A Hybrid POW-POS Implementation Against 51% Attack in Cryptocurrency System

Abdur Rahman
Student Id: 012153013

A Thesis

in

The Department

of

Computer Science and Engineering

Presented in Partial Fulfillment of the Requirements

For the Degree of Master of Science in Computer Science and Engineering

United International University

Dhaka, Bangladesh

July 2019

© Abdur Rahman, 2019

Approval Certificate

This thesis titled "**A Hybrid POW-POS Implementation Against 51% Attack in Cryptocurrency System**" submitted by **Abdur Rahman**, Student ID: **012153013**, has been accepted as Satisfactory in fulfillment of the requirement for the degree of Master of Science in Computer Science and Engineering on 16th July 2019.

Board of Examiners

1.

_____ Supervisor

Prof. Dr. Mohammad Nurul Huda
Professor & Director - MSCSE Program
Department of Computer Science and Engineering
United International University
Dhaka, Bangladesh

2.

_____ Head Examiner

Prof. Dr. Salekul Islam
Professor & Head of the Dept.
Department of Computer Science and Engineering
United International University
Dhaka, Bangladesh

3.

_____ Examiner-I

Prof. Dr. Khondaker Abdullah Al Mamun
Professor & Director - AIMS Lab
Department of Computer Science and Engineering
United International University
Dhaka, Bangladesh

4.

_____ Examiner-II

Mr. Mohammad Mamun Elahi
Assistant Professor
Department of Computer Science and Engineering
United International University
Dhaka, Bangladesh

5.

_____ Ex-Officio

Dr. Swakkhar Shatabda
Associate Professor & Undergraduate Program Coordinator
Department of Computer Science and Engineering
United International University
Dhaka, Bangladesh

Declaration

This is to certify that the work entitled "**A Hybrid POW-POS Implementation Against 51% Attack in Cryptocurrency System** " is the outcome of the research carried out by me under the supervision of Prof. Dr. Mohammad Nurul Huda, Professor & Director - MSCSE.

_____

Abdur Rahman
012153013
Department of Computer Science and Engineering
United International University
Dhaka, Bangladesh

In my capacity as supervisor of the candidate's thesis, I certify that the above statements are true to the best of my knowledge.

_____

Prof. Dr. Mohammad Nurul Huda
Professor & Director - MSCSE Program
Department of Computer Science and Engineering
United International University
Dhaka, Bangladesh

Abstract

Blockchain and cryptocurrencies are drawing more and more attention among the people, due to the overwhelming success of Bitcoin in the market. The success and popularity of Bitcoin mainly focuses the underlying blockchain technology which is totally immutable distributed ledger, highly secured by its P2P network consensus named Proof of Work (PoW). One of the worst threats to a Proof-of-Work based cryptocurrency is 51% attack. If one or more dishonest network peer gains more than 50% of resource such as processing power, then they will become the majority decision maker in the network. Because in this kind of network, peers are competing for faster processing. The peers who have more processing capabilities can mine more blocks than others. They can easily manipulate the block chain by creating fake transactions, fraud other users even cause large scale financial damage to the exchanges. We'll describe this majority attack in detail in chapter 2. There are several researches have already been done on how to prevent this attack and most of them suggest mixing of two or more proof of resource to form a hybrid protocol to tackle this attack. It is already proved that mixing of two or more existing protocol that is called hybrid protocol can make the network enough resistive to this attack. The recent implementations of hybrid protocols have other limitations and problems that they are facing and striving to resolve. Some of them introduce voting system, ticket distribution system, penalties, special nodes and block validator groups for preventing the malicious activities. All these implementations are successful to protect the network from 51% attack. But their main weakness is in distribution of block mining reward to the investors. From the perspective of an investor, an investor invests his hard-earned money in a cryptocurrency for making proper profit from his investment. The main source of this profit is the block reward which is generated and given to the miner on successful mining of a block. So, to ensure this profit is given to proper user on proper time interval, the consistency of block generation time interval is a vital factor. The voting system, ticket system etc. are not time controlled and over all block reward generation interval will not show a uniform distribution of profit. Another big issue is diversifying the peers by creating special committee and groups of validators the concept of P2P network is violated. In this paper we'll describe a step by step process to implement a Hybrid PoW-PoS based consensus protocol. In our proposed system, the

PoW mining process is only used to regulate the block generation time. The actual block generation is done by the same user with PoS consensus mechanism. There is no voting or validating committee. The entire network will validate each block. This is the major difference with other discussed system. The system will not only be able to tackle the 51% attack, it provides a uniform distribution of mining reward to the stake holders and investors by maintaining a precise block generation interval with difficulty adjustment in PoW mining and probability calculation for stake holders according to their matured staking balance. We'll not only show how to make the system non-vulnerable to this attack but also describe in detail about how to validate the transactions and blocks in different stage of creating the block chain.

Acknowledgement

First of all, I would like to thanks the almighty Allah for giving me the capability to participate in higher study after a long gap from my graduation.

Then I would like to thanks my supervisor Prof. Dr. Mohammad Nurul Huda sir, because without his help and well guided supervision, it wouldn't be possible to complete this paper.

I also would like to acknowledge from the bottom of my heart to Prof. Dr. Salekul Islam Sir, Prof. Dr. Khondaker Abdullah Al Mamun Sir, Mr. Mohammad Mamun Elahi sir and Dr. Swakkhar Shatabda sir for their wise advices, guidelines and encouragements to complete this paper.

Also, I acknowledge the open source .Net C# based platform Stratis. I used this platform for creating the cryptocurrency. They provide a huge collection of well-organized code blocks, NuGet packages and DLLs to make it easy for .Net developers to work on blockchain based application. Most of the codes in this project are lent from this open source platform.

And at last but not the least I would like to be thankful to my wife Fatema Parveen and my son Dhrubo Ehan Rahman for cutting down their deserved time for my study, for their continuous support and being always by my side to make me their hero in every part of our life.

Table of Contents

List of Tables

List of Figures

Chapter 1

Introduction

The blockchain and cryptocurrency are the two most discussed buzz word in the industry of software and technology. Although the concept is not recent, the first cryptocurrency came out under the lime light in 2008 and ten years already gone. Many cryptocurrencies are running in the market and some of them are getting more attention and popularity among the people. During this tenure, there are a lot of researches took place and the technology is now grown up in different dimensions. The core functionality of a blockchain based cryptocurrency is its network consensus mechanism. There are several consensus mechanisms evolving in this sector. As the cryptocurrencies are evolving in the market, they also faced different kind of attacks. One of the most dreadful attack which caused some cryptocurrencies great damage is 51% attack [3][4]. A 51% attack on a cryptocurrency network causes unwanted forks, fraud transactions, double spending of same money [18] and many more malfunctioning occurrences which could cause huge damage to the network and eventually collapses the currency. Existing all of the research papers are written on different aspects of blockchain, consensus, block generation parameters, cryptographic algorithms, fraud detection technologies, attacks, the remedy of the attacks etc. There are several theoretical works and many more granular level research works has been done. Some of those study tackle this attack but they arise other issues which are described in further section of this paper. In this paper we decided to illustrate a step by step process of mining and validation of a Hybrid consensus protocol which could be used to prevent a 51% attack on the network. The proposed system will implement a hybrid of Proof of Work and Proof of Stake consensus algorithm which could possess enough resistance to 51% attack. The paper is organized in such a way to present all the relevant terminologies, theories, actors and protocols of the literature in a comprehensive manner, then describe the present situation of the implemented algorithms and their prospects on the problem and then prescribe a solution for the problem. In chapter 2, we present the background of the study and put light on different components, concepts and terminologies of the entire system to make a firm understanding on the problem and the prescribed solutions. At the end of this chapter, we describe what is a

51% attack and what effects it could make on the network. Then we discuss and put light on the present solutions, prospects of those works and limitations they are facing by presenting a comparative analysis on them. Chapter 3 is organized to present our proposed solution in a couple of sections where our proposed algorithm of Hybrid Mining is presented in a step by step algorithmic manner with firm detail of each steps. The chapter 4 shows the result and analysis of the implemented method. At last, chapter 5 consists the concluding discussion on the entire process.

Chapter 2

Background and Literature Review

2.1 Fundamental Concepts and Terminologies

In this section we'll discuss about the fundamental knowledge on the underlying concepts of technologies used in this research. So that the audience will have adequate background on the topic to understand the phenomena perfectly.

2.1.1 Blockchain

In simple words blockchain is a special kind of database system which could store any kind of data in a highly secured manner. Block chain is a constantly growing irreversible chronological ledger which is permanent and secured with cryptographic algorithms, hashes and signatures. It is called modern distributed ledger technology. By design, a blockchain is resistant to modification of data. From the perspective of its construction, it is a chronological chain of records called blocks. Commonly each block consists a block Id which is a cryptographic hash of the block data, the Id of previous block and some other relevant fields like timestamps, block data etc. In cryptocurrencies, the block data consist the transactions.

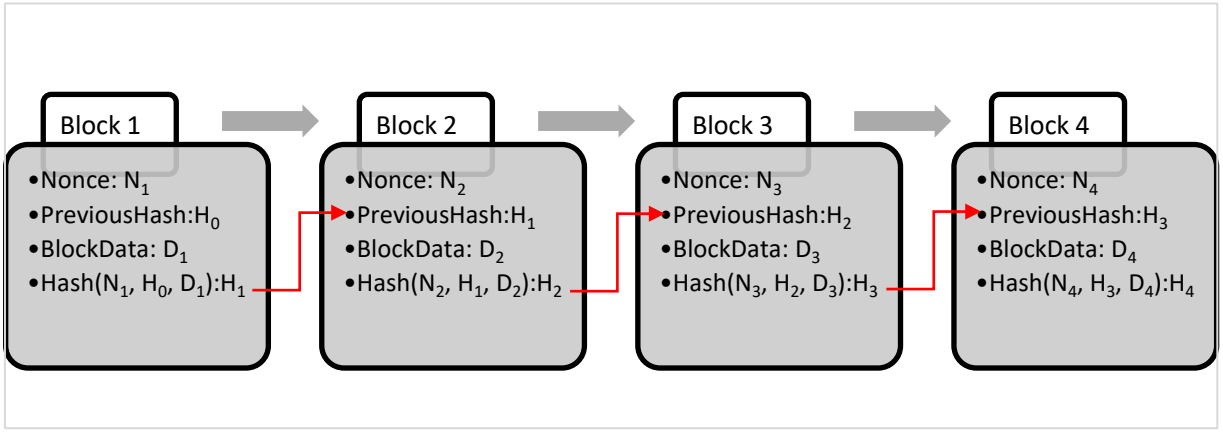

Figure 1: Block Chain Illustrated

The consistency of data is maintained by cryptography. Suppose, Block-1 consists a chunk of data X_1 = “abcd”, previous block hash P_1 = “mnop” and its generated hash value $H_1(X_1P_1)$ = “qrst". Block-2 consists a chunk of data X_2 = “efgh”, previous block hash P_2 = “qrst” and generated hash $H_2(X_2P_2)$ = “uvwx”. Now if someone changes a bit of data in Block-1, then its hash H_1 will be changed. As the hash H_1 is propagated to the next block, the hash value of next block will also be changed. This change will be propagated to the last block of the block chain and the entire trailing chain will be changed. If someone changes a bit of data of a certain block then it affects the entire trailing chain to be invalid. That’s why it is called immutable data structure [3].

Traditional centralized databases are employed for many years by the governments, banks and financial institutions to store data and record transactions of any kind. The data and records are enclosed and carefully guarded by authorized systems where only authorized operators are permitted to make entries and govern the accuracy of data stored in the system.

Blockchain is a purely distributed digital ledger that is stored in a network of computers around the world. Instead of securing data by restricting access, the blockchain data is shared amongst all the users of the network [2]. If the data in the blockchain has been tampered by some node in the network, all the other nodes will oppose to accept this change as it won’t match with the copy of other nodes. They immediately ban the node and broadcast the banning message to all other connected peers. Thus, the network guarantees the integrity of data.

2.1.2 Cryptocurrency

Cryptocurrencies are digital assets used to exchange values between different parties. The main advantage of this cryptocurrency system is the absence of any third-party regulation. That means there is no bank or any financial organization in between the two parties dealing the exchange. The transactional data are stored in block chain and maintained by a network of users.

2.1.3 Peer-to-Peer (P2P) Network

Blockchain protocol operates on a peer to peer network. It is called peer to peer because each node in the network has the same priority and privileges from the perspective of the

protocol. Each node is treated in same manner inside the network and they provide same kind of service to the network. There is no discrepancies, discrimination or hierarchy among the nodes in the network. Each peer connects with several similar peers to form the entire network. A peer can propagate transactions and blocks to all the participants of the network by broadcasting them among the peers it is connected. Then other connected peers validate them and broadcast them to the connected peers of them. Thus, a transaction or a block could be propagated to entire network in a very short time. All peer nodes keep all the records of transactions i.e. the entire block chain so that the integrity of the protocol could be preserved perfectly and minimizes the central point of control or manipulation by providing a firmly decentralized topology of data storage.

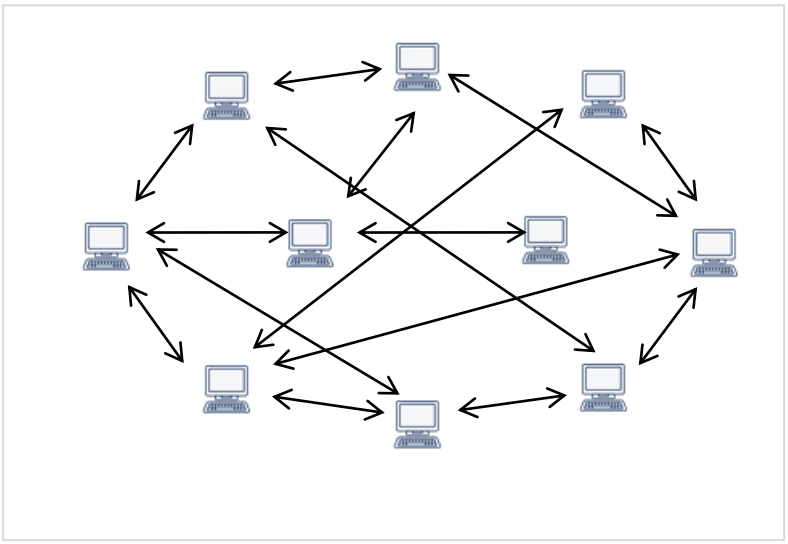

Figure 2: Peer to Peer (P2P) Network.

2.1.4 Consensus Rules and Protocol

Transactions and Blocks are created and added to the blockchain according to some agreement by all the participants. These agreements are known as consensus rules. The word consensus comes from the word consent. Consensus protocols regulate the peers to justify, validate and finalize the transactions and blocks to maintain a single chain among all the nodes. If a major disagreement ever occurs, it causes a hard fork and split the chain into two separate branches [2][5][6].

2.1.5 Longest Chain Rule

The longest chain rule state that, if there are simultaneous blocks generated by multiple nodes in parallel then the longest chain will be accepted by the network. To illustrate the that lets imagine after Block-20 three different miners simultaneously mined two different blocks Block-21_1 and Block-21_2 and broadcasted those two blocks simultaneously. Some part of the network first receive Block-21_1 accept it as it's a valid block. Similarly, some other nodes who first receive Block-21_2 accept it as it is also a valid block [22].

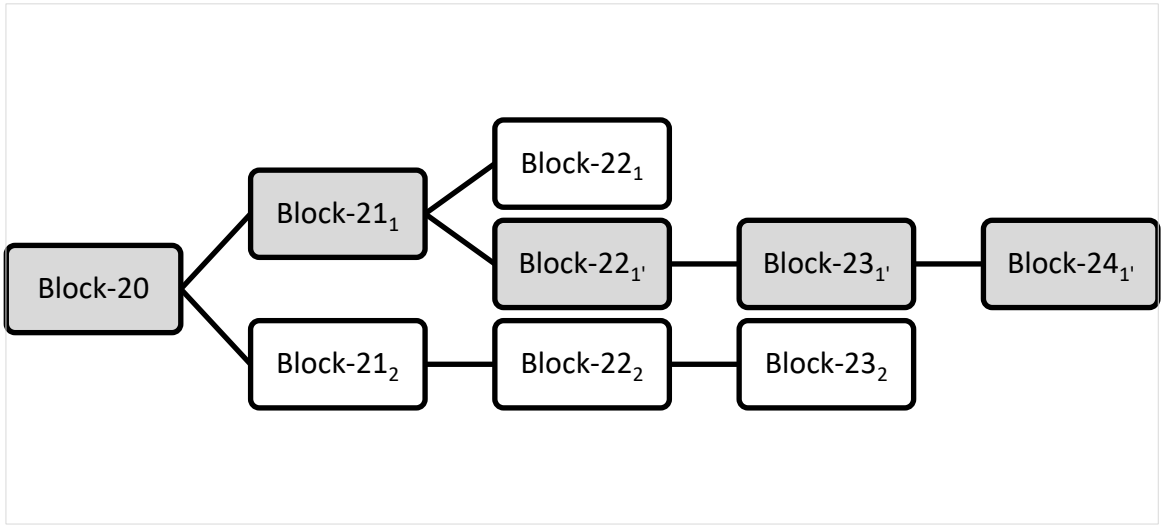

Figure 3: The Longest Chain Rule

Then both the subnetworks mine on those two different branches and continued as shown in the figure below. After some time when the network detects that a fork has been occurred due to network propagation delay or for any reason where all the sub branches are valid, then the network always goes with the longest valid chain. This rule is known as longest chain rule.

2.1.6 Hashes and Digital Signature

Hash is a special function which can map large data of arbitrary length onto data of fixed length. Hashes are special type of encrypted string which could not be reversed back to the original data. Each input data generates a certain unique hash. A little bit of change in the input data generates a totally new another hash. Hashes are used to verify data in the block chain. Digital signatures are used to verify transactions and authenticate the

ownership of users on the output of those transactions. Cryptocurrencies uses two types of unique keys: Private keys and Public keys. Private keys are used to sign the transactions. Public keys are used to generate digital addresses to receive funds.

2.1.7 Mining

Mining is one of the key concepts of cryptocurrency. Fiat currencies are created by the central banks by printing them. But cryptocurrencies are created by mining. Miners are responsible for creating and maintaining the blocks and block chain. Mining process regulates the creation and inflation of the currency [9].

2.1.8 Proof of Work

Mining means creation of a new block by finding a cryptographic hash for the block. In proof of work, the block hash must meet some criteria to be valid in the block chain. For example, in Bitcoin blockchain the block hash must start with four trailing zeros. As the block data which are actually transactional data, could not be changed, it is the nonce that the miner can change in each iteration to generate the predefined pattern of hash. All the network peers compete to find a proper nonce to generate a valid block hash. The miner who finds solution first adds the block to the chain. And announce his success to the network. Mining costs a huge computation power to the miner which involves large electricity consumption. For incentivizing the miner's effort, the system rewards the miner by generating some specific number of coins and reward the miner by giving this newly generated coins. POW mechanism totally relies on the computation power of the miner. The more computation power a miner effort the more chance it gets to mine blocks and get rewards [16].

2.1.9 Proof of Stake

Proof of stake mechanism doesn't rely on the high computation power. It works based on the staked asset of the network peers. The more asset a peer stakes the more chance it gets for mining and getting reward. This mechanism doesn't require huge computation power. Rather it requires very low computation power and thus it reduce unnecessary electricity consumption [15]. There are several drawbacks of PoS system too. Like big investors who stakes large amount of money controls the network and get the maximum benefits from the network. Thus, rich become richer. It will tend the network to be centralized

around some rich people. Also, PoS is vulnerable to a kind of 51% attack. If someone holds more than 50% wealth of the network. He can easily manipulate the block chain for his personal gain.

2.1.10 Block Generation Interval / Block Time

Block generation interval or block time refers to the average time required for a cryptocurrency network to mine a new block.

2.1.11 Coin Age

Coin age is the time duration an unspent coin is staked for. The time span an unspent transaction output is hold for staking is called its coin age [24].

2.1.12 Stakeholders Weight

The weight is calculated by multiplying the matured balance and coin age of each coin. Suppose a user has 10 coins staked for 10 days. Then its weight is 10 x 10 = 100. If a node has K number of UTXOs with C_k coin value and A_k coin age where k = 1, 2, 3… … K, then the total weight of that node is

$$W_i = \sum C_k A_k \quad (1)$$

2.1.13 Network Weight

The network weight is calculated by multiplying the matured balance and coin age of all the nodes in the network. Suppose, there are N number of nodes in the network with their individual weight W_i where i = 1, 2, 3 … … … N. Then

$$\text{Network Weight } W_n = \sum C_i A_i \quad (2)$$

2.1.14 Expected Reward Time

A node's expected reward time is the time interval after which a node expects a chance to get reward by mining a block. It is calculated in seconds by dividing the network weight with the nodes own weight.

$$\text{Expected Reward Time } T = W_n / W_i \quad (3)$$

2.1.15 Memory pool

Memory pool is a physical memory storage where the transactions are stored before it is being added to a block. When a transaction takes place, first it has to pass a lot of validation process call pre-memory-pool validations. After pre-memory-pool validation the transaction is stored in the memory pool. Then the network peer broadcast the transaction. All the other peers then receive the transaction and run the validations. After passing the validations the transaction is added to the memory pool of the respective peer. In most of the cases, an invalid transaction is discarded before added to the memory pool [27][28][29].

2.1.16 Transaction

Each transaction consists inputs and outputs. The transaction outputs could be spent by the receivers of the current transaction. The previous transactions outputs are considered as the input of the next transaction [30][31]. An example could better illustrate the process:

Suppose Ali receives 5000 coins by someone in transaction Tx-1. That means Tx-1 has an output indicating 5000 coins owned by Ali's address. Now Ali sends 2000 coin to Bali by making transaction Tx-2. So, Tx-2 consists Tx-1's hash as its input TxIn-2.1. Tx-2 consists 2 outputs TxOut-2.1 and TxOut-2.2. TxOut-2.1 indicates the 2000 coins owned by Bali's address and TxOut-2.2 indicates the rest 3000 coins owned by Ali's address.

2.1.17 Unspent Transaction Output (UTXO)

UTXOs are those outputs of transaction which aren't still spent by the owner. UTXO consists a pair of transaction Id and order number together with the associated coin value. Each valid coin in the blockchain is represented by some UTXO.

2.1.18 Spent Transaction Output (STXO)

When a transaction output is used for spending in further transaction, it is called STXO. STXOs always represent previous transaction Ids which are already spent.

2.1.19 Coinbase Transaction

The Coinbase transaction is a special transaction which doesn't consist any input transaction reference. It is used to reward the miner for mining blocks in Proof of Work based system.

2.1.20 Coin-stake Transaction

The Coin stake transaction is also a special transaction which doesn't consist any input transaction reference. It is used to reward the stakeholder for staking coins in Proof of Stake based system.

2.1.21 Ancestor Transaction

Ancestor of a given transaction is another in-memory pool transaction that the given transaction depends on.

2.1.22 Descendant Transaction

Descendant refers to in-memory pool transactions those depend on a given transaction.

2.1.23 Coin-Stake Kernel

Coin-stake kernel is a special UTXO that generates a block hash less than the target difficulty hash successfully.

2.1.24 Transaction Fee and Fee Rate

Each transaction in the network costs some processing for the validation of the transaction. Moreover, the peer node that integrates the transaction into a block and mine the block solves complex cryptographic mathematics and processing tasks. To incentivize this work, the sender of the transaction is charged a fee that is to be paid to the miner. This charge is called transaction fee. Transaction fees are calculated by the processing cost of a transaction. It is proportional to the size of the transaction. Fee rate is the rate of charged per kilobyte of virtual size of the transaction.

2.1.25 Coin View

Coin view is the set of all unspent transaction outputs in the block chain. It keeps track of all the coins spendable at the consensus tip. When creating new blocks after completing all the validation steps, the coin view has been updated by recalculating all the UTXOs and STXOs in the new consensus.

2.1.26 Consensus Tip

Consensus tip refers to the height of the block chain at which a consensus has been reached i.e. all the nodes are agreed up to this height of block chain.

2.1.27 Chained Header Tree

Chained header tree is a tree structure consisting only the header information of each block. It keeps all the alternative chains. Sometimes it seems that a new alternate chain's tip is ahead of the consensus tip. If the chain header tree detects such alternate chain. It adds the alternate chain with the tree and the node starts validating that chain. If all validation passed then the consensus will move towards the alternate chain.

2.1.28 Check Point

Check point is a special point in block chain at which the chain cannot be reorganized behind anymore. In other words, the block chain is finalized and unalterable before the checkpoint height.

2.1.29 Merkle Tree and Merkle Root

Merkle trees are tree structures constructed with the hashes of all the transactions in a block. All the transaction hashes are included in the leaf level of the tree. Then the next parent level of the tree is constructed by generating hashes of each two conjugated hashes in the leaf level. Similarly hashing continues until the root level of the tree. The hash at the root of the tree is called Merkle root [23]. The following figure-4 depicts a Markle-Tree.

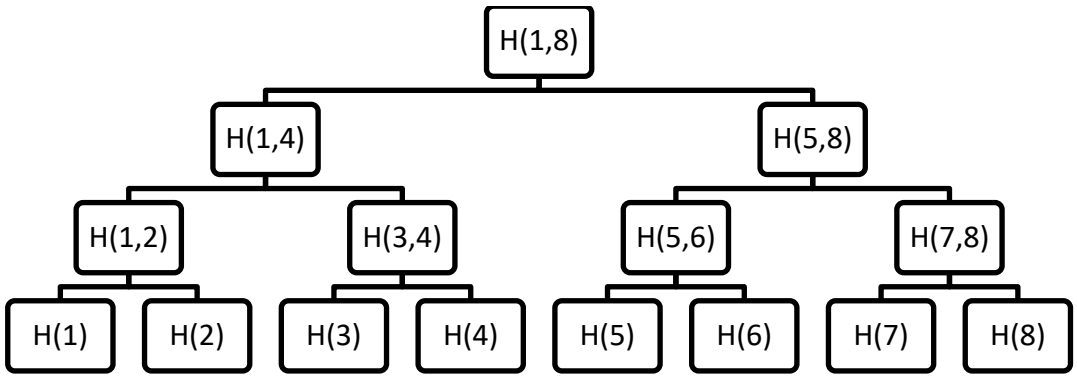

Figure 4: Markle Tree

Markle root plays very important role in validation of block. They secure the information in the block by hiding the actual data in most of the validation process and helps validation of the block data.

2.2 The Problem and Existing Solutions

2.2.1 Majority Attack / 51 Percent Attack

In proof of work, it is the nonce that the miner tries to find to generate a predefined pattern of hash. All the network peers compete to find a suitable nonce. The miner who finds the nonce first, adds the block to the chain and announce his success to the network. Mining costs a huge computation power to the miner which involves large electricity consumption. For incentivizing the miner's effort, the system rewards the miner by generating some specific number of coins and reward the miner by giving this newly generated coins. PoW mechanism totally relies on the computation power of the miner. The more computation power a miner affords the more chance it gets to mine blocks and get rewards. If someone poses a large amount (more than 50%) of computation power, he can do several malicious activities in the block chain for his benefit. Let's think of a malicious user possessing more than 50% of processing capability. As his computation capability is much higher than other, he can mine longer chain in faster time than others. As per longest chain rule [22], his generated chain will have the greatest probability to be accepted by the network. To initiate the attack the corrupt miner continues mining blocks by selecting transactions from the memory pool. But he doesn't broadcast those mined blocks to the network. In the meantime, the mainchain grows by the other nodes of the network simultaneously. In the mainchain the corrupt miner can make transactions with

other nodes by using another wallet application of his own. Suppose he make several big deals and transfers balance to other network users. Also, he can convert his currencies to other cryptocurrency or even liquify huge amount of cryptocurrency into fiat currency from some exchanges. After these transactions are confirmed in the block chain, he'll broadcast the other much longer chain that he mined secretly. When the network receives this much longer chain, which is also valid chain but not containing the transactions the corrupt user did with other users and exchanges, the network accepts the longer chain and discard the shorter chain. Thus, all those transfers and other transactions made by the attacker will discarded with shorter chain and he'll drain a lot of money by cheating the users and exchanges with whom he made those transactions.

Let's have another simpler example. Suppose a fraud user deals with some other user and sends some coins to the user. Whilst the transactions are being confirmed in the block chain. Suppose the transaction is confirmed in block 31. The malicious user utilizes his processing advantage to begin confirming another transaction with the same coins in secret. Then it continues mining more blocks.

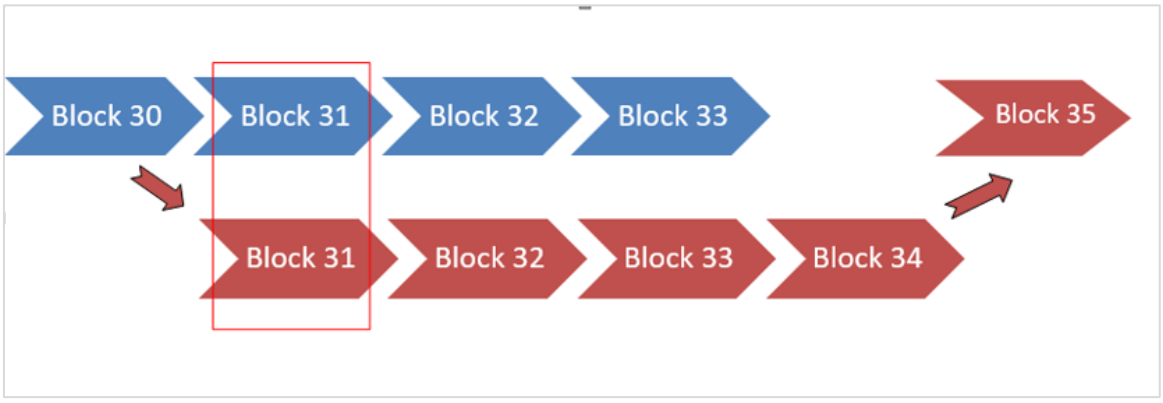

Figure 5: Majority Attack Explained

As his processing capability is quite higher than other, he will mine more blocks quicker than others. After a significant number of blocks mined, he broadcasts the newly created chain in the network where the second transaction resides. As this is the longest valid chain broadcasted in the network the block consisting the first transaction will be dropped by the network and second transaction will be accepted. Thus, the malicious user can double spend [18] his money to fraud the first transaction's recipient. The other network users will not even aware of this fraudulent activity. Because all the other transactions are

confirmed in usual manner only the transactions made by the corrupt user will be vanished as he intentionally mined the second chain in such a way.

This attack can cause several damages to the network and lead the exchanges to be ruined. The attacker can make fake transactions all the time and fraud different targeted people and exchanges for his benefit.

The older and larger networks are at less risk from this attack. Because in such networks the attacker has to invest a very large amount of money to acquire such capability in the network. But the newer and smaller networks are more vulnerable to this attack. In fact, all the new cryptocurrencies which are about to be launched in the market are at most risk to be attacked by it. So, at this moment all the cryptocurrencies which are about to be bloomed are too much concerned about this attack.

2.2.2 Present Solutions

There are several studies, researches and developments going on to tackle the attack. To get rid from this attack, researchers propose mixing of proofs. In a Proof of Work network if Proof of Stake mechanism is added then the attacker has to gain more than 50% of processing capability along with more than 50% of network wealth. That is much harder for a user to afford. Moreover, the total cost should must be much lower than the profit an attacker could gain. In this type of Hybrid network, the cost will be much higher than the profit an attacker can make. Moreover, there are other security measures introduced with this hybridization to tackle this attack [22]. Different researches and developments propose different kinds of prevention on this attack but all of them have some common limitations too. Komodo Platform [26] introduce dPoW mechanism. They take snapshots of their block chain every 10 minutes and store the information in bitcoin block chain. So, if an attacker intends to attack this network, he has to overpower the bitcoin network too. Horizen team the developers of ZEN coin and ZCL coin which are affected by this attack, introduce a delayed block submission penalty system for delayed submission of blocks [20]. Suppose, a miner mines N number of blocks without broadcasting to the network. Then he must have to wait and mine more N blocks in his branch then he can submit the branch to the network. Profitability of this attack is not very high and in the meantime the exchanges monitor his activity and examine delayed submitted blocks for integrity and if any malicious activity found they block the user

immediately. There are several researches undertaken that propose special nodes who will responsible for validating blocks. A variant of hybrid Proof of Stake scheme named Casper a friendly finality gadget was proposed by Ethereum [12]. Casper combines the security deposit concepts with validators voting to reach a consensus, bringing traditional BFT model closer to the PoS system. What Casper suggests is to make deposits by the peers to be elected as validators. A randomized election chooses the validator set of peers [2]. Casper will use PoS consensus to finalize at 50 block intervals with two-thirds of the network voting on the validity of the network. Another variant of this scheme is implemented by Decred coin [21]. Decred introduced a hybrid system where PoW miners mine to create blocks. Shortly after that, the stakeholders 'vote' to confirm if the block is valid. They do so by buying voting tickets, thereby temporarily locking their DCR in the network. Decred team claims it as a hybrid PoW-PoS solution where the mining of block is done by traditional miners and after finding the cryptographic solution to mine a block, the stake holders are being active to vote on the correctness of the mining process. The stakeholders buy voting tickets. When a block is created 5 tickets are chosen randomly from the ticket database and if at least 3 tickets are yes then the block is validated and incorporated in the blockchain. One problem of this protocol is the user who mines a block doesn't signs it. The validator group sign the block. Thus, there introduced a discrepancy in miner and validator peers. This kind of systems result in inconsistent block generation intervals and inconsistent distribution of profit to the stake holders. Because the PoW based algorithm and the voting mechanisms are independent process, they cause unintentional delays to make the block interval inconsistent. Another Hybrid consensus proposed in "Fork-free hybrid consensus with flexible Proof-of-Activity" by Zhiqiang Liu et al [14], A Hybrid of PoW-PoS-PoA Algorithm is proposed. In this proposal the authors present a method where all the PoW chains which are generated simultaneously are submitted to a committee. Then the committee decides the best chain and accept it as the main chain. The election of best chain among the committee members are based on a weight calculation. The weight of each committee member is calculated from the PoW power and PoS capability. So, the 51% attack could be mitigated by this algorithm too. But the block chain will still suffer from other problems. One of the main problems is the distribution of newly generated block reward. When a chain is selected the entire incentive of all the new blocks are given to the miner whose chain is accepted. Other honest nodes who also create valid chain but rejected by the voting committee are

deprived from the profit. In this system if a node consists larger processing capability to generate larger chains, that peer will always win the competition and get the reward. Other nodes will always be deprived from the incentive of their work. Also, the validator committee concept makes some nodes to be special in the network. It differentiates the validators from the other nodes in the network. That violates the P2P network concept where every node should be treated as totally similar weighted entity. Another problem is block generation interval which is directly proportional to the newly generated currency is also be inconsistent. Because, the PoW mechanism maintains a block interval maintaining the time consistently across the nodes. But after that the voting mechanism will create a delay on top of that block interval. As there is no strict block interval mechanism, the system will suffer from inconsistent profit distribution. Thus, the investors won't get the revenue uniformly against their investment. From the perspective of investors, it will not be a promising investment for them. The economic evolution of a currency is directly depending on the investors interest in the currency. So, a cryptocurrency with inconsistent revenue system will not attract the investors to invest their hard-earned money in such a system. The following table-1 presents a comparative analysis on the solutions.

Table 1: Comparison among different hybrid and other solutions

	Supports P2P protocol	**Consistent block time**	**Investment wise proportional profit distribution**	**Autonomous network – Not need any special authority**	**Democratic majority peers are decision makers**	**Penalized corrupted or malicious user**
Casper	No	No	No	No	No	Yes
Decred	No	No	No	No	No	No
Komodo	Yes	Yes	No	Yes	Yes	No
ZEN	No	Yes	No	No	Yes	Yes
Proposed system	Yes	Yes	Yes	Yes	Yes	Yes

Table 2: Explanation of our system's supported features

Features	supports or not	Explanation
P2P protocol	**Yes**	In our proposed system all nodes are equal according to their code base, responsibilities and service to the network. So, it supports the P2P protocol
Consistent block time	**Yes**	The system provides a uniform average block time and that is 166 seconds per block. So, we can say it supports a consistent block time.
Investment wise proportional profit distribution	**Yes**	As the system implements PoS algorithm the block generation probability of the nodes is proportional to their investment. This proportion doesn't show proper distribution because of inconsistent block interval. This problem is mitigated by applying PoW loop inside PoS processing. PoW loop ensures a consistent block interval. Thus, we can ensure proper profit distribution in proper time.
Autonomous network – Not need any special authority	**Yes**	There is no special validator or voter or watcher nodes in this network. All the nodes operate in same manner with same responsibility in the network.
Democratic majority peers are decision makers	**Yes**	As all the nodes are equal in the network and P2P protocol is perfectly maintained, we can say the network is totally democratic.
Penalize corrupted or malicious user	**Yes**	If any malicious activity found in any node then the network ban the node immediately. So, penalization feature is also supported by this system.

Chapter 3

Methodology

3.1 The Proposed Solution

We maintain a uniform average block generation interval by imposing the PoW loop inside the PoS block creation process, so all the PoW and PoS processing could be done by the same single node. The main implementation is done in the mining loop where we compose the Proof of Work consensus mechanism with Proof of Stake mechanism. The mining process starts with checking the stake parameters. These stake parameters are UTXOs, mature balance, coin age, timestamp synchronization, node's current weight and network weight. After the initial validations and time synching prerequisite checks we introduce the Proof-of-Work's nonce finding loop. In this step, at first an empty block template is generated. Then to generate a valid hash, the PoW loop continues to find a suitable nonce. To understand it, let's have a look on the block structure. A block consists of some transactions which could not be altered arbitrarily. Also, other data in the block like timestamps, previous block's hash etc. are unalterable. So, to change the hash to get a valid pattern, the nodes use the arbitrary field nonce. The miners start with 0 and continues by incrementing the nonce in each iteration of the PoW loop and generate hash combining this nonce and other block data. When a valid hash is found which meets the block hash criteria, the peer gets success on mining. To maintain the block time interval a difficulty factor is introduced. It's a 256-bit integer which regulates the nonce finding. The block hash must be lower than this target. This difficulty value is adjusted upon the processing capability of the miner and average block generation interval of last 2016 blocks. By this intentional delay we maintain a farm block generation interval. It is necessary to keep a regulation on the creation of new coins. As the difficulty adjustment is occurred after each 2016 blocks. In the meantime, if a node gains huge hash power to generate nonce earlier than the desired block time and solves this nonce finding puzzle, then it has to pass the Proof-of-Stake validations to mine the block.

Staking loop begins with finding a coin-stake kernel from the staking UTXOs of the miner. Kernel is the first input in the coin-stake transaction. On each calculation, the UTXOs are selected randomly. This randomness is required because without it, the stakeholders with larger amounts will have advantage permanently. The users staking smaller amount could also get the chance of finding a PoS solution. The hashing for each UTXOs are done in parallel threads. The current block timestamp and previous blocks header are also combined during generation of the hash. Then it calculates staking target using the next formula:

Staking Target = Block difficulty * UTXO value

We compare kernel's hash against the staking target. If it is greater, then we meet the criteria and kernel is found. So, the more coins we stake the higher the staking target and so the higher the chance to meet the criteria.

The minimum valid timestamp interval is defined 16 seconds. That means timestamps divisible by 16 are only valid timestamps for mining. This strict spaced timestamp is maintained and the difficulty target of PoS is adjusted after each block. If the timestamp is not maintained strictly, the miners will begin checking their UTXOs again with a new one. So, the system only checks for next valid timestamp for the miner and if it fails, it has to wait until the next round. This strict timestamp barrier is also essential to slow down a powerful miner to keep pace with the other slower miners [19]. The PoS processing checks the last mined block timestamp of the node and decides whether the node meets its expected reward time or not. If not then the whole PoW and PoS processing has been discarded and new iteration starts. The desired time for a node to mine a new block is defined by its staked coin amount, maturity and coin age. If the coin holding of a node meets the desired coin age, the balance is called matured balance. And the probability of the node for mining a new block is directly proportional to its matured balance. Once a node’s matured balance and weight meets the expected reward time constraints for mining a block by the following calculation: Suppose the network weight is W_n. It is calculated from the coin view as we know that all the unspent transaction outputs are tracked by the coin view. So, from iterating each UTXO in the coin view and sum up the multiplied values of coins and coin age, the network weight could be calculated easily. The weight W_i of the node could be calculated by using equation (1).

Then by dividing the network's weight by the node's weight we can get the expected reward time as follows:

$$\text{The expected Reward Time, } T_{exp} = W_n / W_i \text{ Seconds}$$

Now the application checks the timestamp of last block mined by the node T_{last} and current time stamp T_{now}. If

$$T_{exp} < T_{now} - T_{last} \tag{4}$$

Then it got the chance to mine the block. During this mining, an internal transaction from the address of the node to a new address of the same node takes place. The balance is transferred to the new address of the same user to reset the coin age of the transferred balance. So, the user has to wait for maturity again for mining another block with the coins got as change of the previous transaction.

By implementing this methodology, we ensure the block generation time interval very fine tuned. And the profit generated from mining and transaction fees are distributed to the investors in a uniform way. In addition to this mining mechanism another security measure is introduced to protect the network from misbehaving nodes by banning them for a predefined time interval. The banning time for the simulation environment is one hour. So, if any of the peer node mines blocks being disconnected from the network will banned from the network for an hour. Another major constrain of this protocol is equality of all the nodes validation weight. All the nodes in the network are equally weighted in terms of decision making. That means validation of a rich node and a poor node is evaluated equally. All the peer nodes have an equal weight and identical code. Each node can mine blocks validate transactions and blocks and can sign the blocks as they got a chance in the mining process. The frequency of getting the chance is dependent on their staking capabilities.

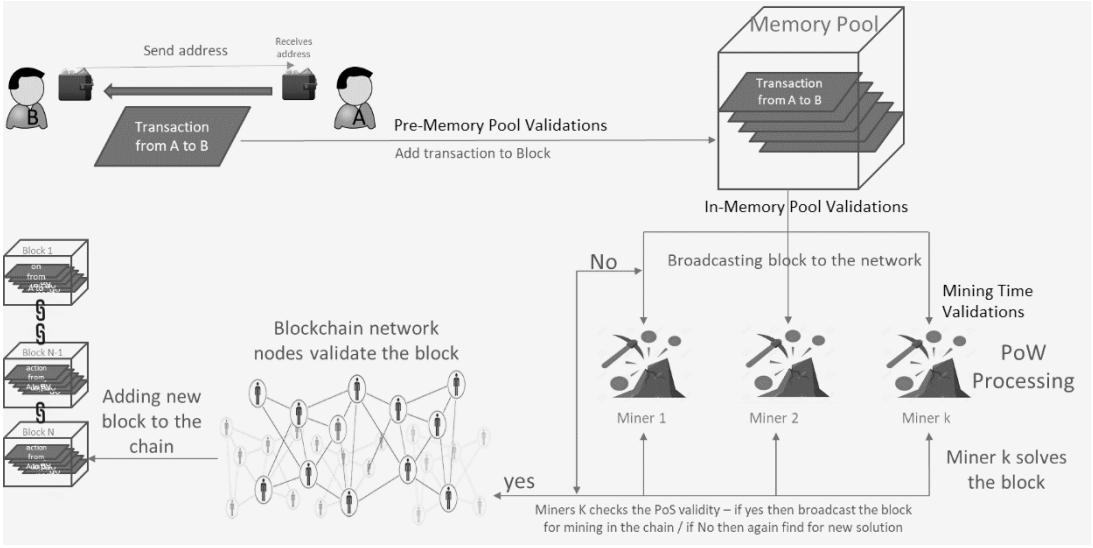

Figure 6: Hybrid PoW-PoS Mechanism

3.2 The Mining Algorithm

Mining process is started with the application start. At first it starts checking as follows:

1. Check if the system time out of sync: Prevent mining if the system time is not in sync with that of other members on the network
2. If system time is properly synced then start the PoS loop:
   A. Check if Initial Blocks Downloaded. Prevent mining if not fully synced. Wait for synchronization before mining can be started.
   B. Checks local chain tip and consensus chain tip are matched or not.
   C. Start PoW Loop:
      1) Generate block template
      2) Search for proper nonce
      3) If nonce found then exit Pow loop otherwise continue loop with another template
   D. Calculate UTXOs (Unspent Transaction Outputs)
   E. Calculate spendable balance and coin maturity
   F. Prepare UTXO Stake Description for staking
   G. Generate PoS Block Template:
      1) Create empty Coinbase transaction with zero value.
      2) Compute block version

3) Compute median time past for the chain tip
4) Calculate cut off lock time
5) Add transactions based on fee rate including unconfirmed ancestors with corresponding statistics. This transaction selection algorithm orders the memory pool based on fee rate of a transaction including all unconfirmed ancestors. Since we don't remove transactions from the memory pool as we select them for block inclusion, we need an alternate method of updating the fee rate of a transaction with its not-yet-selected ancestors as we go. This is accomplished by walking the in-memory-pool descendants of selected transactions and storing a temporary modified state. Each time through the loop, we compare the best transaction with the next transaction in the memory pool to decide what transaction package to work on next.
6) Calculate next target required and Update Headers
7) Test block validity
8) Return block template

H. Stake and Sign block:

1) Get Network Weight
2) Check the last coin stake search timestamp and current search interval
3) Check matured balance is greater than reserved balance or not.
4) Selects UTXOs that are suitable for staking:
   (a) Such a UTXO has to be confirmed with enough confirmations - i.e. has suitable depth. The current height of the chain is used for calculating the number of confirmations a transaction has.
   (b) If not in blockchain, and not in memory pool (conflicted transaction).
   (c) If in memory pool, waiting to be included in a block.
   (d) If included in a block. See how many blocks deep in the main chain.
   (e) It also has to be matured
   (f) Meet requirement for minimal value
5) Calculate the wallet weight.
6) Calculate expected time
7) Calculate weight percentage
8) Try to find staking solution among all the transactions
9) Get reward for newly created block.

10) Add transaction fees with reward
11) Checks whether the coin stake transaction should be split or not. The coin stake is split if the number of non-empty UTXOs we have in the wallet is under the given threshold.
12) Sign Transaction Input
13) Get the serialized size of block and check if it exceeds the limit
14) Successfully generated block.
15) Make sure coin stake would meet timestamp protocol as it would be the same as the block timestamp.
16) We have to make sure that we have no future timestamps in our transactions set.
17) Add coin stake transaction in the block.
18) Update Merkle Root
19) Append a signature to our block.

I. New POS block created and signed successfully.

3. Check Stake: Once a new block is staked, this method is used to verify that it is a valid block and if so, add it to the chain.

A. Accept Block:

1) Validate and execute block: Validates a block using the consensus rules and executes it (processes it and adds it as a tip to consensus):
   (a) Load the UTXO set of the current block. UTXO may be loaded from cache or from disk.
   (b) Attempt to load into the cache the next set of UTXO to be validated. The task is not awaited so will not stall main validation process.
   (c) Validate the UTXO set is correctly spent.
   (d) Persist the changes to the coin-view. This will likely only be stored in memory, unless the coin-view threshold is reached.
   (e) Set the new tip.
2) Check if the error is a consensus failure:
   (a) If our consensus tip is not on the best chain, which means that the current block we are processing might be rejected only because of that. The consensus is on wrong chain and need to be reset. Pull again.

Check witness. If Invalid block received, Chain is reverted back marking the block as invalid. Ban the peer and calculate ban duration.

(b) Else Block accepted

3) Flush if we are at the top of the chain.
4) The newly mined block extends the best chain tip.

4. Broadcast the Chained Block.

3.3 Flow Chart

The following flow chart depicts the whole procedure of proposed Hybrid Proof of work – Proof of Stake consensus mechanism in a pictorial figure.

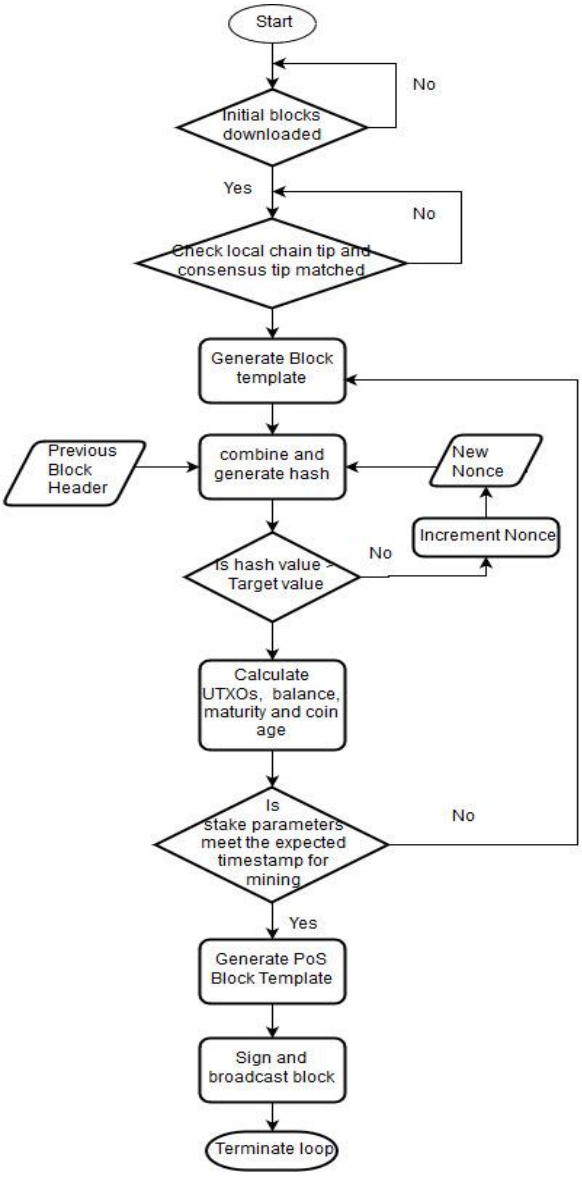

Figure 7: Flowchart Showing Hybrid Implementation of Proposed System

3.4 Network Setup Topology Diagram

We used 7 AWS servers, 6 local veirtual machine and 2 local computers all connected through the internet for setting up the test environment. The topology diagram of our test network is given below:

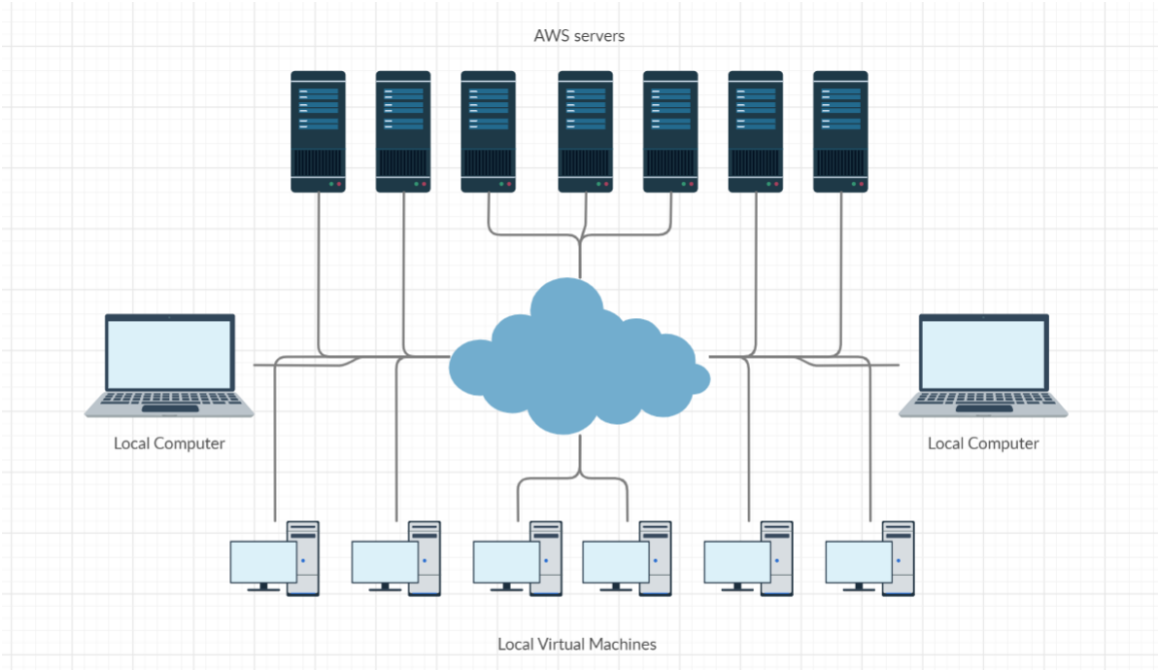

Figure 8: Network Setup Topology Diagram

Chapter 4

Results and Analysis

We have implemented the whole mining algorithm in C# .Net with the help of Stratis framework. In our test environment we set the PoW and PoS both consensus block interval as 150 sec. As PoW processing encounters first, it maintains the interval as close to 150 sec as possible by its difficulty adjustment and nonce finding mechanism. After this delay when PoS mining starts it observes that the last block time is past the delayed by the PoW mechanism. As strict spaced valid timestamp interval is 16 sec the total amount of block interval will approximately 150 + 16 = 166 sec. Then we ran the application in different machines. The first block's mining timestamp was 2019-04-15 11:10:14. At 2019-04-28 00:00:03 the blockchain height was 6618. The time difference in seconds is 1082989.

So, Average block interval = 1082989 / 6618 = 163.64 sec. The following table presents the observed average block time results on different timestamps and heights of the block chain.

Table 3: Average block time interval measured at different height of the block chain

Blockchain height	Measurement timestamp	Average block time
6618	2019-04-28 00:00:03	163.64 sec
7649	2019-04-30 00:00:02	164.17 sec
8174	2019-05-01 00:00:04	164.20 sec
9296	2019-05-06 06:02:24	193.19 sec
11267	2019-05-07 00:00:02	165.14 sec
11790	2019-05-08 00:00:02	165.14 sec
12842	2019-05-10 00:00:02	165.07 sec
13370	2019-05-11 00:00:03	165.01 sec
19575	2019-05-22 19:29:08	164.84 sec
20559	2019-05-24 16:34:56	164.84 sec

We've tested the implementation with different configurations computers with same amount of balance in their wallets.

Table 4: Calculated reward time interval for differently configured computers

Machine Configuration	Staking Balance	Reward Time Interval
3.5 GH_z 4 CPU 8 GB RAM	10 Million coins	130 Minutes
3.5 GH_z 8 CPU 16 GB RAM	10 Million coins	130 Minutes
3.1 GH_z 8 CPU 32 GB RAM	10 Million coins	130 Minutes
2.8 GH_z 8 CPU 16 GB RAM	10 Million coins	130 Minutes
2.8 GH_z 2 CPU 3 GB RAM	10 Million coins	130 Minutes
2.8 GH_z 1 CPU 3 GB RAM	10 Million coins	130 Minutes

The above result was taken at the same timestamp with same wallet balance in all the machine. This reward time interval is always changing with each transaction taking place in the network. And we observed that at same time with same staking matured balance and weight all the nodes with different computing capabilities have the same amount of time interval for getting a block reward.

The memory consumptions and CPU usage is very small for this consensus mechanism. The application consumes 70MB of memory and the CPU usage is almost zero at most of the execution time. Only when PoW mining loop is running then the CPU spikes are generated and the usage is raised to its pick. The following figure shows the memory consumption and CPU usage result from the diagnostic tool of visual studio:

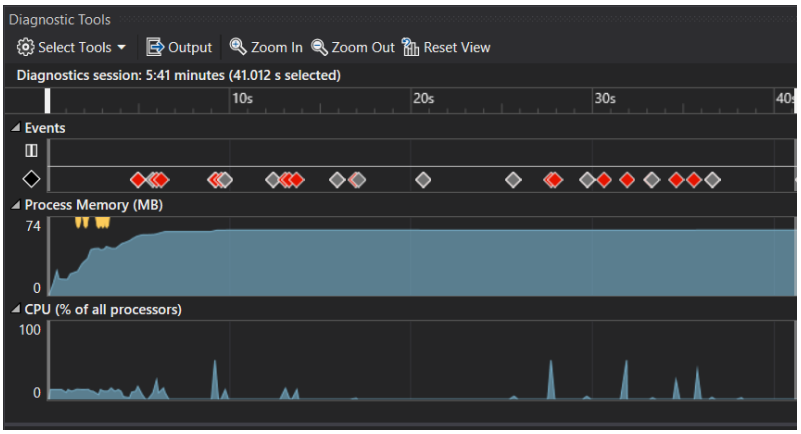

Figure 9: Memory Consumption and CPU Usage of The Application

What we've done in this study is, inject the PoW processing difficulty adjustment model inside the PoS loop to gain a firm block generation interval. The interval and difficulty adjustment are managed in two steps in first step the PoW mechanism is activated. It tunes the difficulty according to PoW rules. After finding a correct nonce the PoW loop ends. But the node cannot mine that block at that moment. After that, the PoS validator checks for the expected staking time interval and last block generation time. Here the block interval is tuned again and difficulty adjustment again takes place that checks if it meets the staking criteria or not. If not then it should have to wait for next staking cycle. If all the criteria meet correctly, then the node could mine the block, get the reward and broadcast to the network. The PoS mechanism also provides coin age calculation that facilitates the renewal of the coin age after each spending that prohibits nodes to use same staking capabilities after each transaction. In this system if someone with huge computation capability may find PoW solution in fastest interval of time should have to wait for the PoS validation barrier. Similarly, a node with most staking wealth have to wait until to solve the PoW puzzle.

If some malicious node possesses largest computing capability and largest amount of staked coin tries to manipulate the block. Let's imagine a node possesses 51% of total network's processing capability and 51% of total network's wealth. Then the probability getting a chance of mining in the combined PoW-PoS system can be calculated by the following calculation:

$$P(\text{PoW-PoS}) = P(\text{PoW}) \text{ AND } P(\text{PoS})$$

$$= 51\% \text{ X } 51\%$$

$$= (51/100) \text{ X } (51/100)$$

$$= 26.01\ \%$$

To get this network down by majority attack, the malicious node has to gain minimum 71% of processing capability and 71% of staked asset. Then it will possess the combined probability

$$P(\text{PoW-PoS}) = P(\text{PoW}) \text{ AND } P(\text{PoS})$$

$$= 71\% \text{ X } 71\%$$

$$= (71/100) \text{ X } (71/100)$$

$$= 50.41\%$$

Though, it is quite impossible and unrealistic to gain such capabilities, if some node gains these capabilities, it is also be tackled in the system by strict spaced valid timestamp mechanism. The strict spaced timestamp will slow down the mining process and keep pace of generating blocks in the network. Moreover, from the perspective of verification capabilities, each node possesses the same weight in the network about decision making. So, illegally mined blocks and transactions by the malicious node will also be discarded by the network immediately after broadcasting. What the bad node can do at most is initiate a new hard fork on the chain to be separated from the network. For that case the honest network can retrieve all its assets by initiating a reorg, banning the bad nodes and continue.

Chapter 5

Discussion and Conclusion

While a new cryptocurrency is launched in the market, there are couple of things it has to ensure for drawing attention of the investors. Because the investors are the main source of fuel to start and run a cryptocurrency. They play a vital role in crowd funding and initial fund-raising process for a newly launched cryptocurrency. If no one is interested to invest on the currency then it could not evolve in the market and will collapse eventually. The investors always seek for security of their investment and guarantee of making proper competitive profit from their investment. In cryptocurrency systems the profit is gained from the mining reward and transaction fees by mining blocks. In a pure PoS based system a node with large staking amount mines block in a very frequent time interval and generates profit frequently. To ensure the profit generation of the entire network with a time-based and uniformly distributed manner, we must have to ensure the block generation interval. In this paper, we have presented a comprehensive study on creating the Hybrid PoW-PoS based cryptocurrency that can tackle the 51% attack in most feasible and sophisticated way. To illustrate the process in front of the audience we described the basic theories of mining protocols. We also described almost all the relevant entities, actors, concepts and terminologies that resides in the literature to help understand the whole process and mechanism of creating the protocol. We organize the sections with farm details to help the reader understand the protocol most accurately. In other present solutions against majority attack, the block generation interval fluctuates a lot due to use of both PoW and PoS mechanism in parallel with combination of some other methods like voting, ticketing, deposit schemes without regulating the timeframe for mining blocks. By applying this method, we found a firm block generation interval. We described the 51% attack, its impact on the network and how it is mitigated by applying both Proof of Work and Proof of Stake mechanism. We propose a hybrid system that could prevent this majority attack by mixing Proof of Work and Proof of Stake in a single thread with applying strict time spacing for block generation to achieve a firm and resilient consensus among the nodes in the peer to peer network and guarantee the distribution of profit in accordance to the investment ratio of the stakeholders. Someone

possessing a large amount of hash rate is not guaranteed to be the first to generate a block as his staking amount is also in consideration to be able to generate a block. Similarly, a user with large amount of staked money cannot rule the network as staking asset is not the only playmaker in the network. If a user or a group of users possess a large amount of CPU power and staking asset, although that is a rare case scenario, if it happens in the network, the strict spaced timestamp barrier slows down the node to be much faster than the other node and other validators will reject those manipulated mal-transactions immediately even before putting them into their memory pool. We not only show the mining process in this hybrid implementation but also, we've focused on all the validation steps carried out on the blocks and transactions in different stage of the mining. The methodology section illustrates this whole implementation in a very detailed algorithmic presentation to give the audience a firm step by step approach to achieve the correct possible coding structure.

References

[1] Satoshi Nakamoto. Bitcoin: A peer-to-peer electronic cash system. 2008. http://bitcoin.org/bitcoin.pdf.

[2] Marie Vasek, Micah Thornton, and Tyler Moore. Empirical Analysis of Denial-of- Service Attacks in the Bitcoin Ecosystem. 2014.

[3] Marianna Belotti, Nikola Bozic, Guy Pujolle, Stefano Secci. A Vademecum on Blockchain Technologies: When, Which and How. 2019. <hal-01870617>

[4] Yli-Huumo J, Ko D, Choi S, Park S, Smolander K. Where Is Current Research on Blockchain Technology? — A Systematic Review. 2016.

[5] I. Eyal and E. Gun Sirer. Majority is not Enough: Bitcoin Mining is Vulnerable, 2013. http://arxiv.org/pdf/1311.0243v5.pdf.

[6] L. M. Bach, B. Mihaljević,and M. Žagar. Comparative Analysis of Blockchain Consensus Algorithms < MIPRO 2018/SP>

[7] M. Rosenfeld. Analysis of Bitcoin Pooled Mining Reward Systems. http://arxiv.org/pdf/1112.4980.pdf.

[8] A. Shoker, "Sustainable blockchain through proof of exercise",2017 IEEE 16th International Symposium on Network Computing and Applications (NCA), 2017.

[9] D. Kuhnert. The Dogecoin survival guide. Accessed:2019-01-28. [online]: https://imgur.com/a/Sgyox.

[10] Wenbo Wang, Dinh Thai Hoang, Peizhao Hu, Zehui Xiong, Dusit Niyato, Ping Wang, Yonggang Wen. A survey on consensus mechanisms and mining management in blockchain networks, 2019. http://arxiv.org/abs/1805.02707v3.

[11] A. Laszka, B. Johnson, and J. Grossklags. When Bitcoin Mining Pools Run Dry: A Game-Theoretic Analysis of the Long-TermImpact of Attacks Between Mining Pools. 2015. Unpublished

[12] G. Karame, E. Androulaki, Bitcoin and Blockchain Security,Norwood, MA: Artech House, 2016.

[13] V. Buterin and V. Griffith. Casper the friendly finality gadget.arXiv preprint arXiv:1710.09437, 2017.

[14] Proof of Authority. Accessed: 2019-01-28. [online]: https://wiki.parity.io/Proof-of-Authority-Chains.

[15] Zhiqiang Liu, China Shuyang Tang, Sherman S.M. Chow, Zhen Liu, Yu Long. Fork-Free Hybrid Consensus withFlexible Proof-of-Activity. 2017.

[16] Xiwei Xu, Ingo Weber, Mark Staples, Liming Zhu, Jan Bosch, Len Bass, Cesare Pautasso, Paul Rimba. A Taxonomy of Blockchain-Based Systems for Architecture Design. 2017.

[17] Florian Tschorsch, Björn Scheuermann. Bitcoin and Beyond: A Technical Survey on Decentralized Digital Currencies. 2015.

[18] Danny Yuxing Huang. Profit-Driven Abuses of Virtual Currencies. 2013.

[19] Aggelos Kiayias, Ioannis Konstantinou, Alexander Russell, Bernardo David, Roman Oliynykov. A Provably Secure Proof-of-Stake Blockchain Protocol. 2016.

[20] Robert Viglione, Rolf Versluis, and Jane Lippencott. Zen White Paper. 2017.

[21] Christina Jepson. DTB001: Decred Technical Brief. 2015.

[22] BitFury Group. Proof of Stake versus Proof of Work. 2015.

[23] Muhammad Saqib Niaz, Gunter Saake. Merkle Hash Tree based Techniques for Data Integrity of Outsourced Data. 2015.

[24] Pavel Vasin. Black Coin's Proof-of-Stake Protocol v2. www.blackcoin.co

[25] Serguei Popov. A Probabilistic Analysis of the Nxt Forging Algorithm. 2016.

[26] https://komodoplatform.com/51-attack-how-komodo-can-help-prevent-one/

[27] https://coinsutra.com/bitcoin-mempool/

[28] https://99bitcoins.com/what-is-bitcoin-mempool/

[29] https://www.mycryptopedia.com/mempool-explained/

[30] https://klmoney.wordpress.com/bitcoin-dissecting-transactions-part-1/

[31] https://davidederosa.com/basic-blockchain-programming/the-first-transaction-part-one/