Blockchain based Land Registry with Delegated Proof of Stake (DPoS) Consensus in Bangladesh

by

Mohammad Muhtasim Shahriyer
16301055
Mobashir Monim
16101114

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 and Engineering

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:

Mohammad Muhtasim Shahriyer	Mobashir Monim
16301055	16101114

Approval

The thesis/project titled "Blockchain based Land Registry with Delegated Proof of Stake (DPoS) Consensus in Bangladesh" submitted by

1. Mohammad Muhtasim Shahriyer (16301055)
2. Mobashir Monim (16101114)

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 26, 2019.

Examining Committee:

Supervisor:
(Member)

Dr. Mahbub Alam Majumdar
Professor and Chairperson
Department of Computer Science and Engineering
BRAC University

Program Coordinator:
(Member)

Dr. Mahbub Alam Majumdar
Professor and Chairperson
Department of Computer Science and Engineering
BRAC University

Head of Department:
(Chair)

Dr. Mahbub Alam Majumdar
Professor and Chairperson
Department of Computer Science and Engineering
BRAC University

Abstract

Land Registry documents are legally binding documents provided by the government to owners of land as proof of their ownership. In developing countries such as Bangladesh, it is essential to combat the challenges which a traditional Land Registry system faces. To keep a digital ledger of information about land assets in a transparent an secured manner, Blockchain technology can be used to overcome the hurdle. However, any Blockchain system could fail in the hands of an attacker if the right kind of consensus protocol is not used to secure the chain. The thesis proposes a novel approach on enhancing the Delegated Proof of Stake consensus to provide a private ledger based system secure for transacting land assets which can be easily integrated into the existing traditional Land Registry system for smooth operation. Witnesses are elected genetically while blocks have been customized to cover all the intricate details of the Land Registry Documentation while the system Architecture have been improved to include all sides of the stakeholders. Designated nodes have different roles which enhances the overall model to a structured Hierarchy and also withstand attacks. With the implementation of a Blockchain based system to maintain Land Registry document will allow for data transparency, and immutability therefore making counterfeits and forging almost impossible. This also cuts down the hassle of collecting different documents from different agencies making it easier to obtain land registry documents.

Keywords: Blockchain, Mining, Consensus, Delegated Proof of Stake, Land Registry, Bangladesh, Security, Protocol, Cryptography, Proof of Work, Bitcoin, Hash Function, SHA256

Acknowledgement

Firstly, all praise to the Great Allah for whom our thesis have been completed without any major interruption.

Secondly, we thank our supervisor Dr. Mahbub Alam Majumdar for giving us this opportunity to research on this topic and assisting us through the process. We would like to express our special gratitude and appreciation to him for giving us such attention and time. We thank Dr. Md. Golam Rabiul Alam for giving us time to discuss about the topic and referring us to resources and research materials for our Thesis.
We are also thankful to Sk Imtiaz Ahmed, Sadman Sakib and S.M. Azwad-Ul-Alam for helping us with research and supporting us with their valuable suggestions.

Table of Contents

List of Figures

List of Tables

Nomenclature

The next list describes several symbols & abbreviation that will be later used within the body of the document

$DApp$ Distributed Application

$DDoS$ Distributed Denial of Service

$DPoS$ Delegated Proof of Stake

$p2p$ Peer to Peer

$pBFT$ Practical Byzantine Fault Tolerance

PoS Proof of Stake

PoW Proof of Work

Chapter 1

Introduction

The thesis introduces methods to combat the challenges of Land Governance in a developing country such as Bangladesh by digitizing Land Registry records and keeping them in a secured and transparent way by integrating Blockchain technology to existing Land Registry process.

1.1 Problem Statement

One of the biggest challenges in Land Governance of developing countries is keeping an updated and accurate land registry documentation which is secured from attackers or corruption. Many developing countries, such as Bangladesh do not have a proper ledger to keep records of land transactions. The physical records kept by the Land registry offices are subject to inconsistencies, damage and vulnerable to tampering. Correctly keeping land records in a densely populated country is one of the biggest hurdles a developing country could face, as unclear ownership leads to widespread dispute.

1.2 Motivation

Digital Bangladesh is one of the nation's dreams. Special emphasis is given on the application of digital technologies to realise Vision 2021, which we commonly call Digital Bangladesh. Land Registry is one of the leading challenges a developing country may face and hence, digitizing it is an important task. Blockchain technologies, which are relatively new compared to traditional technology could in fact provide the right resources and features to build a secure and permanent Land Registry system which is immune to tampering.

1.3 Solution

Our proposed solution provides a novel approach in Digitizing Land Registry documentation process of Bangladesh while making the documentation secure. The proposed system integrates to already existing land registry services provided by the Government of Bangladesh. By using Blockchain technologies in land registry, the information of land assets included in land registry documentations are securely kept in a private ledger and is kept linked to each other by means of cryptographic

hashes. Our proposed solution improves upon existing land registry and other systems using Blockchains with consensus protocols such as Proof of Stake and Delegated Proof of Stake to maintain Land Registry documents that would allow for data transparency, and immutability therefore making counterfeits and forging almost impossible. Moreover, it works at a decentralized level by dividing the land into zones where nodes are selected to operate on. The system does not make nodes compete on computationally complex puzzles and hence, saves computational power and enhances energy efficiency for the system.

Chapter 2

Related Work

2.1 The essence of Blockchain

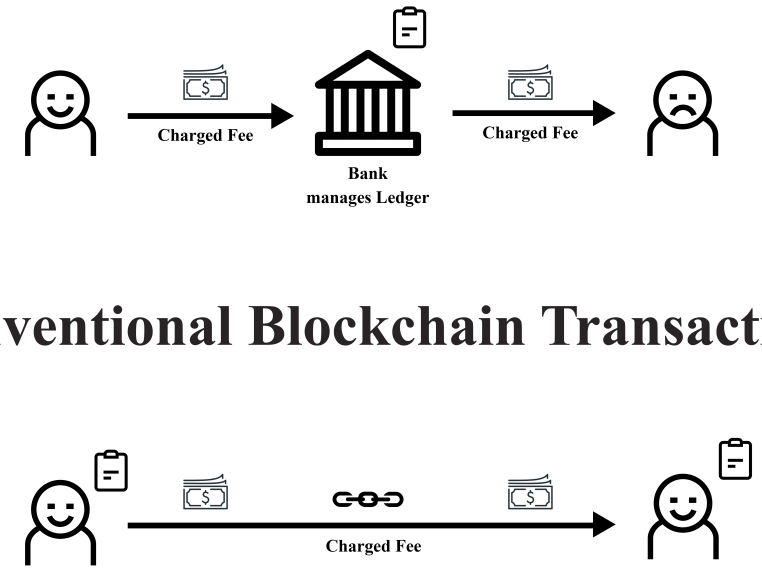

Figure 2.1: Conventional Transaction Process vs. Conventional Blockchain Transaction

Cryptocurrency technology is one of the many modern technologies that takes the main front of applications. Blockchains being at the heart of Cryptocurrencies, enable transactions to work in a decentralized peer-to-peer network by providing security with cryptography. However, this technology is not only useful in keeping Cryptocurrencies secure, but also operates it at a transparent level, avoiding corruption of data. The Blockchain technology can be translated to many other applications, one of which being used in Land Registry Documentation systems.

The theory of Blockchain originally came from the idea of Time-Stamping a digital document by Stuart Haber and W. Scott Stornetta[2]. From their findings, the theory of a continuously growing list of records called Blocks, which are linked and secured using cryptographic puzzles, came of use. Blockchain technology being safe and secure can keep these documents digitally with a secure cryptographic fingerprint[5], one which cannot be changed so easily. The cryptographic puzzles often operated within set rules or consensus protocols, by which an action is executed and mined to a new block in the chain. With the help of a decentralized system and secured protocols, Land Registry documentation will be secured safely throughout the network from illegal attacks[4][15].

2.2 Characteristics of a Blockchain System

A typical Blockchain based system provides major improvements over traditional systems. Land Registration systems provide a clear record of ownership rights over land, and prevents unlawful takeover. This is an intricate process usually carried out by a governing body. A Blockchain based land registry system, could improve the current traditional systems with its major beneficial characteristics:

- **Immutability**: All of the data records which are created are permanent. Hence, it cannot be modified in any form or deleted.
- **Traceability**: All transactions of the system can be easily tracked through the Blockchain.
- **Time-Stamp**: Every transaction entered will be secured and verified with a time-stamp.
- **Fail proof**: The Blockchain is distributed through the network, to prevent a single point of failure.
- **Anti-Fraud**: Blockchains operate through a consensus which validates the entry before adding the block to the chain, providing security and removing the risk of fraud.
- **Transparency**: All transactions on the system are transparent. Entities which are provided the authority can view the transactions.
- **Smart Contracts**: Conditions which are needed to carry out the transactions are pre-set in the system. The contracts are triggered automatically when all the conditions are met.

2.3 Structure of a Blockchain

Blockchain is a data structure of ordered back linked-list containing "blocks" which consists of a list of transactions[5]. Blockchain is secured by linking each block with cryptography. Each block will have its own hash, created by a specific hashing algorithm, along with the hash of the previous block, linking it cryptographically. Each block, along with the list of transaction as its Data, has other attributes which makes the Blockchain secure. This includes, but is not limited to:

- **Timestamp**: Time when the block was created.
- **Block number**: Number of the block in the Chain.
- **Nonce**: Number, which provides as a measure to validate work done, with the data to create the hash.
- **Prev. Hash**: Hash of the previous Block.
- **Hash**: Hash generated from the Data and Nonce of current block.

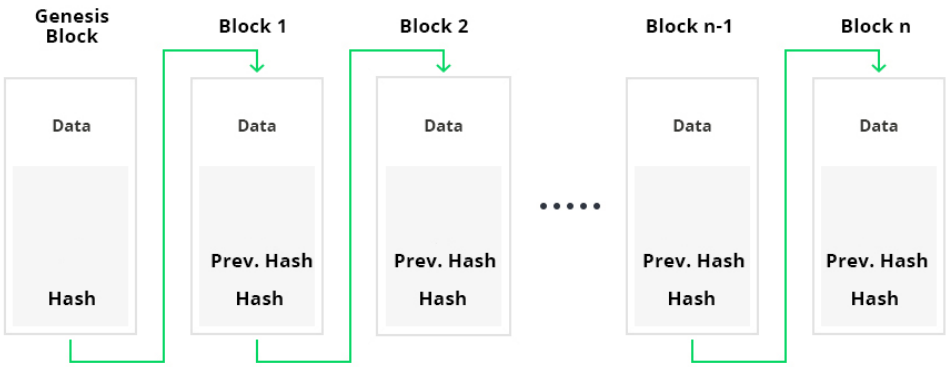

Figure 2.2: Structure of a Blockchain

The reason why Blockchain is secure is if any attacker would like to change the information in the block, the hash of the block would automatically change, and so the previous hash information of the next block would not match the newly generated hash, hence making the chain invalid. This is one of the main reasons why Blockchain is secure and can be used as a technology to apply it to the Land Registry Process and make it faster, secure and a transparent process for an individual to buy/transfer/sell land assets.

2.4 Land Registry documentation of Bangladesh

Considering the land registry process in Bangladesh, over the general information as mentioned above, the land registry document needs to contain the following information:

- **Mouza**: this defines the area in which the land in question is located.
- **Khatian number**: this is a number which connects to a paper which identifies a piece of land.
- **Daag number**: This is a number assigned to individual piece of land separate and identify land boundary in Mouza Map.

- **Khazna**: this is the document of government tax payment made by the parties in question against the piece of land.
- **DCR**: this is a document which verifies the ownership of a piece of land by someone.
- **Porcha**: this document contains the historical records of all the previous owners.

Each of these documents are provided by a different entity and therefore makes the entire transaction process even longer. The conclusion being that in the current status quo there is a lack of security in the documentation as well as the duration for transfer is enormous. This causes both distress and loss of personal property and resources.

2.5 Land Registry Procedure in Bangladesh

An entity would need to follow the required steps to complete the Land Registry procedure for purchase of a piece of land for residential or business purposes in the current traditional system in Bangladesh[14]:

- Confirm the record of rights from the land office.
- Conduct mutation on property and record the name of the new owner in the Khatian.
- Obtain inspection for RS mutation.
- Obtain the non-encumbrance certificate from the relevant sub-registry office.
- Pay stamp duty and prepare the deed of transfer.
- Pay capital gains tax, registration fee, VAT and other taxes at a designated bank.
- Apply for registration at the relevant Sub-registry.
- Register the change in ownership at the Land Revenue Office.

2.6 Blockchains with Immutable Ledger

Blockchain is an ever growing list of records stored as "blocks" connected together by a cryptographic puzzle and linked across a network of computers[5]. It creates a permanent storage where data immutability is the priority. As a block is added to the chain, the data is hashed and stored with the block. A reference to the previous block is also stored by saving the hash of the previous block in the current block. That way, the blocks in the chain can always refer back to the parent blocks, resulting in a secured connection. Traversing all the way back in a chain would get us to the genesis block, which is the only block in the chain which does not record the hash of the previous block, as there is none.

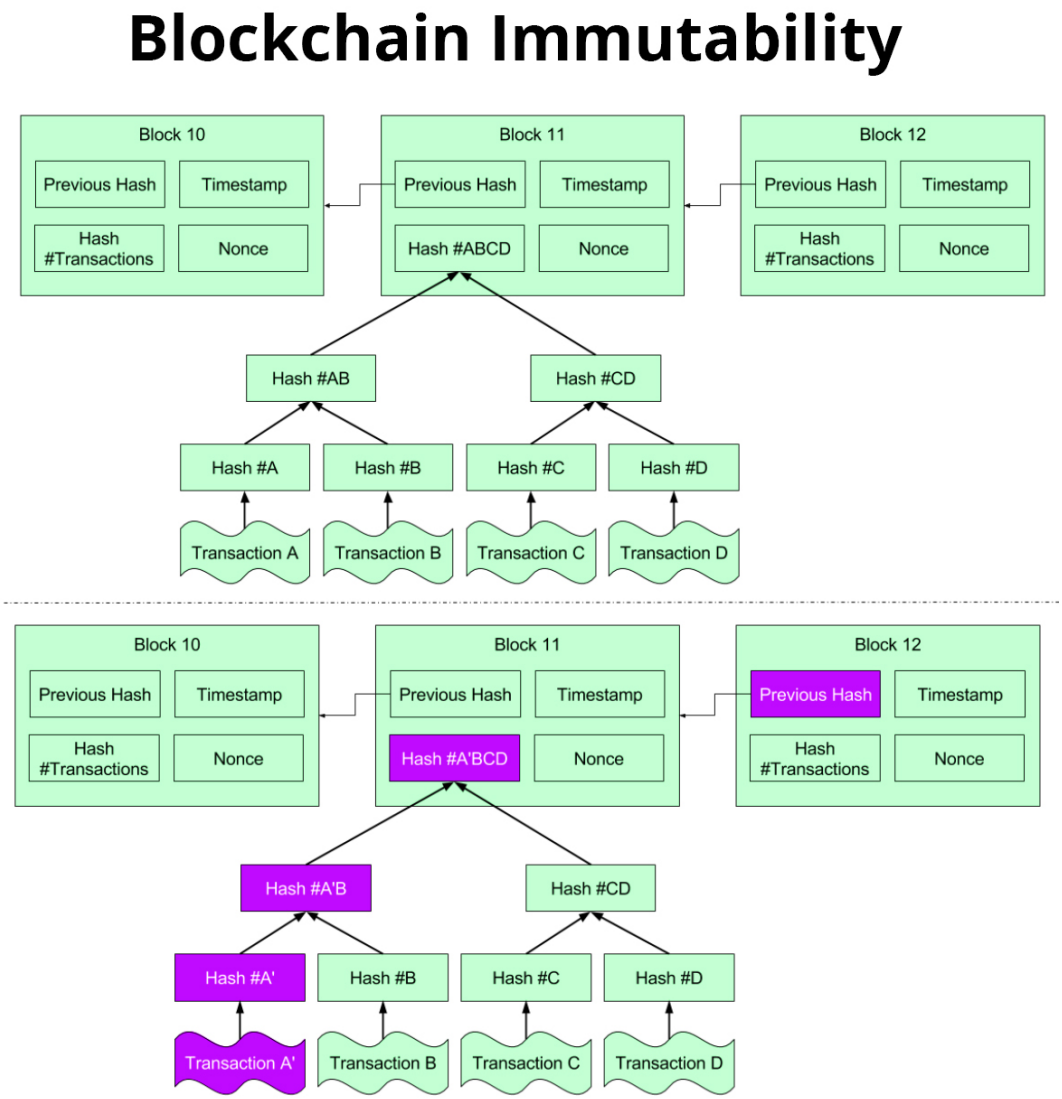

Figure 2.3: Immutability of a Blockchain

Many Blockchain based Land Registry systems have been developed in recent times. One of the most prominent one is by Land LayBy Group who first founded and operated in Kenya and then moved to other countries. Amongst other popular Blockchains, HM Land registry in the UK and Samsung backed Blocko in South Korea.
There are mainly three types of blockchain networks:

- **Public Blockchain**: An open-source network where all nodes are equal and anyone can participate in this network. There is no access or rights management in this network and all transactions are public.
- **Private Blockchain**: Entrants of this network are required to gain permission from the single governing entity managing the network to participate in the blockchain. This architecture allows networks to use Blockchain technology without making the data public to everyone.

- **Consortium Blockchain**: This is a hybrid blockchain operating under a group of entities instead of a single governing one.

Blockchains can also differ on the basis of permissions given to an entity on data accessibility while joining the network. Permissioned blockchains only allow nodes with permissions to access the data in the chain while permissionless blockchains give access to the data to all participating nodes [10].

2.7 Cryptographic Hash

Blocks in a blockchain are connected through the use of Hashes. A Hashing algorithm is used to generate the hash from the data and create a link. Each block in the Blockchain has the hash of the previous block stored within them. This is how the chain is protected from malicious attacks, if the data of a block is changed; the hash also gets changed for the block, which results in the link being broken as the next block cannot link back to its previous block, rendering the chain invalid. This results in early detection of the attack.
Bitcoin uses a hashing algorithm called Secure Hash Algorithm-256 (Or SHA256), developed by the National Security Agency in the US. While Etherium uses SHA-3 which is a subset of the broader cryptographic primitive family Keccak, designed by Guido Bertoni[6]. There are many other algorithms which are used by other Blockchain based systems. Recent technological advancements have introduced Elliptical Curve Hashing Algorithms which are used for generating public keys. Most popular blockchains like Bitcoin, Ethereum and others, use an elliptic curve algorithm called secp256k1 to generate public keys[5].

2.8 Distributed Peer-2-Peer Network

Peers are computer systems connected together through the internet. In a peer-2-peer network, a computer can communicate with another computer if they are both in the same network, without the help of any server computers[3]. Each of the nodes, act both as a server and a client. The first p2p network was introduced by Napster, which was used for sharing compressed audio mp3 files. When a node is connected to a p2p network, it can search and copy files from another node as well as communicate with each other. There are two types of p2p networks: A hybrid p2p network adds a central entity to their network, while a pure p2p network has all equal nodes. The distributed architecture of a blockchain network is essentially made of peers. In most blockchains, there is no single central entity for the sole purpose of removing a central point of failure. All nodes act as equal and store and interact with the chain in the same way. By using a p2p network, the chain is copied to all the nodes, making it harder for malicious attacks, as they would have to attack the whole network at once and change most of the chains to deem it to be genuine, which is very costly as well as time consuming. This discourages attackers to attempt attacks on a Blockchain.

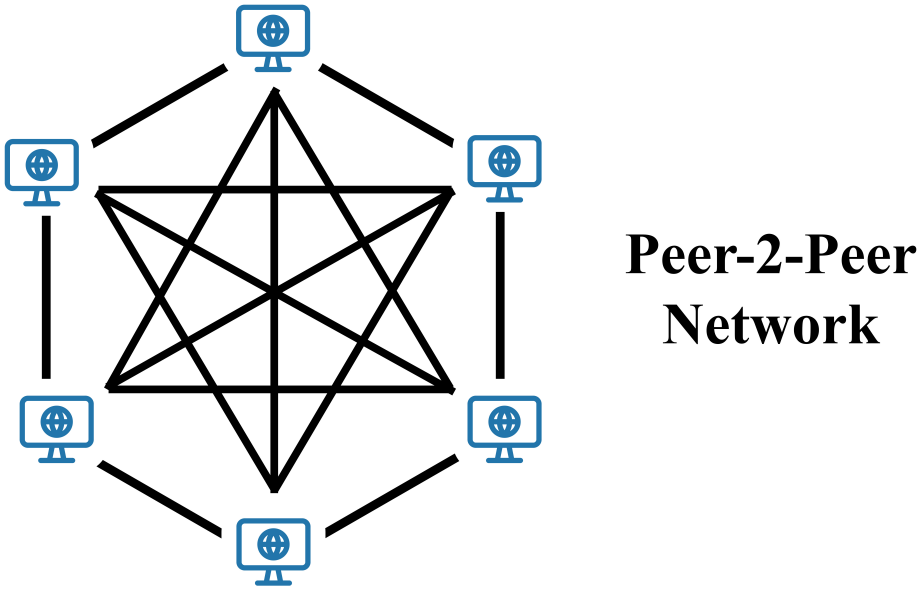

Figure 2.4: Structure of a Peer-to-Peer Network

2.9 Blockchain Mining

Mining is a process on how blockchain maintains its decentralized security. Miners in a blockchain "mine" new blocks by validating new transactions and adding them as blocks to the existing chain. In Bitcoin, on average, a new block is mined every 10 minutes, where all the miners compete with each other to solve a complex mathematical problem with a hashing algorithm. When a block is validated and the problem is solved, all the transactions related to the blocks are considered confirmed. This is carried out by a consensus algorithm which is called "Proof of Work" which proves that the miner has spent time and computational power trying to solve the problem[5]. The process of validating blocks may differ in other blockchains but the mining process is more or less the same. The complex calculation in PoS consensus systems are necessary so to provide security measures in the chain. In Bitcoin, miners receive rewards based on transaction fees and creating new bitcoin in the ecosystem. However the reward of new bitcoins decrease as new blocks are mined and after a certain period it will go down to zero, which after that only the transaction fees will be rewarded to the miner. Mining is done by brute forcing a number value called the nonce or number used only once. Miners change this number constantly and call the hashing algorithm to produce a hash which is less than the target hash given in the problem. If it is larger than the target hash, the miner tries again with another number. The miner who successfully solves the problem before others is rewarded and all other miners copy the latest chain in their system and start computing for the next block.

2.10 Blockchain Consensus Protocols

Consensus protocols are the core part of the Blockchain. In Blockchain there is no central body which manages the system. Instead, all nodes must reach a consensus to the pre-set conditions which enables them to validate and verify the transactions happening in the system without having a proper third-party to do the work. This consensus allows the Blockchain to maintain its security without a central body. This enables cryptocurrencies to be transacted between two entities without the help of a bank. Bitcoin is transacted with the help of its consensus "Proof of Work" which uses miners to solve a complex cryptographic puzzle to verify and validate the new transactions[5]. Proof of Work works very well in keeping a Blockchain secure, but it has its limitations due to high energy consumption and computational complexity making it costly for the system to operate. Other consensus protocols try to improve over the current systems and implement new conditions to keep the energy consumption and computational complexity low without decreasing the security of the system. Some of the other most popular consensus algorithms are: Proof of Stake, Delegated Proof of Stake, Practical Byzantine Fault Tolerance, Zero Proof. Consensus algorithms also help us to solve a problem in the p2p network called blockchain forks. As a decentralized system, the latest copy of the blockchain is stored within all the nodes in the network, however there are some important factors such as network latency, geographical locations to be considered as well as computational power. The problem arises when two competing miners of different nodes successfully mine blocks at the same time. As a result two blocks are created together with different identifier numbers, as both of them have a valid proof, none of the blocks are rejected at the start. In such cases, both chains remain in the network and are propagated throughout, the first chain to reach a new node is kept saved by that node. The miners who mined the blocks have their rewards kept on hold. After this, the process of creating a new block begins and everyone starts competing to solve the new block. The miner who solves the new block will decide which chain gets kept in the network, as there are two local chains, the chain which gets referenced from the new block is kept in the network and the other one is discarded. The miner whose block gets discarded does not receive the reward for mining that block, and every node in the network then copies the longest chain into their systems[5].

Chapter 3

Evolution of Blockchains

The structure of different Blockchain systems may seem similar to each other, however they differ at consensus protocols, which controls and administers the Blockchain to meet all of the preset conditions required to mine a block and add to the chain. Throughout the years, there have been multiple methods and implementations of consensus protocols which improve a Blockchain system to be more efficient, fast, and secure.

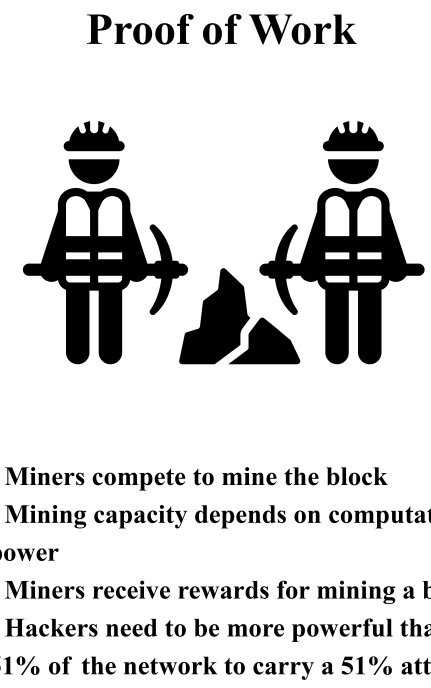

Figure 3.1: Proof of Work Consensus

3.1 Proof of Work

Proof of Work is a consensus algorithm, mainly documenting and verifying the information of calculations which satisfy particular conditions. It was mainly proposed by Adam Back in "Hashcash - A Denial of Service Counter-Measure" but popularized by Bitcoin which uses it as their consensus algorithm. HashCash is used to limit email spam and denial of service attacks[4]. Bitcoin uses its hashcash function to verify that work has indeed been done for the creation of a new block. It is impossible to predict which node in the network will be able to mine the new block. To approve the block as genuine, the system would need to check if the hash value is lower than the specified target.
PoW helps Bitcoin to protect itself from DDoS attacks, provides measures to verify that work has been done and reduce the influence of holders of large capital who would try to make decisions for the network[5]. It would take a considerable amount of computing capabilities to attack the network and would subject to high costs which does not make the attack worthwhile. However, due to these characteristics, complex calculations require expensive hardware which is combated by groups of miners instead of individuals, making the system gradually convert to a centralized one.

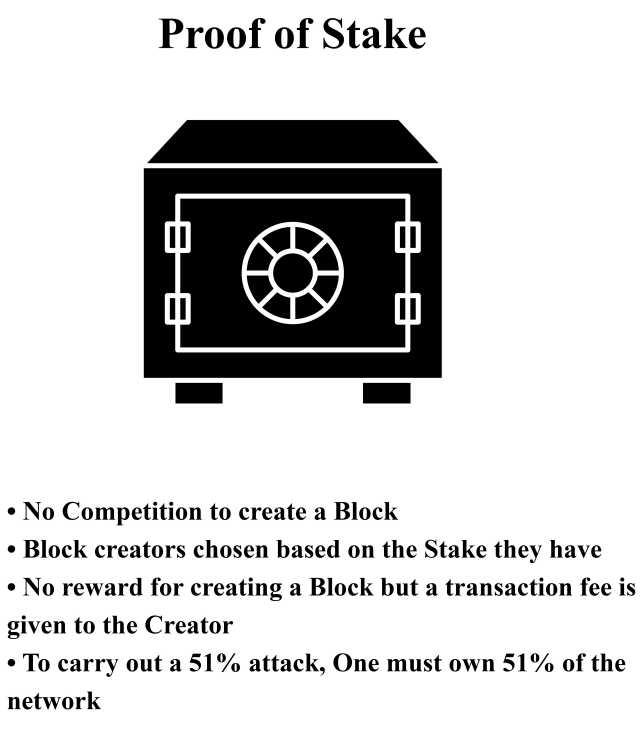

Figure 3.2: Proof of Stake Consensus

3.2 Proof of Stake

Proof of Stake has been developed to secure the Blockchain network as an alternative to PoW, where the users are requested to show ownership of a certain amount of currency[8]. It does not use hashing algorithms to validate transactions, and is used in many currencies including Peer-Coin where it is used as a supplement to PoW[7]. Various methods have been implemented to find the next valid block in a PoS system. BlackCoin uses randomization which uses a formula to find out the lowest hash value in combination to the size of stake, to predict which account will receive the authority to mine the next block with certain amount of accuracy. PeerCoin uses a system of "Coin Age" where owners with coins which are more than 30 days old try to compete for mining the next block where the owners of the oldest coins have the higher probability of getting the chance[7]. After mining, the owner starts over with "Zero Coin Age" and must wait 30 days before signing another block with a stake, i.e. coins. DashCoin uses masternodes which are decentralized servers as a form of staking[12].
While PoS seem to be more energy efficient than PoS, there are major differences between the two in terms of how they work. PoS can potentially solve the attacks a PoW system might face, such as DDoS attacks, unless the attackers own a large share of stake. However, there has been criticism regarding a new kind of problem, where block-generators can cheat to vote for multiple blockchain-histories without having anything to lose. This problem is known as "Nothing at Stake" [11].

3.3 Delegated Proof of Stake

Delegated Proof of Stake is a consensus algorithm which improves upon the security flaws of Proof of Stake, where stakeholders could potentially cheat the system, while improving upon the energy-efficiency which Proof of Work delivers. It was created by an American software developer - Daniel Larimer. Popular use of DPoS could be seen in BitShares, an open-source public financial platform which is now part of Microsoft Azure Blockchain as a Service package[13].
DPoS is a scalable consensus as opposed to classic consensus algorithms, and is fast in almost every stage of the network's development. It is a system which mimics democracy, and uses voting and elections to secure the network from centralization and malicious uses. The election process is maintained where active users vote to elect Witnesses and Delegates by putting their tokens on the names of the candidates. DPoS differs from PoS as everyone gets a chance to vote, whereas smaller stakeholders are usually restricted from the decision making in PoS systems[13].
There are multiple ways in how Delegates and Witnesses operate, however, no Witness have the right to change information within a transaction. Witnesses are responsible for validating the blocks, in some chains; they also have the power to block transactions, if deemed malicious. Witnesses can operate as a group of block forgers, or operate alone. If a witness becomes offline, its responsibilities are transferred to the next witness. They can be rewarded for validating the transactions. Delegates on the other hand, oversee parameters such as block size, witness pay, transaction fees and block intervals. They are not granted transaction fees unlike Witnesses.
Voting is done according to the Stakeholder's size. The stakeholder can vote as per the amount of tokens they may have, however no one is ever restricted from voting

rights. The election is continuous and there may be cases of re-elections in this consensus. By mimicking the voting from real life system, DPoS is considered to be democratic. However, it is also posed to challenges faced by traditional real-life election systems. Small stakeholders may feel their votes do not affect the decisions as opposed to bigger stakeholders and may decide not to vote. Successful use of the network requires participation of all who are interested, to provide effective governance. Still, the network may be subjected to centralization as the number of Witnesses are limited.

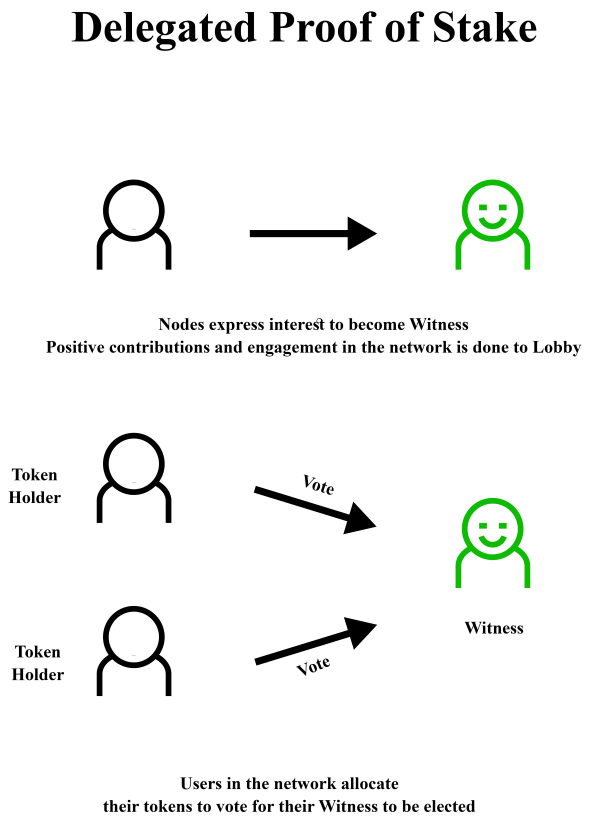

Figure 3.3: Delegated Proof of Stake Consensus Step 1

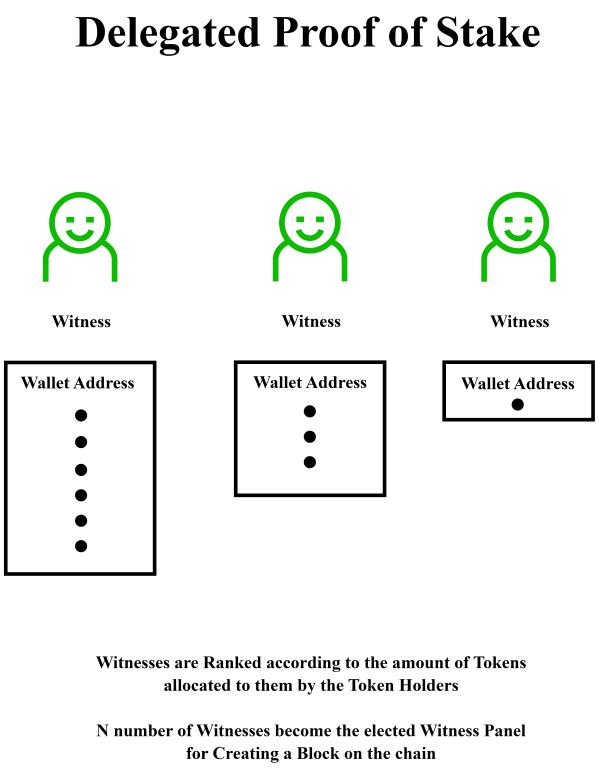

Figure 3.4: Delegated Proof of Stake Consensus Step 2

Chapter 4

Problem Statement Analysis

Land Registration systems officially record land property rights through deeds. It officially gives an Entity public ownership which has inherent rights. Current Land Registry process in Bangladesh is done physically by hand. Most to all documentations are stored physically as well. This proves to be a process containing many challenges.

4.1 Challenges in Traditional Land Registry

The main challenge Land Registration authorities face is to ensure and verify that the land is owned by the right Entity. Many properties do not have a record of ownership history as well, making it harder to determine if the land owned by the current Entity has obtained it legally in the past. Current systems, where most of the paperwork is traditional, fail to verify and prevent frauds, which leads to unauthorized sale of land assets to third parties causing financial damage and turmoil to both the rightful owner of the land and the party purchasing the land. These paper-based registration processes are also carried out in a prolonged manner, where purchases or transfers may take more than a month to process and a slight inaccuracy in land valuation could cause properties to have incorrect tax and insurance premiums[14].
Moreover, the Traditional Land Registry documentation process of Bangladesh is not dependant on a single government department, but rather has to deal with several other departments to obtain all the necessary information to be included in the registry document. This results in a more complex system with multiple failure points where a mistake can take place and at the same time requiring the entire process to take much longer time.

4.2 Challenges in Traditional Blockchain Systems

Implementation of a traditional Blockchain based system for Land Registry process could also pose challenges in such cases. Land Registry is a tedious process and has many stakeholders. There are multiple verification steps made along the way, where any of them may be subject to inaccuracy or change. Disputes with ownership of property and unreliable documentation can cause problems in time, and verifying the ownership of property can be a laborious task.

Such a complex system cannot be directly translated to traditional Blockchain systems to carry out the process of securing digital Land Registry documentation. Several changes need to be applied to common Blockchain architectures which are used mostly for Cryptocurrencies for specific applications. Proof of Work consensus can also become a hindrance than a competent consensus for such an application, as different stakeholders interact with the process at various levels with multiple classes of authority.
With PoW being incapable of generating a competent enough system which would consist of the complexities of the current Land Registry system, Proof of Stake can be explored to implement a system which can afford the intricacies of the matter. However, the implementation of both the PoW and PoS would require the general public to mine the blocks whenever a transaction takes place, and there has to be a rewarding mechanism for the entities completing the puzzle. Moreover, the computational efficiency of PoW and PoS provides a disadvantage to the entire system, regardless of if being capable of mimicking the complex Traditional Land Registry system, thus resulting in being less energy efficient.
The problems of both PoW and PoS can be overcome with the implementation of the Delegated Proof of Stake, as it follows a democratic system, perfect to integrate with systems which operates through the government in real-life. With the usage of DPoS, there will be no computational loss and therefore leading to higher energy efficiency[13]. However, the final problem which the DPoS needs to overcome is to have a system where the data access is controlled. Using a Public Blockchain with DPoS will cause problems since not all the information should be publicly available, and using a Private Blockchain will hinder with transparency and access of public information. Therefore the resulting system will be a hybrid of both Public and Private Blockchains, known as Consortium Blockchain which will have the features of a Permissioned Blockchain to give access to data to only authorized personnel.

Chapter 5

Customizing the Blockchain

As seen in the preceding chapters, the problems of the Traditional Land Registry system and Traditional Blockchain systems have been analyzed. The concluding system for the system was a Permissioned Consortium Blockchain which implements the DPoS protocol. Since the resulting system is owned by a single entity, the Land Registry Authority, as per the definition of Consortium Blockchain, the system architecture has to be customized to the needs of the higher functions and features[9].

5.1 Structure of the Block

We defined a custom block structure for our system's private ledger which can be easily integrated with the current information structure recorded physically for Land Registry purposes in Bangladesh. It follows the standard block structure of a Blockchain[5] however we have included a Target range instead of only a Lower Hash Target Limit which a standard Blockchain has. For our consensus Protocol, we have also included a Start Value and End Value for Miners to Mine in a range if the work is divided within Miners.
The main block structure of the Blockchain is:

Block Number 000000	
Hash	256bit Hash
Upper Limit	Upper Target
Lower Limit	Lower Target
Start Value	Start limit
End Value	End limit
Block Data	

Table 5.1: Main Structure of a Block

Block Data consists of all information required for a transaction between two entities who is purchasing or selling Land Assets and registering them. The Specifics part of Block data consists of all the information required for Land Registry.

Block Data	
txID	Transaction ID
from	Seller
to	Buyer
Specifics	Land Information
File	Filename
ext	File extension
Nonce	value
Previous Hash	256bit Hash
Timestamp	Time/Date

Table 5.2: Structure of Block Data

Specifics	
Daag	Land ID
Mouza	Area information
Khatian	Khatian ID
Khazna	Tax Information
DCR	Documentation
Porcha	Ownership History

Table 5.3: Structure of Specifics

5.2 System Architecture

The proposed model of blockchain implementation of Land Registry document involves zoning, server hierarchy and blockchaining. In this model, involvement of financial institutions which are involved in land transaction is essential to overcome the Majority attack that is otherwise possible if the entire system had been based on a model where the Land Registry authorities are in complete control. Provided the involvement of financial institutions and the requirement of a distributed network of computers which will be mining to create blocks, the proposed model contains a hierarchy of servers, from here on to be called nodes, to implement a small degree of control while still maintaining the consensus protocol which is the core of a blockchain system.

The entire model architecture has been constructed based on six core focuses:

- Data Security
- Data Backup
- Data Immutability
- Data Synchronicity
- Separation of Concern
- Reduced Response Delays

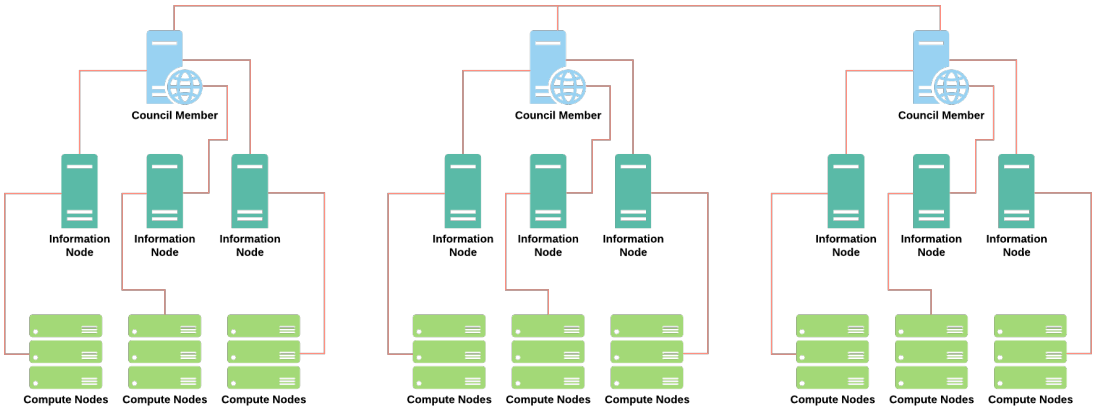

Figure 5.1: Server architecture of the proposed model

5.3 Zoning

Focusing on data security, data backup, faster response time and separation of concern, the model contains division of the geographical locations of Bangladesh into different area units, to be called "zones". Each of the zones will contain a hierarchical system of nodes which are disconnected to all the zones except for one single point of connection. For ease of zoning, the method behind zoning is based on an existing official model of area separation of a country which divides the geographical locations into the largest unit. In the case of Bangladesh, each zone will be considered to each of the divisions of Bangladesh and therefore will result in eight different zones.

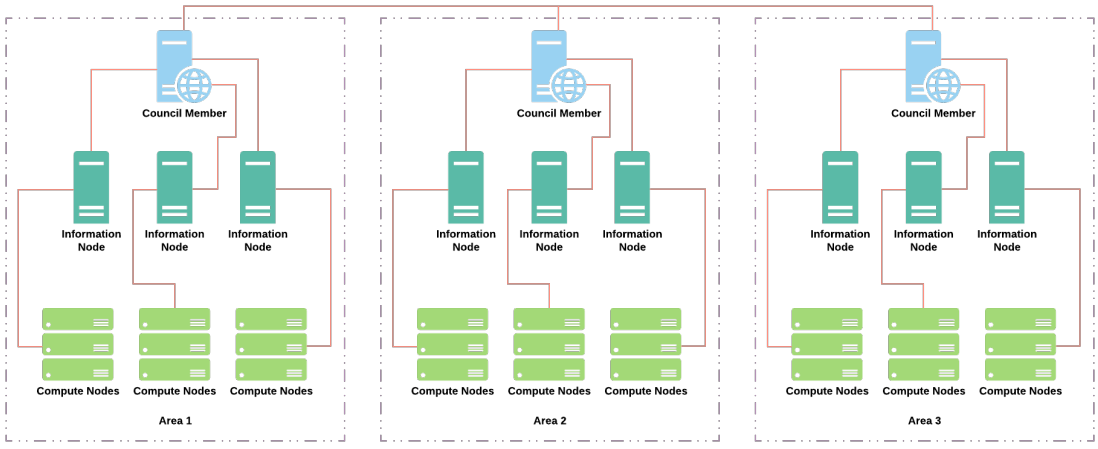

Figure 5.2: How the servers are Zoned in the proposed model

5.4 Node Hierarchy

In the proposed model, a three layer hierarchy is constructed within the system architecture. Hierarchical models presents an aspect of authoritative control to a

certain degree over other nodes and is limited by consensus protocol. The three proposed nodes and their respective responsibilities are as follows:

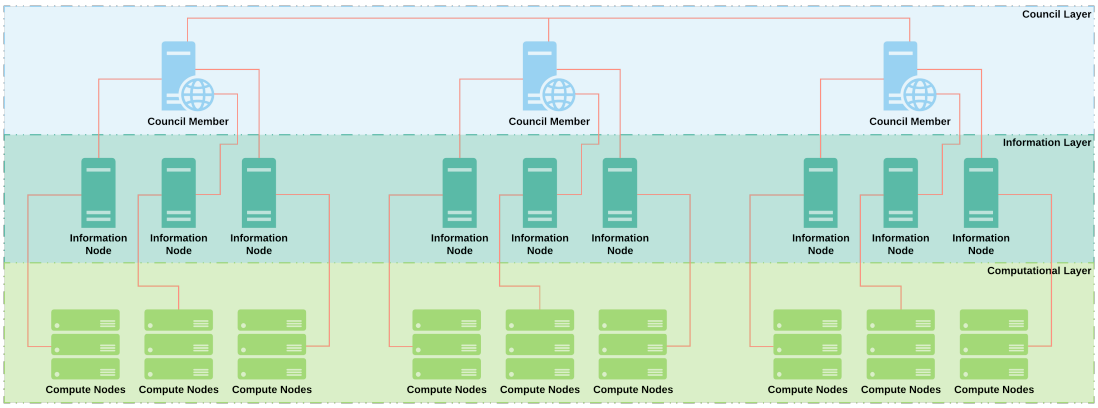

Figure 5.3: Server Hierarchy of the proposed model

Computational Nodes: These are regular mining computers which will mine a block whenever the Council Node sends out a mine command. These computers will be controlled by local land registry authorities and financial institutions involved in land transactions. In a particular zone, there will be several Computational Nodes to ease the mining process. These computers will also contain the blocks of all previous transactions without the information in it, these blocks will only contain the previous hash and the current hash pertaining to the transactions of the zone in which it belongs. The Computational Nodes are the lowest level of computers in the hierarchy and are only connected to particular Information Nodes. Computational Nodes are comparable to miners of a general DPoS system where their job is to mine blocks whenever they have won in a vote.
Information Nodes: These are larger servers with greater storage and computational capacity and placed above Computational Nodes in the hierarchy. Information Nodes are responsible to store the complete information of transactions that has happened. There are a few Information Nodes per zone and they are connected to several Computational Nodes. All the Information Nodes of a particular zone are connected to each other and also with the Council Node of that zone. Information Nodes are also responsible to relay commands from the Council Node to the Computational Nodes and to check the validity of the transaction information and verifying the transaction request before sending to the Council Node. These Servers will also aid in the maintenance of the consensus protocol between all the nodes in the zone and maintain the integrity of the chain in a zone. The Information Nodes will be controlled by financial institutions which are involved with land transaction dealing. Information Nodes are comparable to the witnesses of a general DPoS system which can switch its own role between a witness and a miner.
Council Nodes: For each zone, there will be exactly one Council Node which is controlled by government authorities. The Council Nodes of each zone is connected to the Council Nodes of other zones, and to the Information Nodes of the zone in which it belongs. The primary task that this node performs is to provide approval for the mining of a block whenever a transaction is reported and commands the rest of the nodes of its zone to start mining based on that information. Furthermore, whenever

it receives a mine request, it sends the information to the other Council Nodes in the other zones for safekeeping and to cross check if the information has been tampered with while the block is being mined. The Council Nodes are also responsible to keep the complete information of all the transactions for every zone so that the consensus protocol can be maintained for each of the Master Nodes in each zone. The council nodes will be hosting the DApp through which all the information will be entered and transaction requests are made. Council Nodes are comparable to the Delegates of a general DPoS system, where they vote for the node which will mine the block.

5.5 Architectural Limits and Scalability

Owing to the fact that the proposed system architecture has three leveled hierarchy and needs to have an uneven number of nodes to enable successful Byzantine Fault Tolerance, there is a requirement of a minimum number of nodes to implement this architecture and to scale it to greater extents. For the successful implementation of this architecture a minimum of thirty-nine (39) nodes are required in the minimum architecture which are divided across a three (3) zones. Each of the zones in the architecture has the following node structure:

- **One** (1) Council Node
- **Three** (3) Information Nodes
- **Nine** (9) Computational Nodes, where there are **three** (3) Computational Nodes under each Information Node

The scaling of this architecture can occur in one of three ways:

- Incrementing Councils: To scale using zone-wise, exactly two zones with the minimum architecture needs to be added to the existing architecture. Therefore, after an initial **thirty nine** (39) nodes architecture, the next zone-wise scaling will contain a total of **sixty five** (65) nodes with a total of **five** (5) zones.

- Incrementing Information: To scale using Information nodes, exactly **four** (4) nodes needs to be added to under any of the Council Nodes, where **one** (1) will be Information Node and the other **three** (3) nodes are Computational Nodes. Therefore, there will be a cumulative of **forty three** (43) nodes after the initial minimum architecture when incrementing Information.

- Incrementing Computes: To scale using Computational Nodes, exactly **two** (2) Computational Nodes needs to be added to under any of the Information nodes in any order at each scaling. Therefore, scaling the minimum **thirty nine** (39) nodes architecture will result in **forty one** (41) nodes where there will be either **two** (2) Information Nodes with **four** (4) Computational nodes or **one** (1) Information Node with **five** (5) Computational Nodes.

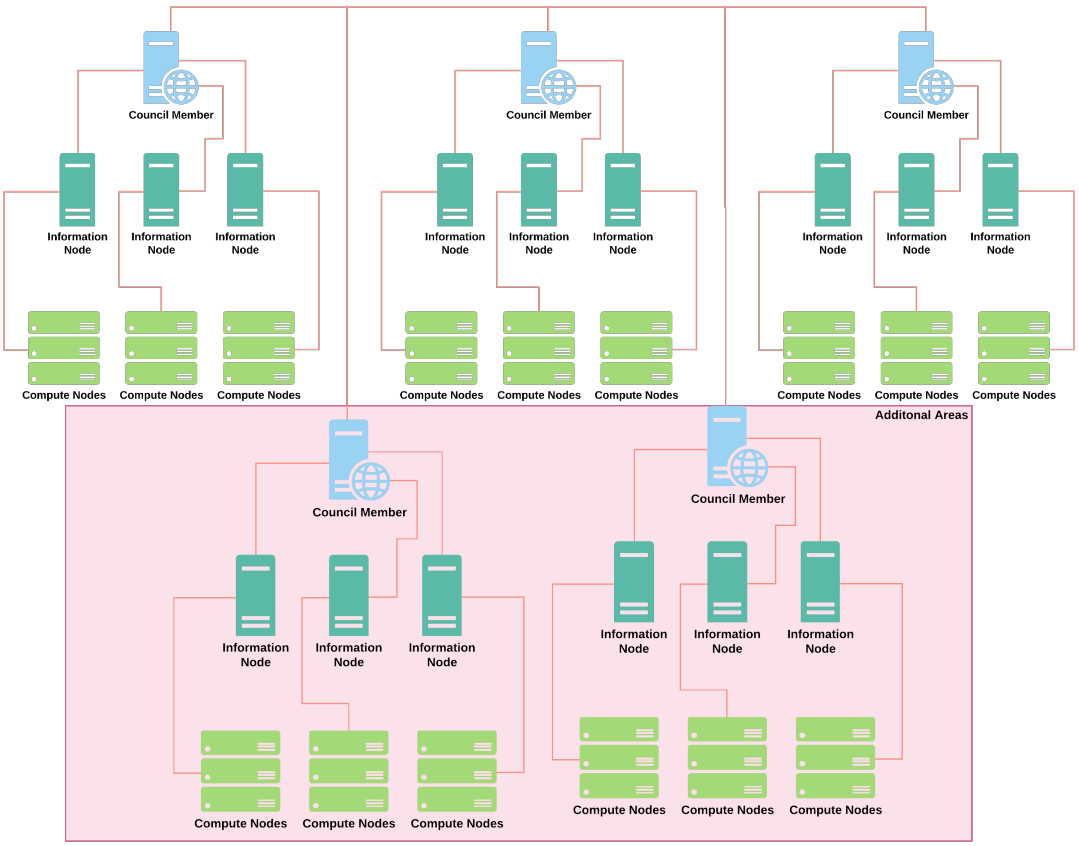

Figure 5.4: How zone-wise scaling works

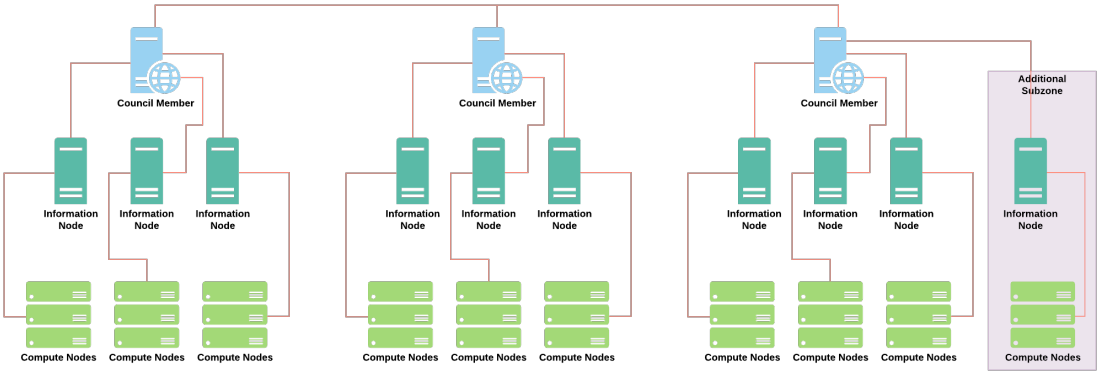

Figure 5.5: How information-wise scaling works

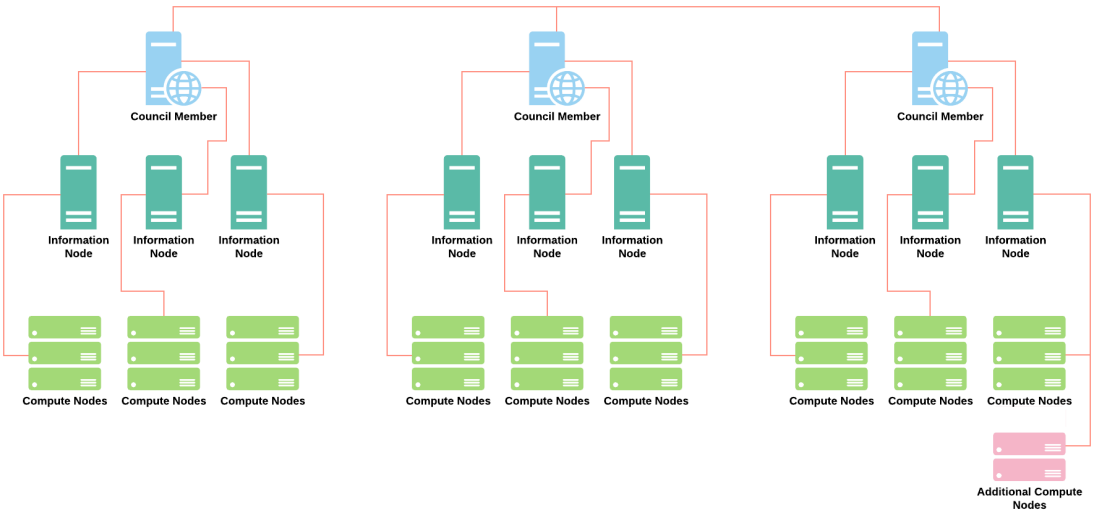

Figure 5.6: How compute-wise scaling works

Chapter 6

Council Protocol

With the overall problems of the Traditional Land Registry system, Traditional Blockchain and the proposed system architecture in mind, the regular consensus protocol would fail to serve the purpose of identifying the problem at hand. Therefore a new Blockchain protocol is required which will bypass all the stated parameters and encompass the problems completely. The proposed Council Protocol will circumscribe all the aforementioned parameters with components of the Consensus Protocol to overcome the problems faced in it as well as allow for data immutability as well as add a new paradigm of authorized accessibility to data.

6.1 Democratic Consortium

Enabling a democratic system, where votes is the determining factor, in a consortium based system, where the existing members are fixed, is one of the major problems which needs to be addressed in the beginning. Since the consortium members are fixed, therefore the Council Protocol holds the consortium member nodes as the Council Nodes which will be the ones electing the miners. The Council Protocol keeps the roles of the nodes the same, therefore adhering to the Consortium structure. This means that a node which started off as an Information Node will remain to be an Information Node, and a node which starts as a Computational Node will remain to be a Computational Node throughout. The consortium becomes democratic through the action of the Council Nodes which elects the Computational Node which will mine a particular block. Therefore, whenever traction(s) needs to be mined to be added to the Blockchain, the Council Nodes holds an election to elect a single Computational Node in any of the zones under any of the Information Nodes present in the current architecture.

6.2 Tiered Genetic Election/Delegation

Following the process of Genetic Algorithm as developed by Professor John Holland[1], the Council Protocol takes an initiative to randomize the election/delegation process. During the election process, the Council Node receiving the transaction request, generates a randomized array of n - 1 zones, where n represents the total number of zones, and proposes this array to the other Council Nodes each of which then randomly elects one member of the randomized array. If the resulting election

results in a majority number of votes for any of the zones, the next election proceeds, otherwise the initial Council Node randomly removes one of the zones and hold the first tier election again, repeating the process unless a majority zone is elected. Completing the first tier election, the second tier begins where the initial Council Node generate a randomized array of [m - 1] of Information Nodes, where m is the total number of Information Nodes under the Council Node of the elected zone. The second tier election occurs in a manner identical as the first tier, which then proceeds to the third tier of election where the candidates of the election are a randomized array of [p - 1] Computational Nodes under the elected Information Node, which are elected identically to the first and second tier election. The resulting Computational Node after the three tiered genetic election gets delegated to mine the block of the incoming request. The elected Computational Node is sent the data for the block including a timestamp and a randomly generated difficulty/upper limit.

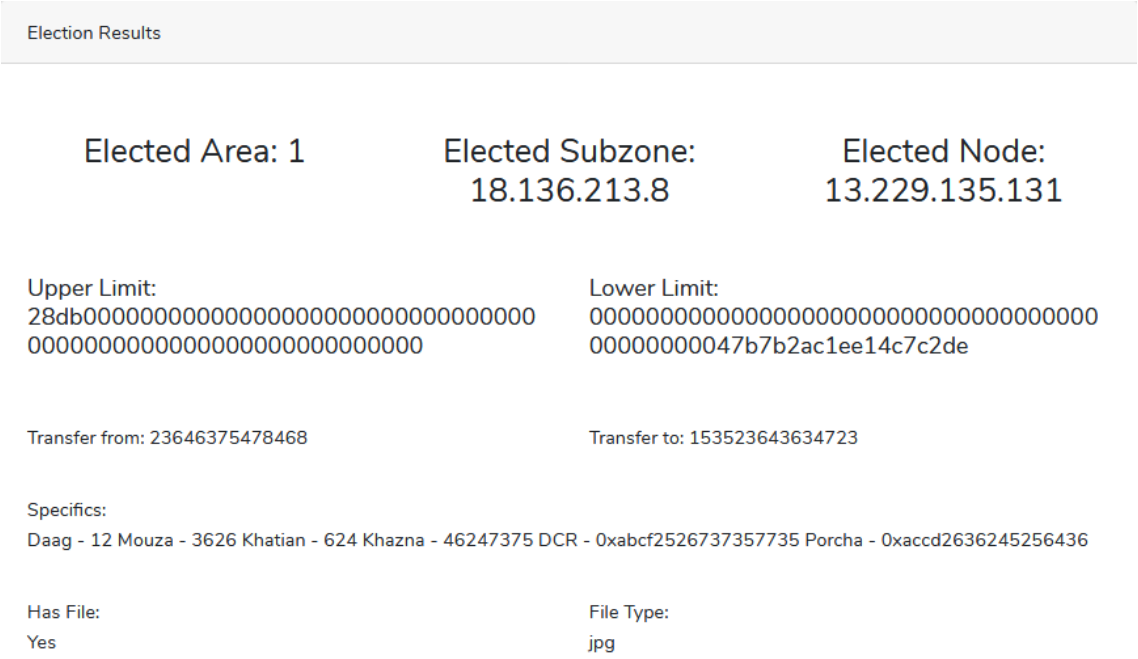

Figure 6.1: Node Election Proccess Breakdown

6.3 Consented Mining

Upon receiving the data from the initial Council Node, the elected Computational Node performs tests to check the integrity of the chain that it contains and to update it in the case of corruption in the chain. The elected Computational Node generates a randomized list of nodes from the set of all the nodes existing in the architecture excluding itself, which numbers between (x / 50 + 1) to (x * 0.75), where x is the total number of nodes in the current architecture. All the nodes in the list are then requested to send the hash of the latest block added to their chain, after which the majority of the latest hash is found. The elected Computational Node compares its own latest hash in its own chain to the majority chain to find if there is a discrepancy in its own chain. In the case that a discrepancy exists, the elected chain drops its

own chain and copies the chain from any of the nodes containing the majority hash. Finally, the elected Computational Node mines the data within a given time frame and send the mined block to this controlling Information Node after validating, where the block gets re-validated by the Information Node and start the chaining protocol.

6.4 Sub-zone Locking

If the elected Computational Node fails to mine the block within the given time limit, it sends out a request to its controlling Information Node with the final nonce that it has calculated. This triggers a subzone that the elected Computational Node belongs in (the Information Node of the elected Computational Node and its and its sibling Computational Nodes). The subzone's Information Node notifies its own Council node to lock the subzone so that it gets excluded from any election until the current block is mined, at the same time the Information Node changes its own status from a witness to a miner. The now miner Information Node delegates all the Computational Nodes under it to start mining the block at non-overlapping ranges of the nonce outside of the nonce limit that has already been computed, as well as assigns itself to start mining at a non-overlapping range of nonce. As soon as any node within the locked subzone finishes successfully mining the block, the Information Node gets notified and normal chaining procedure begins but unlocking the subzone.
During the subzone locking, if any of the nodes in the subzone are busy, the computing a block, the Information Node finds a subzone across all the zones which is fully free to be locked. This subzone will function normally through the subzone locking protocol until the block has been successfully mined.
There is also a limit to the maximum time that any subzone can stay within the subzone locked stated. In the case that the subzone exceeds the time limit, the Information Node sends the data its respective Council Node as a mimicking a user request so that all the data remains the same other than the timestamp and the difficulty/upper limit and the entire Council Protocol restarts for this transaction data.

6.5 Chaining Protocol

The chaining protocol always begins at the Information Node of the elected Computational Node or subzone, where the Information Node will first validate the nonce and hash. In the case the nonce and hash are not valid; the Information Node sends back a request to continue mining. However, with a valid nonce and hash, the Information Node will send a request to perform locking the databases of all the nodes along with a timestamp, which ensures that no race conditions occur and thus not creating false sub chains in the nodes. After the database lock has been confirmed, the Information Node will send out a request to all of its adjoining nodes to add the mined block to their chain. The nodes receiving this request will add the block to their own chain, and at the same time if the node was mining, the referenced previous hash will subsequently change to the now newly added block and will start mining from the beginning.

Once all the nodes successfully adheres to the chaining command, the requesting Information Node will then send requests to unlock the database of all the nodes so that normal processes can continue.

Chapter 7

Conclusion

If Blockchain technology is applied to the existing Land Registry system for registration and verficiation purposes, it would yield us the following benefits:

- Land transaction process time reduced to a few days instead of months.
- Verification of ownership is accurate and fast.
- Completely digital system without the need of much paperwork.
- No missing documentations as everything will be registered into the Blockchain during a transaction/registration.
- High security and prevents fraud.

Land Registry being manual, is a rigorous process to deal with in Bangladesh. By digitizing this process and using Blockchain to store the transactions and documents, we make this system more transparent, simpler, more secure and faster to process. Blockchain technology has come a long way and it is only going to improve further. Newer consensus algorithms will give us a better advantage at dealing with conflicts and attacks while at the same time reduce the computational power needed to run the chain but increasing output. As this technology is rapidly evolving in the current environment, we hope to conquer the challenges regarding compatibility with existing technologies; cost efficiency and conflicts are handled properly.

References

[1] J. H. Holland, "Genetic algorithms", *Scientific american*, vol. 267, no. 1, pp. 66–73, 1992.

[2] D. Bayer, S. Haber, and W. S. Stornetta, "Improving the efficiency and reliability of digital time-stamping", in *Sequences II*, R. Capocelli, A. De Santis, and U. Vaccaro, Eds., New York, NY: Springer New York, 1993, pp. 329–334, ISBN: 978-1-4613-9323-8.

[3] R. Schollmeier, "A definition of peer-to-peer networking for the classification of peer-to-peer architectures and applications", Sep. 2001, pp. 101–102, ISBN: 0-7695-1503-7. DOI: 10.1109/P2P.2001.990434.

[4] A. Back, "Hashcash - a denial of service counter-measure", Sep. 2002.

[5] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system", *Cryptography Mailing list at https://metzdowd.com*, Mar. 2009.

[6] G. Bertoni, J. Daemen, M. Peeters, G. Assche Van, and R. Keer Van, "Keccak implementation overview", 2012.

[7] S. King and S. Nadal, "Ppcoin: Peer-to-peer crypto-currency with proof-of-stake", 2012.

[8] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A provably secure proof-of-stake blockchain protocol", in *Advances in Cryptology – CRYPTO 2017*, J. Katz and H. Shacham, Eds., Cham: Springer International Publishing, 2017, pp. 357–388, ISBN: 978-3-319-63688-7.

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

[10] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. D. Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolic, S. W. Cocco, and J. Yellick, "Hyperledger fabric: A distributed operating system for permissioned blockchains", *CoRR*, vol. abs/1801.10228, 2018. arXiv: 1801.10228. [Online]. Available: http://arxiv.org/abs/1801.10228.

[11] J. Brown-Cohen, A. Narayanan, C. Psomas, and S. M. Weinberg, "Formal barriers to longest-chain proof-of-stake protocols", *CoRR*, vol. abs/1809.06528, 2018. arXiv: 1809.06528. [Online]. Available: http://arxiv.org/abs/1809.06528.

[12] D. Core Group, "Dash: A payments-focused cryptocurrency", 2018. [Online]. Available: https://docs.dash.org/en/stable/introduction/about.html.

[13] G. Chaumon, P. Bugnot, Z. Hildreth, and B. Giraux, "Dpops: Delegated proof-of-private-stake, a dpos implementation under x-cash, a monero based hybrid-privacy coin", Jul. 2019. [Online]. Available: https://x-network.io/whitepaper/XCASH_Yellowpaper_DPoPS.pdf.

[14] M. S. Islam, "Land verification system using blockchain technology in bangladesh", Nov. 2019. [Online]. Available: https://medium.com/coinmonks/land-verification-system-using-blockchain-technology-in-bangladesh-f718ebd39f13.

[15] H. MÜLLER and M. SEIFERT, "Blockchain, a feasible technology for land administration?", 2019. [Online]. Available: https://www.fig.net/resources/proceedings/fig_proceedings/fig2019/papers/ts01i/TS01I_seifert_mueller_10110.pdf.