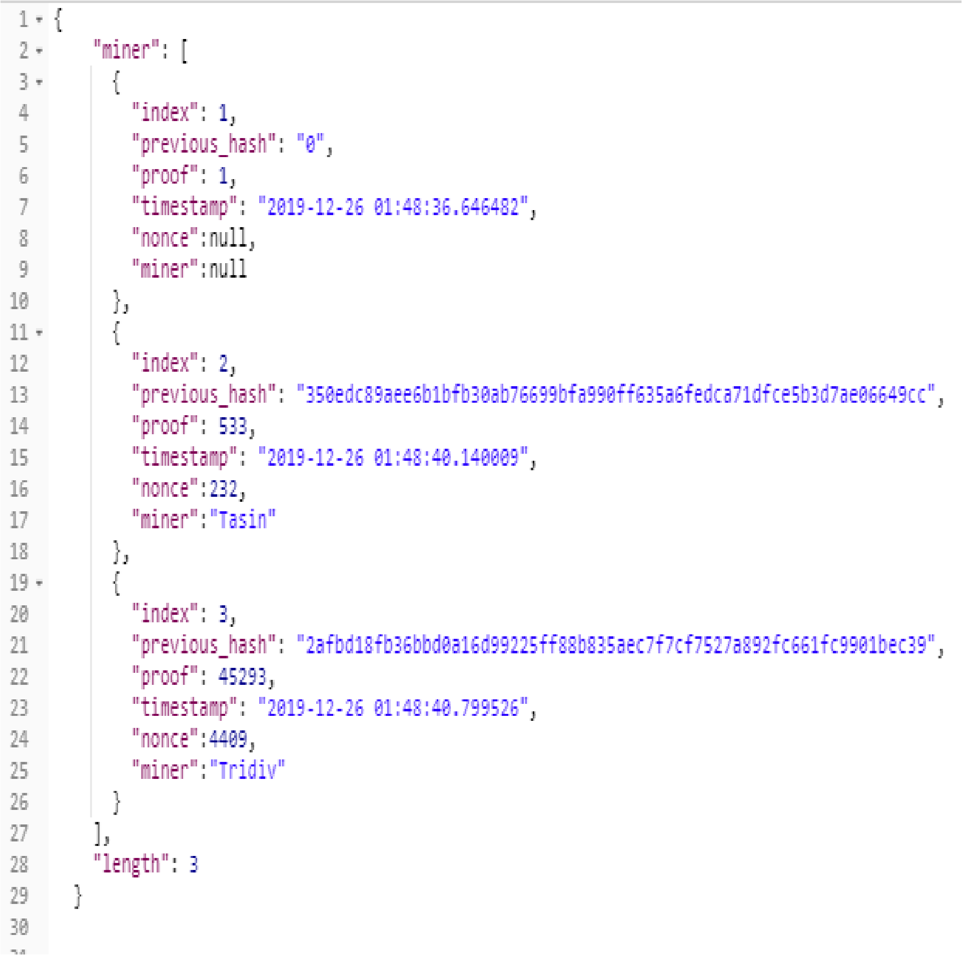
In our system we get JSON output when there is a change in the system. If someone registers the land then it will added in the separate blockchain list. The same thing will happen in case of transaction and mining information. Each of the transaction will be stored in a separate block.



```
{
  "transaction": [
    {
      "index": 1,
      "previous_hash": "0",
      "proof": 1,
      "timestamp": "2019-12-26 01:57:23.031120",
      "Sender": null,
      "Reciever": null,
      "Amount":null
    },
    {
      "index": 2,
      "previous_hash": "947ca8578b8603089f73ceaf482cf4be7cda963582557b8c50e9cf729b4c32ce",
      "proof": 533,
      "timestamp": "2019-12-26 01:57:29.924511",
      "Sender": "Sab",
      "Reciever": "Tas",
      "Amount":129800
    },
    {
      "index": 3,
      "previous_hash": "8129f60c7abb9d31cba46b3652ee56f7232b361f487e566d8334db9c7996f3e6",
      "proof": 45293,
      "timestamp": "2019-12-26 01:57:31.014821",
      "Sender": "Tri",
      "Reciever": "Sab",
      "Amount":129800
    }
  ],
  "length": 3
}
```

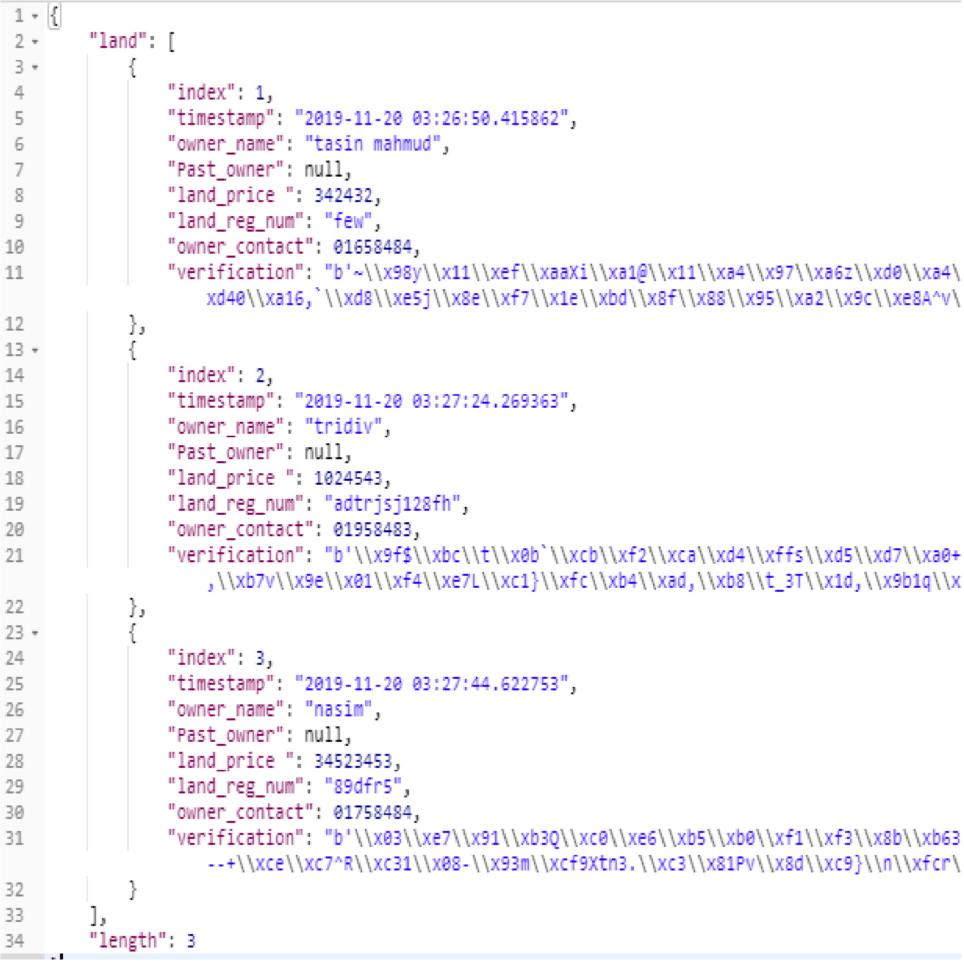
Figure 8.10: Transaction blockchain

In mining blockchain there will be list of nonce and the name of miner.



```
{
    "miner": [
      {
        "index": 1,
        "previous_hash": "0",
        "proof": 1,
        "timestamp": "2019-12-26 01:48:36.646482",
        "nonce":null,
        "miner":null
      },
      {
        "index": 2,
        "previous_hash": "350edc89aee6b1bfb30ab76699bfa990ff635a6fedca71dfce5b3d7ae06649cc",
        "proof": 533,
        "timestamp": "2019-12-26 01:48:40.140009",
        "nonce":232,
        "miner":"Tasin"
      },
      {
        "index": 3,
        "previous_hash": "2afbd18fb36bbd0a16d99225ff88b835aec7f7cf7527a892fc661fc9901bec39",
        "proof": 45293,
        "timestamp": "2019-12-26 01:48:40.799526",
        "nonce":4409,
        "miner":"Tridiv"
      }
    ],
    "length": 3
  }
```

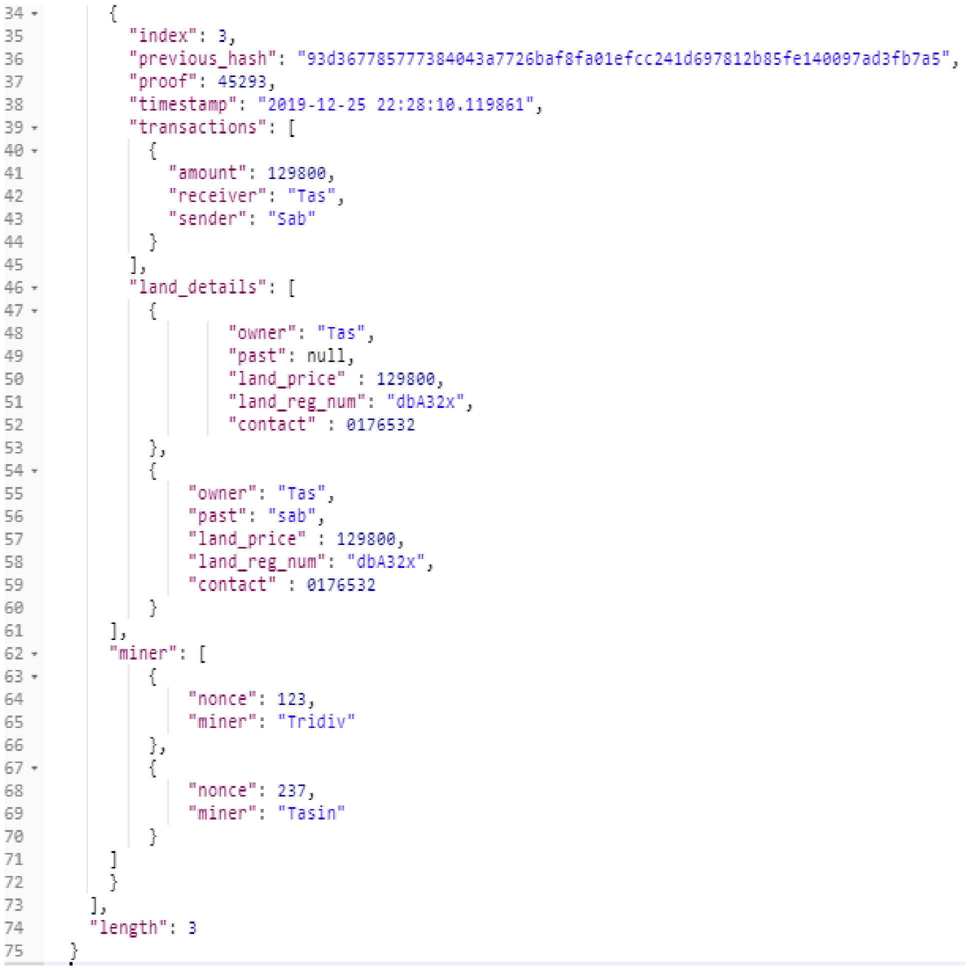
Figure 8.11: Miner blockchain



```
{
    "land": [
        {
            "index": 1,
            "timestamp": "2019-11-20 03:26:50.415862",
            "owner_name": "tasin mahmud",
            "Past_owner": null,
            "land_price ": 342432,
            "land_reg_num": "few",
            "owner_contact": 01658484,
            "verification": "b'~\\x98y\\x11\\xef\\xaaXi\\xa1@\\x11\\xa4\\x97\\xa6z\\xd0\\xa4\
                xd40\\xa16,`\\xd8\\xe5j\\x8e\\xf7\\x1e\\xbd\\x8f\\x88\\x95\\xa2\\x9c\\xe8A^v\
        },
        {
            "index": 2,
            "timestamp": "2019-11-20 03:27:24.269363",
            "owner_name": "tridiv",
            "Past_owner": null,
            "land_price ": 1024543,
            "land_reg_num": "adtrjsj128fh",
            "owner_contact": 01958483,
            "verification": "b'\\x9f$\\xbc\\t\\x0b`\\xcb\\xf2\\xca\\xd4\\xffs\\xd5\\xd7\\xa0+
                ,\\xb7v\\x9e\\x01\\xf4\\xe7L\\xc1}\\xfc\\xb4\\xad,\\xb8\\t_3T\\x1d,\\x9b1q\\x
        },
        {
            "index": 3,
            "timestamp": "2019-11-20 03:27:44.622753",
            "owner_name": "nasim",
            "Past_owner": null,
            "land_price ": 34523453,
            "land_reg_num": "89dfr5",
            "owner_contact": 01758484,
            "verification": "b'\\x03\\xe7\\x91\\xb3Q\\xc0\\xe6\\xb5\\xb0\\xf1\\xf3\\x8b\\xb63
                --+\\xce\\xc7^R\\xc31\\x08-\\x93m\\xcf9Xtn3.\\xc3\\x81Pv\\x8d\\xc9}\\n\\xfcr\
        }
    ],
    "length": 3
```

Figure 8.12: Registered land blockchain

In the main chain all the information will stored gradually. Anyone willing to see our whole system information can get thorough the main chain.



```
    {
      "index": 3,
      "previous_hash": "93d367785777384043a7726baf8fa01efcc241d697812b85fe140097ad3fb7a5",
      "proof": 45293,
      "timestamp": "2019-12-25 22:28:10.119861",
      "transactions": [
        {
          "amount": 129800,
          "receiver": "Tas",
          "sender": "Sab"
        }
      ],
      "land_details": [
        {
                "owner": "Tas",
                "past": null,
                "land_price" : 129800,
                "land_reg_num": "dbA32x",
                "contact" : 0176532
        },
        {
            "owner": "Tas",
            "past": "sab",
            "land_price" : 129800,
            "land_reg_num": "dbA32x",
            "contact" : 0176532
        }
    ],
    "miner": [
        {
            "nonce": 123,
            "miner": "Tridiv"
        },
        {
            "nonce": 237,
            "miner": "Tasin"
        }
    ]
    }
  ],
  "length": 3
}
```

Figure 8.13: Main chain List

8.3 Comparative Analysis

8.3.1 RSA vs ECDSA

RSA is the principal boundless calculation which gives non-intelligent calculation, both for marks and uneven encryption. So, RSA basically executes through two calculations. One is for encryption part, and another is for marking work. These two may utilize a similar key organization. RSA depends on both the difficulty of figuring huge whole numbers into two particular prime variables and the concealed exponentiation. The convention is broken by information on the two primes, p and q. Still, correspondence is secure as long as these are stayed discreet. Unfortunately, RSA has been proven to be broken by utilizing Shor's calculation on an adequately amazing quantum PC.

Whereas, ECDSA is a more novel type of cryptography. It is a variation of DSA, a mark calculation procedure that uses the discrete logarithm issue of old style PCs for calculation difficulty. ECDSA doesn't have encryption rather it is just for marks. DSA depends off of limited fields, explicitly prime fields. It utilizes plane bends considered Elliptic Curves over prime fields to deliver security that is comparable to RSA encryption system of a specific key length, yet with better compact keys. Additionally ECDSA utilizes a crash safe hash work, mostly a NIST standard, however any open hashing plan is also supported. Its confirmation has additionally been projected to be more CPU effective contrasted with RSA of comparable security. However, as like both DSA and RSA, ECDSA is also powerless against Shor's Algorithm for tackling the discrete logarithm issue.

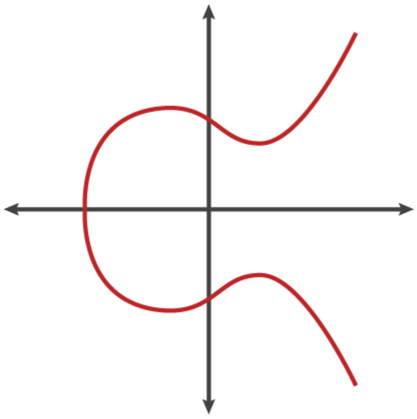


Figure 8.14: Elliptic Curve for Digital Signature Algorithm

Turns out that prime numbers are commonly utilized in trapdoor capacities. However, that does not work accordingly with quantum PCs. Also, additional current calculations creates other numerical issues, or straight up issues in material science to keep up security crosswise over quantum correspondences, for example, the utilization of superposition and snare.

8.3.2 Proof-of-Work (PoW) vs other consensus algorithm

Currently, there are a number of consensus algorithm to choose from. Among them, Proof-of-Work (PoW), Proof-of-Stake (PoS), Delegated Proof-of-Stake (DPoS) and Proof of Elapsed Time (PoET) are some of the most popular consensus algorithms. In the model the Proof of Work (PoW) consensus algorithm has been used. There are number of reasons for not applying all the other algorithm in the proposed system. To begin with, Proof-of-Stake algorithm faces with vulnerability issues. For example, if a person has enough money to invest, he can bring great damage to the system because on PoS the highest bidder gets the chance to mine new block. Moreover, this algorithm only gives the opportunity to rich miner get wealthier. This is because, for not having enough stake, small or new miner will not get chance to mine a new block as they might not have enough stake to win the chance to mine. Another very big issue might be, miner could just spend way more money on bidding and spending less on the equipment. For this, the mining process can become very slow due to having devices with less computational power. If Delegated Proof-of-Stake had been used then the system might encounter with issues like the witnesses who are responsible for mining might create a cartel. So, they will have the power to control the whole system. Because, every time they will invest the most and select one of their own people as a delegate who will have the power to create new block. Thus, the system will begin to become centralized as a few people will have the power to control the mining process. It can also lead to the state where the famous "51%" attack might occur very easily. It is the very famous hypotheses regarding an attack on a block-chain which is occurred by minors who control more than 50% computation power and control mining rights. Proof of Elapsed Time is very popular consensus algorithm in the work environment of permissioned as well as public block-chain. Since, the proposed model is a hybrid, meaning a permissioned block-chain it would be easier to adopt this algorithm in the system. However, if this algorithm was used, the system would rely somewhat on Intel who has developed this algorithm and possess some control over it. So, it will not be a good move to adopt this algorithm where a very important aspect of the model is to get rid of trusting third parties involvement. Apart from this, to properly utilize PoET some specialized hardware is required. On the other hand, Proof-of-Work is highly scalable. It is a must to have feature for this model since the system will work by undergoing rapid size change. Additionally, although it is not fully immune to the "51%" attack but due to having an unsynchronized mining selection process it will be very difficult to conduct this attack. Thus, PoW will ensure better security to system. For all of these, PoW has been chosen as the consensus algorithm over other standard ones.

8.4 Distinctive Feature

To begin with, the system is a permissioned blockchain. Permissioned blockchain can ensure an extra level of security. It can ensure access control to complete some certain task. In this system this access control is used to separate miners from normal users. Only certified and identified participants will be allowed to mine in the system. For this, although some functionality of the model is public and open to all, it is still a secured system thanks to its hybrid nature. In addition to that, the model proposed the system for direct transection of currency with the help of proper bank account information. This feature has not been discussed in any other existing blockhcian based land registry model. Also, the separate functionality for two different class of users are another unique addition to the system. Use of ECDSA to generate hash key is also distinctive for land registry purpose. Moreover, utilizing Proof-of-Work consensus algorithm for the sake of land registry is also something out of the box. Last but not the least, concept of building a hybrid system with administrative control is never seen before in this sector since all the existing work either adopt public blockchain approach or private blockchain procedure.

Chapter 9

Future work and Conclusion

9.1 Future Work

Right now, all block-chain based systems face some difficulties. Since it is an emerging technology, having such issues is not at all worrisome. Currently, one of the biggest issues that this proposed model faces is that it can use excessive energy. Due to its proof of work algorithm, where a lot of computational power is needed, this system might sometime become inefficient. Apart from this, the scalability is another weakness for the system. Due to its complex algorithms, its adaptability is still in work in progress state. Since, it does not provide any offline data storage functionality, if for any reason the nodes containing the chains are hampered the system might lose valuable information. Another big issue in current block-chain system is that, its performance might hamper over time. To improve the system more, these issues can be looked into in future work.

9.2 Conclusion

The main goal of this paper is to suggest a better alternative to the existing troublesome land registry system. Instead of just showing all the bright side of the system, it also contains limitations of the system. Although the system has a few number of drawbacks, it also contains a huge number of advantages over current land registry system. Fortunately, alternative procedure of many of these issues are already on test. Rest of the issues can hopefully be solved in upcoming days. As a result, block-chain based system is expected to take over all the record-keeping sectors in coming days. For this, block-chain based improved distributed ledger system can be a blessing to current traditional way of land registry system.

Bibliography

[1] V. L. Lemieux, "A typology of blockchain recordkeeping solutions and some reflections on their implications for the future of archival preservation", in *2017 IEEE International Conference on Big Data (Big Data)*, Dec. 2017, pp. 2271–2278. DOI: 10.1109/BigData.2017.8258180.

[2] U. M. Ramya, P. Sindhuja, R. Atsaya, B. Bavya Dharani, and S. Manikanta Varshith Golla, "Reducing forgery in land registry system using blockchain technology", in *Advanced Informatics for Computing Research*, A. K. Luhach, D. Singh, P.-A. Hsiung, K. B. G. Hawari, P. Lingras, and P. K. Singh, Eds., Singapore: Springer Singapore, 2019, pp. 725–734, ISBN: 978-981-13-3140-4.

[3] A. Mizrah, "A blockchain-based property ownership recording system, 2015", *URL http://chromaway. com/papers/A-blockchain-based-property-registry. pdf.[Online*, 2017.

[4] N. N. Peiró and E. J. M. Garcıa, "Blockchain and land registration systems", *European Property Law Journal*, vol. 6, no. 3, pp. 296–320, 2017.

[5] R. Thomas and C. Huang, "Blockchain, the borg collective and digitalisation of land registries", *The Conveyancer and Property Lawyer (2017)*, vol. 81, 2017.

[6] J. W. Kariuki, W. N. Karugu, and M. M. O. Opiyo, "Challenges facing digitization projects in kenya: Case of implementation of national land information management system", *International Journal of Technology and Systems*, vol. 3, no. 1, pp. 23–42, 2018.

[7] M. Swan, "Anticipating the economic benefits of blockchain", *Technology innovation management review*, vol. 7, no. 10, pp. 6–13, 2017.

[8] N. Kshetri and N. Kshetri, "The indian blockchain landscape: Regulations and policy measures", *Asian Res. Policy*, vol. 9, no. 2, pp. 56–71, 2018.

[9] S. Ølnes, J. Ubacht, and M. Janssen, *Blockchain in government: Benefits and implications of distributed ledger technology for information sharing*, 2017.

[10] K. Schmidt and P. Sandner, "Solving challenges in developing countries with blockchain technology", *Frankfurt School Blockchain Center Working Paper. Retrieved March*, vol. 2, p. 2018, 2017.

[11] J. Garzik and J. C. Donnelly, "Blockchain 101: An introduction to the future", in *Handbook of Blockchain, Digital Finance, and Inclusion, Volume 2*, Elsevier, 2018, pp. 179–186.

[12] M. Tunstall, A. Caplan, N. Prescott, and B. Sandler, "Real property transfers ripe for blockchain disruption",

[13] N. Kshetri and J. Voas, "Blockchain in developing countries", *It Professional*, vol. 20, no. 2, pp. 11–14, 2018.

[14] V. L. Lemieux, "Trusting records: Is blockchain technology the answer?", *Records Management Journal*, vol. 26, no. 2, pp. 110–139, 2016.

[15] G. Miscione, R. Ziolkowski, L. Zavolokina, and G. Schwabe, "Tribal governance: The business of blockchain authentication", in *Prepared for the Hawaii International Conference on System Sciences (HICSS)*, 2018.

[16] M. Themistocleous, "Blockchain technology and land registry", *The Cyprus Review*, vol. 30, no. 2, pp. 199–206, 2018.

[17] A. Alketbi, Q. Nasir, and M. A. Talib, "Blockchain for government services—use cases, security benefits and challenges", in *2018 15th Learning and Technology Conference (L&T)*, IEEE, 2018, pp. 112–119.

[18] J. Collindres, M. Regan, and G. Panting, "Using blockchain to secure honduran land titles", *Fundacion Eleutra, Honduras*, 2016.

[19] V. L. Lemieux, "Blockchain and distributed ledgers as trusted recordkeeping systems", in *Future Technologies Conference (FTC)*, vol. 2017, 2017.

[20] R. Thomas, "Blockchain's incompatibility for use as a land registry: Issues of definition, feasibility and risk", *European Property Law Journal*, vol. 6, no. 3, pp. 361–390, 2017.

[21] L. Carlozo, "What is blockchain?", *Journal of Accountancy*, vol. 224, no. 1, p. 29, 2017.

[22] S. Ammous, "Blockchain technology: What is it good for?", *Available at SSRN 2832751*, 2016.

[23] J. Vos, "Blockchain-based land registry: Panacea, illusion or something in between", in *IPRA/CINDER Congress, Dubai. European Land Registry Association (ELRA)*, 2017.

[24] L. S. Sankar, M. Sindhu, and M. Sethumadhavan, "Survey of consensus protocols on blockchain applications", in *2017 4th International Conference on Advanced Computing and Communication Systems (ICACCS)*, IEEE, 2017, pp. 1–5.

[25] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey", *International Journal of Web and Grid Services*, vol. 14, no. 4, pp. 352–375, 2018.

[26] D. C. Vitt, "Breaking bitcoin: Does cryptocurrency exchange activity lead to increased real activity outside cryptocurrency exchanges?", *SSRN Electronic Journal*, 2013, ISSN: 1556-5068. DOI: 10.2139/ssrn.2371343. [Online]. Available: http://www.ssrn.com/abstract=2371343.

[27] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends", in *2017 IEEE International Congress on Big Data (BigData Congress)*, IEEE, 2017, pp. 557–564.

[28] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, "A review on consensus algorithm of blockchain", in *2017 IEEE International Conference on Systems, Man, and Cybernetics (SMC)*, IEEE, 2017, pp. 2567–2572.

[29] D. Johnson, A. Menezes, and S. Vanstone, “The elliptic curve digital signature algorithm (ecdsa)”, *International journal of information security*, vol. 1, no. 1, pp. 36–63, 2001.

[30] B. Driessen, A. Poschmann, and C. Paar, “Comparison of innovative signature algorithms for wsns”, in *Proceedings of the first ACM conference on Wireless network security*, ACM, 2008, pp. 30–35.

[31] T. Cheneau, A. Boudguiga, and M. Laurent, “Significantly improved performances of the cryptographically generated addresses thanks to ecc and gpgpu”, *computers & security*, vol. 29, no. 4, pp. 419–431, 2010.

[32] S. Xu, C. Li, F. Li, and S. Zhang, “An improved sliding window algorithm for ecc multiplication”, in *World Automation Congress 2012*, IEEE, 2012, pp. 335–338.

[33] X. Zhou, Q. Wu, B. Qin, X. Huang, and J. Liu, “Distributed bitcoin account management”, in *2016 IEEE Trustcom/BigDataSE/ISPA*, IEEE, 2016, pp. 105–112.