Efficient Blockchain System based on Proof of Segmented Work

by

Rashad Ahmed
15201037
Alif Ahmad
19241039
Maruf Monem
19241041
Jumana
16101275

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 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:

Rashad Ahmed 15201037	Maruf Monem 19241041
Jumana 16101275	Alif Ahmad 19241039

Approval

The thesis/project titled "Efficient Blockchain System based on Proof of Segmented Work" submitted by

1. Jumana (16101275)
2. Alif Ahmad (19241039)
3. Rashad Ahmed (15201037)
4. Maruf Monem (19241041)

Of Fall, 2019 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science and Engineering on December 26, 2019.

Examining Committee:

Supervisor:
(Member)

Hossain Arif
Assistant Professor
Department of Computer Science and Engineering
Brac University

Program Coordinator:
(Member)

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

Head of Department:
(Chair)

Mahbubul Alam Majumdar, PhD
Chairperson
Department of Computer Science and Engineering
Brac University

Abstract

The use of Blockchain in Cryptocurrency introduces a technology that acts as an unswervingly growing ledger with the capability to keep an everlasting record of all the transactions that have taken place, in a secure chronological and immutable system. It removes dependency on central financial service providers such as banks, essentially removing the middle-man from the transaction. Bitcoin is one of the biggest users in blockchain and holds the highest share in the cryptocurrency market. However, bitcoin has three major problems which are excessive power consumption, confirmation time and fair reward distribution. Hence, we are proposing a system where we have tried to reduce energy consumption by limiting the participation of all the nodes in the network and worked on increasing the propagation speed in the network. Finally, we have put a lot of emphasis on the concept of fair reward distribution which is not considered in most cryptocurrencies. Apart from this, we tried to prove our systems efficiency by comparing the energy consumption with the two most used crypto currencies Bitcoin and Ethereum mathematically. And have reached the conclusion, that our proposed system shall reduce energy consumption by about 80.0% and 46.68% when compared with Bitcoin and Ethereum if each node in our network consumed the equivalent energy as an average node in the bitcoin network, on the otherhand, 92.41% and 79.76% if each node in our network consumed the equivalent energy as an average node in the ethereum network.

Keywords: Bitcoin, Blockchain, Cryptocurrency, Consensus Algorithm, Proof of Segmented work, FaircoinBD.

Acknowledgement

Firstly, all praise goes to the Almighty Allah for whom our thesis have been completed without any major interruption.
Secondly, to our thesis supervisor Mr. Hossain Arif for his kind support and advice on our work. He helped us whenever we needed guidance.
Thirdly, Andreas Antonopoulos for helping us understand the concepts of cryptocurrency thourgh his book Mastering Bitcoin. Even though, we did not know him personally his materials and book guided us throughout the research.
And finally to our parents, without their throughout support it may not have been possible. With their kind support and prayer we are now on the verge of our graduation.

Table of Contents

Declaration i

Approval ii

Abstract iii

Acknowledgment iv

Table of Contents v

List of Figures vii

List of Tables 1

1 Introduction 2

2 Literature Review 4
2.1 Cryptocurrency and Blockchain 4
2.1.1 Cryptocurrency 4
2.1.2 Blockchain 5
2.2 Wallets and Digital Signatures 6
2.2.1 Key, Address and Wallet 6
2.2.2 Digital Signature 9
2.2.3 Schnorr Signature 9
2.2.4 Elliptic Curve Digital Signature Algorithm (ECDSA) 10
2.3 Insights of Bitcoin Transactions 11
2.3.1 Creation 11
2.3.2 Propagation 12
2.3.3 Validation 13
2.3.4 Addition in the Block 14
2.3.5 Transaction Fees 14
2.3.6 Understanding Bitcoin transaction locktime 15
2.3.7 What impact has Segregated Witness (SegWit) had on fees? . 15
2.4 Block Structure in the Blockchain 16
2.5 Consensus Protocols/Algorithms 17
2.5.1 Proof of Work 19
2.5.2 Proof of Stake 19
2.5.3 Proof of Elapsed Time 20
2.5.4 Related works concerning Consensus Algorithms 20
2.6 Mining Pool 21

2.6.1 Pool selection and Reward system . . . 23

3 Algorithm & Design of the Model 24
3.1 Motivation . . . 24
3.2 Registration . . . 25
3.2.1 Becoming a FaircoinBD user . . . 25
3.2.2 Becoming a FaircoinBD miner . . . 25
3.2.3 Stake . . . 27
3.2.4 Addition to main pool . . . 27
3.2.5 Sub pool Creation . . . 27
3.3 Transactions . . . 28
3.4 Proof of Segmented Work . . . 30
3.4.1 Coordinator selection . . . 32
3.4.2 Random Function . . . 32
3.4.3 Nonce Solving . . . 33
3.4.4 Switching at Intervals . . . 35
3.4.5 Forwarding Hash Range . . . 35
3.4.6 Block Structure . . . 35
3.4.7 Adding the Block . . . 35
3.4.8 Propagation . . . 36
3.4.9 Rewards Distribution . . . 36
3.5 Flowchart of the proposed model . . . 38
3.6 Final thoughts . . . 39

4 Comparison and results 40
4.1 Comparison with similiar networks . . . 40
4.1.1 Comparing our system with the Bitcoin network . . . 40
4.1.2 Comparing our system with the Ethereum network . . . 41
4.1.3 Comparing our proposed model with Bitcoin and Ethereum . 42

5 Conclusion 45
5.1 Accomplishments . . . 45
5.1.1 Provides chance to participate for low configuration computers 45
5.1.2 Possibility of Fork is minimal . . . 45
5.1.3 Energy Consumption is minimal . . . 45
5.1.4 Carbon Footprint is low . . . 46
5.2 Drawbacks . . . 46
5.2.1 Quantum Supremacy . . . 46
5.2.2 Time consumed at each interval . . . 46
5.2.3 Bandwidth consumed by the coordinator . . . 47
5.3 Future Work . . . 47
5.4 Conclusion . . . 47

Bibliography 52

List of Figures

2.1 A simple Blockchain 5
2.2 Key Pair Relationship 6
2.3 Public Key to Bitcoin Address 7
2.4 Visual representation of coinbase wallet 8
2.5 Digital Signature 9
2.6 Transaction information 11
2.7 Visual representation of transaction propagation across bitcoin network 13
2.8 Change in bitcoin transaction fee over time. 15
2.9 Demonstration of the PPLNS mechanism 23

3.1 Use Case for User and Miner 26
3.2 Task of Mempool 29
3.3 Block Creation 29
3.4 Node selection and Nonce solving 31
3.5 Flowchart of the proposed model 38

4.1 Energy consumption by country (BITCOIN) 40
4.2 Energy consumption by country (ETHEREUM) 41
4.3 Different Computational Power of Pools 42
4.4 Comparison of Energy Consumption by Bitcoin, Ethereum and FairCoin if each node of FairCoin consumes same energy as in Bitcoin. . . 43
4.5 Comparison of Energy Consumption by Bitcoin, Ethereum and FaircoinBD if each node of FaircoinBD consumes same energy as in Ethereum. 43

List of Tables

2.1 Payment Status Description. 7
2.2 Transaction field of Bitcoin. 12
2.3 Transaction output fields. 12
2.4 Block Structure. 16
2.5 Block Header Structure. 17

Chapter 1

Introduction

Cryptocurrency is a digital unit of exchange that has been designed to work in the internet-based medium which uses cryptographic functions to secure financial transactions. At present, there are about 2000+ cryptocurrencies being traded in the world [1]. However, among these, Bitcoin is still the most popular [2]. The main purpose of using cryptocurrency is the benefit of eliminating a tertiary party acting as a central control during the transfer of funds. Furthermore, Bitcoin's longevity, resilience with diversity and technique of survival from malicious attacks makes it the most preferred digital asset [3].

Though, bitcoin has some quite strong pros like security, immutability, resilience etc., it is also subject to many problems. The most prominent among the cons is, high energy consumption of a computational node (also known as a miner) while solving the cryptographic puzzle called nonce. Nonce solving is a process of generating a cryptographic hash that gains consensus from all nodes in the network. Bitcoin uses Proof of Work consensus algorithm to determine the accuracy of a solved nonce. It is an essential part in adding a stack of transactions stored in a block to the bitcoin blockchain and in this process tremendous amounts of energy is wasted in the sense that all nodes in the network are constantly trying to mine the block they have created, but only one node which solves the nonce before everyone else in the network gets the privilege of adding the block and is rewarded. In most cases, the node with the highest computational power, solves the nonce.

Another issue of bitcoin is that, compared to credit card, PayPal or other digital currencies, it has higher confirmation time, that is, for large transactions it would take a long time for the transaction to be confirmed. It is possible to consider a transaction valid after 1 confirmation hoping that the next 5 will be received soon after, which in turn will completely confirm the transaction. Most confirmations take less than 10 minutes and for Coinbase (Cryptocurrency broker) you need 3 confirmations before an amount is spendable. This takes time and many attempts are being made to reduce it.

Alongside these issues, there is also another gap in the Bitcoin network that has recently come to light. The more computational power one holds, the more probability of finding a solution by that node or group of nodes is obtained. In the long run this can aid in biasness, in fact, it already has [4].

Thus, focusing on the stated problems, we have designed a system that uses the consensus algorithm, Proof of Work (PoW) just as in bitcoin but in a much efficient manner. Unlike in the bitcoin network, where all of the nodes indulge in mining, we propose a method that limits the number of nodes involved in the nonce solving process. The number of nodes participating is randomly selected from the whole network every time a new block has been added. Then for the confirmation time, we have proposed a way to increase the propagation speed by merging the concepts of two other cryptocurrencies propagation methodology with some additional tweaks. Lastly, we want the reward to be distributed fairly, thus creating the possibilities for computational devices with low or moderate computational power to win the rewards.

Precisely, in this paper, we propose an enhanced and an improved system to add a block to the blockchain with the help of our own model of cryptocurrency, FaircoinBD. Our main goal is to improvise the current mining technique by reducing the computational cost, mine the block in less time, propose a better rewarding system and give a fair chance for all types of nodes with different computational power (low, medium and high) to participate as well.

Chapter 2

Literature Review

2.1 Cryptocurrency and Blockchain

2.1.1 Cryptocurrency

In history's pages, we can observe the use of gold, silver and other precious materials as currency. In the 7th century, paper money backed by the government was introduced and slowly every country in the world adopted the concept. But in the last 50 years, technology has played a vital role in humanity's advancements and with the introduction of digital cash (1983) and cryptocurrency (2009) it has started taking over the concept of currency everywhere.

Throughout history, paper money has been the prime currency that has been corrupted time and time again. As paper money is controlled entirely by the government, the authority responsible can do whatever they want. They can print more money, devalue the currency whenever they want and although unlikely disappear the currency completely. But with the introduction of cryptocurrency these form of disruptions can be easily avoided [5].

Although the concept of virtual currency, digital currency and cryptocurrency is used interchangeably they have a subtle difference- Virtual Currency- According to the European Central Bank (2012) definition a virtual currency is - " type of unregulated, digital money, which is issued and usually controlled by its developers, and used and accepted among the members of a specific virtual community ". Digital Currency represents a form of virtual currency which is created and stored electronically. Cryptocurrency represents a form of digital currency which uses cryptography as a security measure [6].

There are several cryptocurrencies actively operating around the world. Among them Bitcoin, Ethereum, Ripple, Litecoin are the most prominent. Most of the cryptocurrencies are based on decentralized networks using blockchain technology, a distributed ledger enforced by a disparate network of computers. Some of the cryptography used in today's cryptocurrencies were developed for military application and made efforts to control them by legal restrictions but on the grounds of freedom of speech civilians gained the right to use them. The prime goals of a cryptocurrency is to eliminate the need for a trusted third party while making a transaction.

Currently the third parties are represented by Banks, Credit Card Company or the Government. Instead the transactions are secured using public keys and private keys to generate a signature and the system works due to different incentive system based on consensus algorithms such as Proof of Work or Proof of Stake. Even though the concept of cryptocurrency is widely popular, it still has some disadvantages. As the currencies are not rooted to any material goods it is criticized to appear out of thin air. The semi-anonymous nature of cryptocurrency transactions also make them well-suited for hostile activities. But the most prominent issue of cryptocurrency does not lie within its blockchain system but rather on its connecting components such as wallet and exchange systems which are not immune to the threat of hacking [7]

2.1.2 Blockchain

In one word, blockchain for bitcoin can be described as a 'Public Ledger'. It is a database that contains all data executions till date. In bitcoin, the blockchain network is constantly growing and creates a new block roughly every 10 minutes. Initially, each block had the size of 1mb and consisted of roughly 2700 transactions in each block. Each block in such a network is added in a linear chronological order where the current block is directly correlated with the previous block and any change in the block will actively disrupt this correlation with previous blocks. This in turn makes the network immutable and highly secure [8]. In this book, we will only look into the application of blockchain as a cryptocurrency but its potential in every other field is significant. It is used to create and exchange 'smart contract', keep track of inventory in the supply chain, create secured transactions between banks etc. The blockchain is considered as the primary innovation of Bitcoin because it uses the trustless property of a blockchain to eliminate any third party. So in turn bitcoin can be a currency which provides security to its users using cryptography and digital signature and secures the transaction using the immutable and trustless system [8]. A simple visualization is given in figure 2.1.

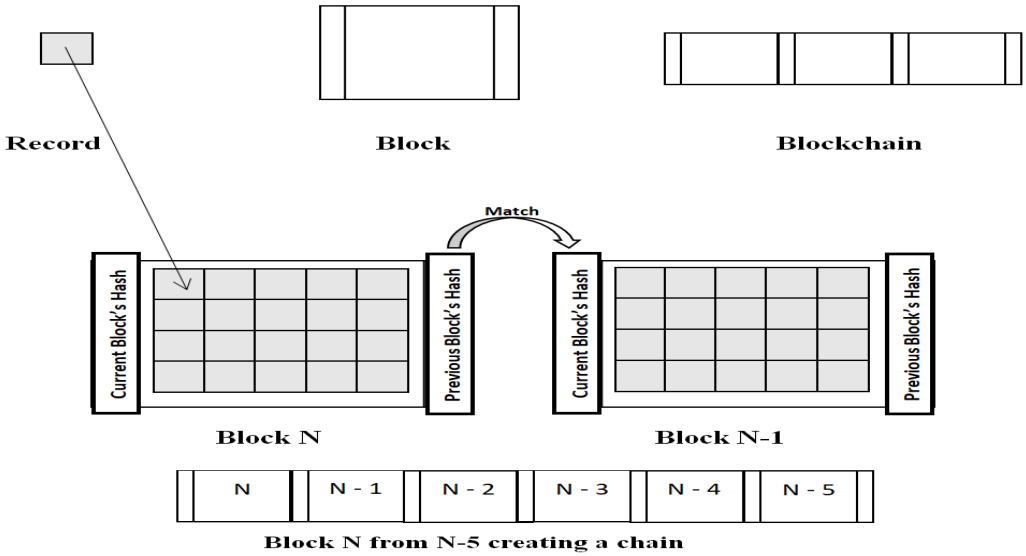

Figure 2.1: A simple Blockchain

2.2 Wallets and Digital Signatures

2.2.1 Key, Address and Wallet

Cryptocurrency wallet is software that contains cryptographic keys which allows its users to store and perform transactions. In Bitcoin each user must have his own Bitcoin wallet to take part in any transactions. Each wallet has a key pair that controls access to the Bitcoins. The key pair consists of 2 parts one being private key and the other one is public key. There are mathematical relationship between the private key and the public key which generates the public key from the private key. Currently Bitcoin uses the mathematical function of secp256k1 with Elliptic Curve Digital Signature Algorithm (ECDSA) [8]. So, the public key is generated from the private key using elliptic curve multiplication. This function is a one way cryptographic function meaning you can easily generate the public key from the private key but can't go the other way around. The relationship between them has been illustrated in figure 2.2.

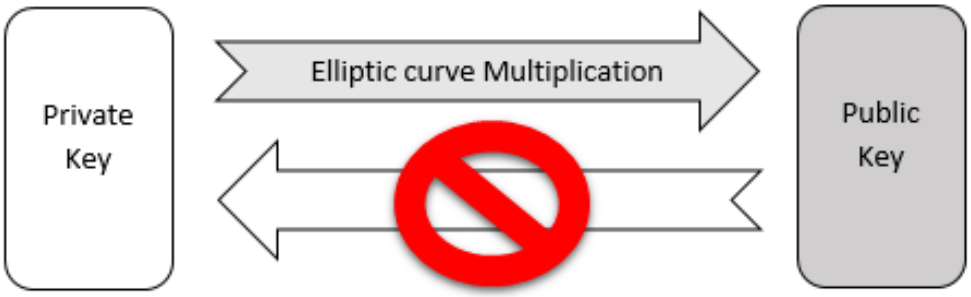

Figure 2.2: Key Pair Relationship

Private Key: The Bitcoin private key is just a number. Bitcoin software uses the underlying operating system's random number generation to produce 256 bits of entropy initialized by a human source of randomness. The private key can be any number between 1 and n-1 where n = 1.158 * 1077, which is an unfathomably large range. Below is a randomly generated private key shown in hexadecimal format-

1E99423A4ED27608A15A2616A2B0E9E52CED330AC530EDCC32C8FFC6A526AEDD

Public Key: The public key represents the address of the user and works similarly to an account number. It does not need to be kept secret as the private key cannot be generated from the public key. This reverse operation is known as- 'finding the discrete logarithm' which basically suggests trying brute force to try all possible values of the private key.
If we consider public key as P and private key as k then,

P = k * G where G is a generator point defined by elliptic curve [9].

Bitcoin address: The bitcoin address is a string of digits and characters that is created for sharing with anyone you the user wants to allow transactions with. It mostly appears as the 'recipient' in a transaction. The bitcoin address works similar to the 'pay to the order of' part on a cheque. It represents someone's name or their publicly available information.

The Bitcoin address is derived by hashing the public key twice with Secured Hash Algorithm (SHA-256) and Race Integrity Primitives Evaluation Message Digest (RIPEMD160) hashing algorithms. Then the public key hash is encoded using Base-58 Encoding system. The generated result is known as the Bitcoin address [9] The relationship is shown in Figure 2.3.

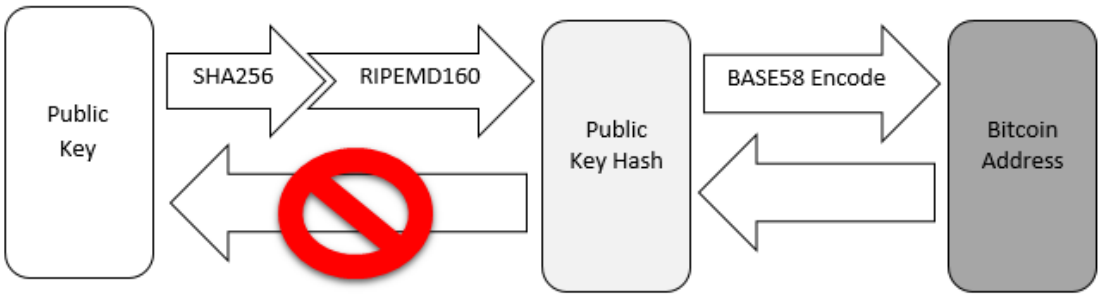

Figure 2.3: Public Key to Bitcoin Address

Wallet: This Bitcoin address is used to make transactions. Wallets only contain the keys but the coins itself is stored on the block-chain. Coinbase is one of the most popular cryptocurrency exchange system. In coinbase the wallet uses push payment method meaning the customer pushes the payments directly to the merchant including the address and amount. When a payment with cryptocurrency occurs a charge request is created. When a payment is made the transaction is broadcast over the network for confirmation. The charge request then waits for inbound payments and each charge has an associated payment status [10] Some of the payment statuses are described in table 2.1.

Pending	**Completed**	**Expired**
Transaction detected in Blockchain but not yet validated.	Transaction validated and confirmed by the network.	Charge request has been alive without payment for 60 minutes.
Unresolved	**Resolved**	**Cancelled**
Transaction has been confirmed but some other complication occurred.	The transaction has been confirmed and marked as resolved.	The request has been cancelled. (It cannot be cancelled if a charge has been detected).

Table 2.1: Payment Status Description.

The visual representation of coinbase wallet is given in figure 2.4 [10].

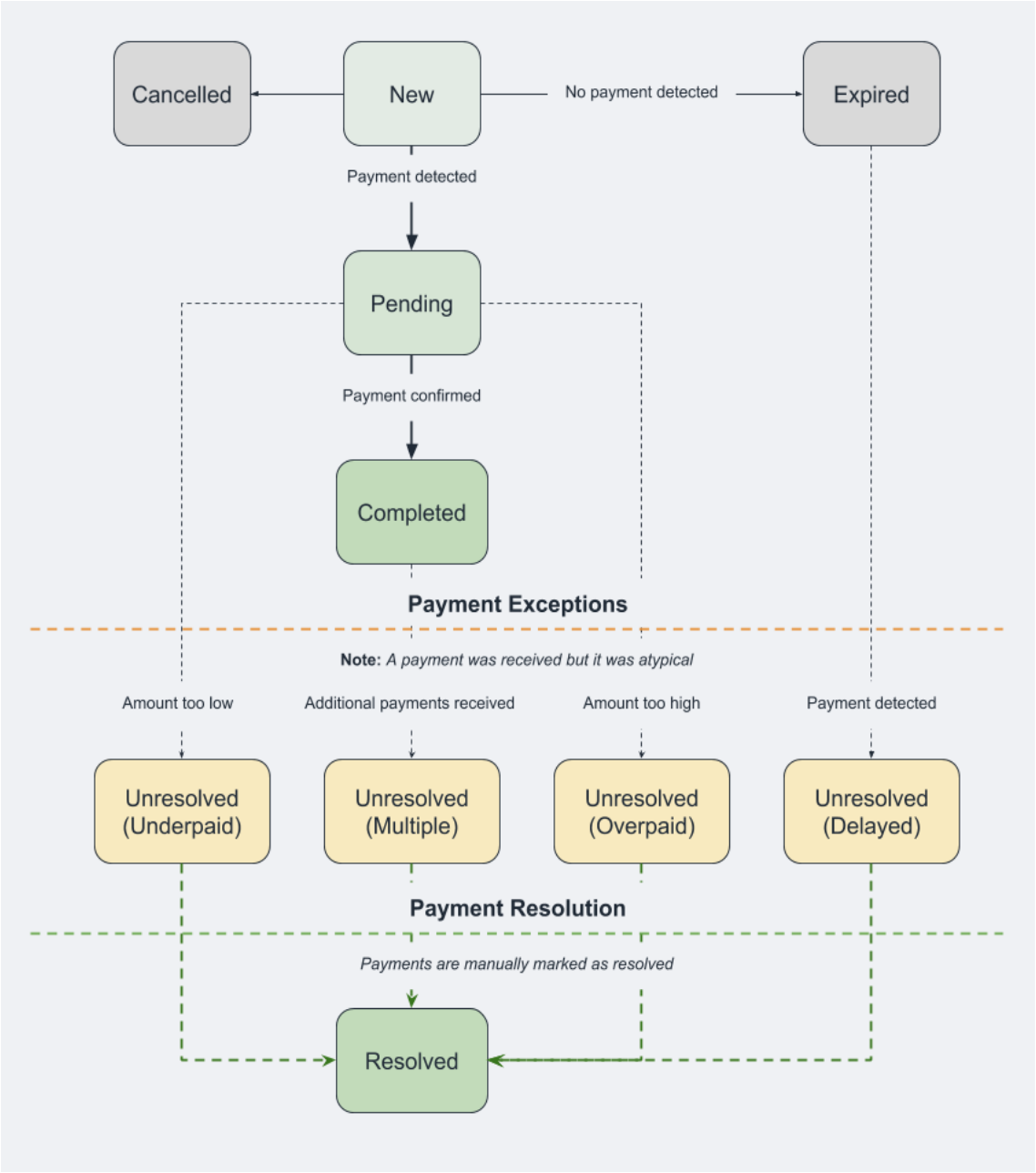

Figure 2.4: Visual representation of coinbase wallet

2.2.2 Digital Signature

A digital signature is basically a mathematical scheme that ensures authenticity of the transaction. As the name suggests it is the digital equivalent of handwritten signature but provides more effective security. Digital signatures are based on public key cryptography which is also known as asymmetric cryptography. The visual representation of a basic digital signature is shown in figure 2.5. If User1 wants to send some Bitcoins to User2, the wallet of User1 has to encrypt the transaction using his private key and User2's public key. Then, the transaction is propagated to the network. In the network, every node tries to open the transaction using their private key, however, only User2 with his/her private key and User1's public key can open the transaction.

.

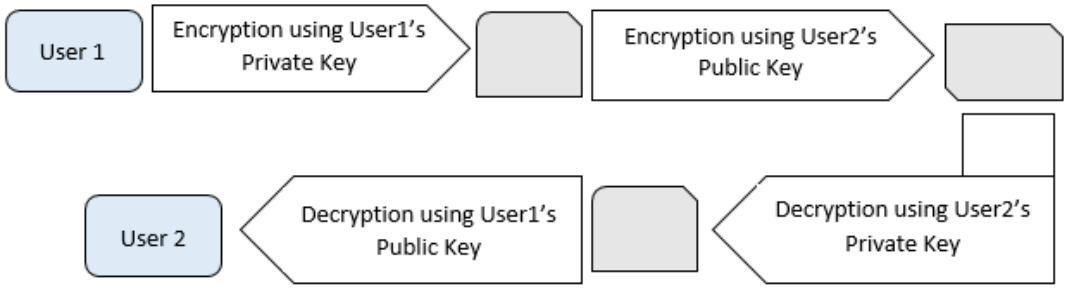

Figure 2.5: Digital Signature

2.2.3 Schnorr Signature

Schnorr signature is considered the next big implementation in the cryptocurrency industry after the introduction of Segwit. Schnorr signature is a digital signature system named after Claus Schnorr. The main advantage of Schnorr signature is that it allows MultiSig. MultiSig or Multisignature is a technique that requires another user or users other than the one making the transaction to sign the transaction before it's broadcasted effectively adding an extra layer of security. There are some MultiSig protocol that are being used right now but they are reported to have some drawbacks such as- Scripting errors, Efficiency loss etc. Schnorr signatures solves this problems and maintains the property of linearity. The main difference between Schnorr Signatures and Elliptic Curve Digital Signature algorithm is that Schnorr Signatures are linear even though both of them use a random point on the elliptic curve.[11] In a paper written by G. Maxwel, A. Poelstra, Y. Seurin, P. Wuille they provided an implementation of Schnorr Multi-Singature with its application to bitcoin. They have designed a protol that was simple and efficient, having the same key as the standard schnorr Singature with the same verification method as standar schnorr signature. [12] So, with the implementation of Schnorr Signature in cryptocurrencies secuirity and efficiency will surely bring about a positive change.

2.2.4 Elliptic Curve Digital Signature Algorithm (ECDSA)

ECDSA and all other elliptic curve cryptography are based on the belief that finding a solution to the discrete logarithm problem on an elliptic curve is extremely difficult. Although there hasn't been any proof that it cannot be solved in polynomial time. Considering,

U = user, m = message, M = merchant, a = secret integer chosen by user.
Given that,
$F_q = Finitefield$,
E = Elliptic curve,
P = Base point,
H = Hash function,
r = Order,
s = Signature
The elliptic curve is over a finite field so, E/F_q &
The base point $P \in E(F_q)$ of order r [Represents the base of alogarithm]
Private Key, k = a mod r, i.e. a $\in Z/rZ$
Public Key, Q = aP.

Then,
signing and verifying is done in 4 steps-

1. U choses a random number(different each time) where, $1 \leq n < r$, and finds R using the formula,

$$R = nP \in E(F_q)$$

2. U computes s by using the formula, $s = K^{-1}(Hm + ax_R)$ in Z/rZ,

The derived Signature is (x_R, s)

3. M computes $u_1 = s^{-1}H(m)$ and $u_2 = s^{-1}x_R$ in Z/rZ and then.

$$V = u_1P + u_2Qon(E)$$

4. M verifies the signature of U by matching x_R & x_V where,

Z/pZ holds

The private key k can only be calculated from P & Q if it is somehow possible to compute the discrete logarithm extremely quickly [13]

2.3 Insights of Bitcoin Transactions

Transactions are a core part of bitcoin and without it the whole system would become meaningless. Transactions go through few steps before being included in the blockchain. There are basically 4 steps involving transactions:

1. Creation
2. Propagation
3. Validation
4. Addition in the block

2.3.1 Creation

Transactions are data structures that encode the transfer of value between participants in the bitcoin system. The data that is entered into the bitcoin ledger is basically a double entry book, meaning it records both the input and output. A glimpse of the transaction information is given in figure 2.6 [14].
.

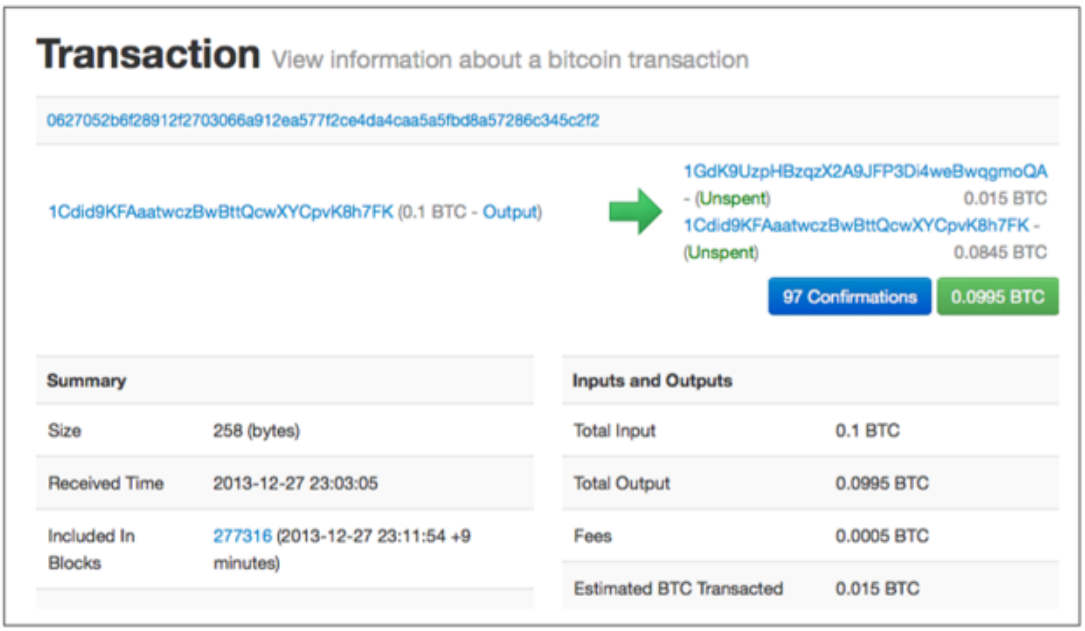

Figure 2.6: Transaction information

In bitcoin, the money is also a data structure and the transfer of money or the transactions can be created both online and offline by anyone who is in the bitcoin network. As soon as the transaction is created, it is signed by the owner of the funds. If it was properly formed and signed, the signed transaction becomes valid and has the necessary information needed to transfer funds. This valid transaction has to reach the bitcoin network so that miners can validate it and put in their memory pool for creation of next blocks. The size of each transaction is 300-400 bytes of data. There is no concept of trust in the process of exchanging the data

with the node that is going to propagate (as long as they send it to more than one). Unlike credit card transactions, which contains sensitive information and can only be transmitted through encrypted networks, transactions have no confidential information such as the private keys or credentials, and as a result it can be publicly broadcasted as long as it reaches the bitcoin network. The transation fee of Bitcoin and the transaction output fields have been describe in tables 2.2 and 2.3 [15].

Size	Field	Description
4 bytes	Version	Specifies which rules this transaction follows
1-9 bytes(VarInt)	Input Counter	How many inputs are included
Variable	Inputs	One or more transaction inputs
1-9 bytes(VarInt)	Output Counter	How many outputs are included
Varibale	Outputs	One or more transaction outputs
4 bytes	Locktime	A Unix timestamp or block number

Table 2.2: Transaction field of Bitcoin.

Size	Field	Description
8 bytes	Amount	Bitcoin value in satoshis (10^{-8} bitcoin)
1-9 bytes (VarInt)	Lockink-Script Size	Locking-Script length in bytes, to follow
Varibale	Locking-Script	A script defining the conditions needed to spend the output

Table 2.3: Transaction output fields.

Now the question arises, output or input, which comes first? Outputs come first because coinbase transactions generate new bitcoin, they have no inputs and create output from thin air. Coinbase transactions are the bitcoins generated when a block is added to the blockchain. These are rewards for the miner who is able to find the nonce first. These transactions have no input rather they are shown as output to the miners' addresses. As of December 2019, it is 12.5 BTC.

2.3.2 Propagation

Transactions are propagated to the adjacent nodes [16], [17]. If all the conditions are met a success message will be returned synchronously to the originator and vice versa. This process allows the transaction to propagate through to the whole network in a few seconds. Furthermore, as every node is responsible for checking the transaction,it helps to reduce the possibility of network attacks such as DOS

and DDOS [15]. An illustration in figure 2.7 shows how transaction are propagated across the bitcoin network.

.

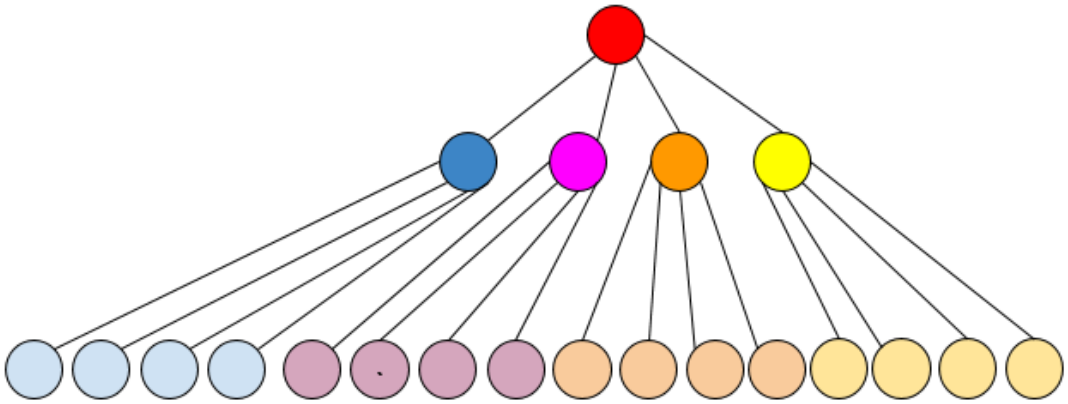

Figure 2.7: Visual representation of transaction propagation across bitcoin network

2.3.3 Validation

UTXO stands for unspent transaction output. These basically are indivisible chunks of bitcoin currency same as a 100 dollar bill. However, as this is a crypto currency it is locked to a specific owner and recorded on the blockchain which everybody in the network recognizes. As soon as a user receives bitcoins, it is recorded within the blockchain as a UTXO. It means that a user can have many UTXO (Dollar bills) spread across hundreds of blocks.
As a user's total amount is basically a combination of multiple UTXO's, there might be cases where the amount (UTXO) is much larger than what he is spending on. However, same as actual money, it has to be totally consumed and the change would be generated. For example, if Jumana has 10 bitcoin UTXO and wants to pay Maruf 5 bitcoins, her transaction has to consume the entire 10 bitcoin UTXO and generate 2 outputs:

1. paying 5 bitcoins to Maruf
2. 5 bitcoins in change back to her wallet

The UTXO that Jumana gave is called the transaction inputs, while the UTXO generated by a transaction are called transaction outputs. Transactions consume UTXO unlocking it with the signature of the current owner and create UTXO locking it to the bitcoin address of the new owner.

According to Andreas M.Antonopoulos in his book Mastering Bitcoin, the transactions are verified though 18 criteria however these criteria change over time based on different requirements and they are mostly responsible for preventing DOS and DDOS attacks to the bitcoin network. Some of these criteria are simple as just checking the syntax and data structure on the other hand some are complex like validating the unlocking scripts for each input [15].

2.3.4 Addition in the Block

The best thing about bitcoin is that mining nodes (who are also full nodes) do 2 things in parallel,

1. Create a draft block known as the candidate block and put transactions in that block and try to add it to the blockchain.

2. The node is listening for transactions and verifying them and putting it in their own transaction pools (memory pool) and passing it on to other adjacent nodes.

Once the block the miner is trying to create is mined by someone else, he looks in the transaction pool (memory pool) if any of these transactions have been added to the newly created block.

Once recorded on the blockchain and confirmed by sufficient subsequent blocks (confirmations), the transaction becomes a permanent part of the bitcoin ledger and is accepted as valid by all participants.

2.3.5 Transaction Fees

Transaction fees are an essential part of bitcoin network however as more versions have appeared the concept of fee less transaction have been depreciated. At one-point transaction fees were not necessary and your transaction would be added to the blockchain anyways but at a cost of time.
Transaction fees are basically the excess of inputs minus outputs. That is,

$$Fees = \sum input - \sum output \tag{2.1}$$

Thus, whenever making a bitcoin transaction, if you forget to add a change output in a manually constructed transaction you will be paying the change as a transaction fee and you might end up giving 100's dollars to the miner.

Transaction fees are there to encourage miners to add the transaction to the blockchain. The higher the fee, the quicker it gets added to the chain.

Miners have the luxury to pick and choose which transactions are included in each block, and there is a limit to the number of transactions that a block can fit (1MB of data). As a result, miners prioritize transactions with higher fees over those with low or average fees. The amount of the fee is changed based on a condition. For example, if the network is congested, meaning there are a lot of people making transactions, a user is likely to pay a higher transaction fee for their transaction to be processed at all, let alone quickly. This actually happened in the late 2017 when the price of Bitcoin's was a record high as transactions were happening at a very high rate and the average fee for a transaction was nearly $40 [17]. A graphical representation has been shown in figure 2.8 [17].

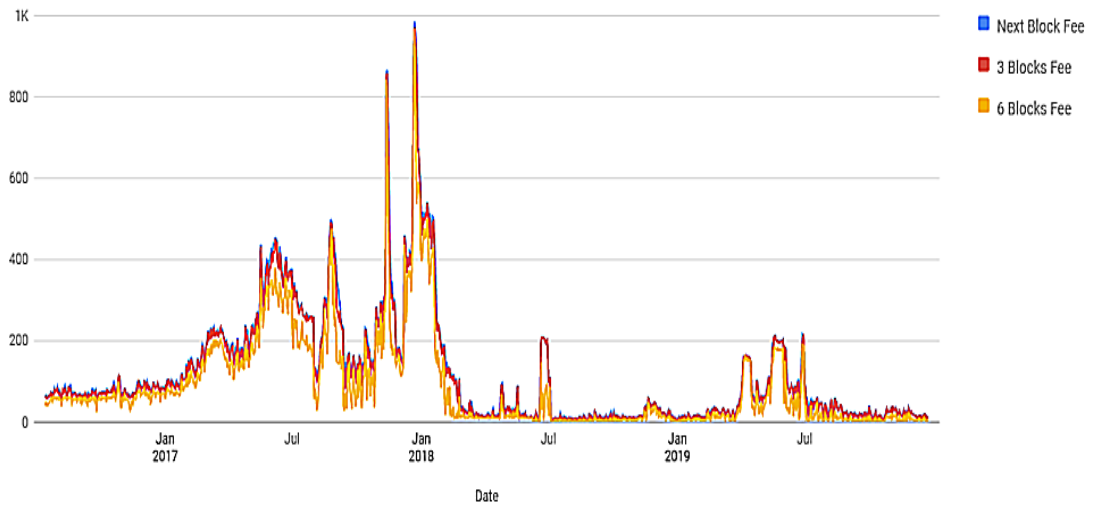

Figure 2.8: Change in bitcoin transaction fee over time.

.

2.3.6 Understanding Bitcoin transaction locktime

The Bitcoin transaction locktime is basically the time at which a transaction would be added to the blockchain. There are two types of transaction locktime. First of all, when the locktime number is less than 500 million, it is interpreted as a block number (block height) and the miner has to wait until that block number has been reached. However, If the figure is above 500 million it is considered a unix timestamp (a unix timestamp being the number of seconds since January 1st 1970) [16].

Even though bitcoin sounds trustable way of transferring money it has some problems namely higher fees for small transactions, transaction malleability and high confirmation time.

2.3.7 What impact has Segregated Witness (SegWit) had on fees?

Segregated Witness (SegWit) is a Bitcoin code upgrade that was implemented in August 2017. The main goal of this update was to fix a problem known as transaction malleability. According to Bisola Asolo "Transaction malleability is the process of changing the unique identifier of a transaction by first changing the digital signature used to create it" [18].

Let's say Jumana sends 10 bitcoin to Alif with a transaction id tx J. However, before the transaction even gets confirmed, Alif changes the signature data of the transaction and generates a new Tx id A. Having received the 10 bitcoin but with Tx id A, Alif then informs Jumana that he has not received the bitcoin. When Jumana searches a block explorer using Tx id J to confirm Alif's claim, she isn't able to find the transaction. As a result, she thinks that the transaction never reached

Alif and sends the bitcoin again resulting into Alif having 20 bitcoins now.

The solve for this was by separating the transaction data and the digital signatures with them to prevent the changing of the transaction ID to affect the digital signature. As the digital signatures were removed from the block the block had more free space thus the increase in the amount of transactions per block.

2.4 Block Structure in the Blockchain

A block is a data structure that can contain a collective number of transactions which requires to be added to the distributed ledger, blockchain. A block consists of 2 things, namely a header that is of 80 bytes and a stack of transactions with an average size of at least 250 bytes that fill up the block. On average a block contains about 500 transactions or more [14]. The structure of the block has been detailed below in figure 2.11.

However, the block header can be broken down further. Figure 2.12 shows the structure of the block header in detail but in precise it contains 3 things:

1. Reference to the previous hash of the block
2. Timestamp and the nonce (required for mining process)
3. Merkel Tree Root (a hash of all the hashes of the transactions in the block [15])

Block structure is demonstrated in the table 2.5 and table 2.6 [19].

Size	Field	Description
4 bytes	Block Size	The size of the block, in bytes, following the field
80 bytes	Block Header	Several fields form the block header
1-9 bytes (VarInt)	Transaction Counter	How many transactions follow
Variable	Transactions	The transactions recorded in this block

Table 2.4: Block Structure.

Size	Field	Description
4 bytes	Version	A version number to track software/protocol upgrades.
32 bytes	Previous Block Hash	A reference to the hash of the previous(parent) block in the chain
32 bytes	Merkle Root	A hash of the root of merkle tree of this block's transactions
4 bytes	Timestamp	The approximate creation time of this block (seconds from Unix Epoch)
4 bytes	Difficulty Target	The Proof-of-Work algorithm difficulty target for this block
4 bytes	Nonce	A counter used for the Proof-of-Work algorithm

Table 2.5: Block Header Structure.

2.5 Consensus Protocols/Algorithms

Cryptocurrencies are built on the architecture of blockchain and one of the most crucial part of every blockchain network is ensuring the presence of security and integrity which is achieved via consensus protocols/ algorithms in the decentralized and distributed network. To be clear, consensus protocols refer to the primary rules of a blockchain, whereas, consensus algorithm refers to the mechanisms through which these rules are followed [20]. More precisely, in the bitcoin network, bitcoin is a consensus protocol and Proof of Work (PoW) is a consensus algorithm.

A consensus protocol defines :

- the way nodes should interact
- the way data must be transmitted among them
- what requirements shall be fulfilled to validate a successful block

A consensus algorithm :

- verifies balances
- verifies signatures
- confirms transactions
- validates a successful block

In blockchains, there is no central authority to validate and verify the transactions, yet the claim is that each and every transaction in the blockchain is secured and verified. This is due to the presence of the consensus protocol/algorithm in the blockchain network. Consensus algorithm is basically a means to create a mutual agreement among the peers in the network about the state of the distributed ledger.

Objective of consensus algorithms

- Agreement
- Co-operation
- Equal rights to every node
- Mandatory participation of each node in the consensus process

3 things are achieved explicitly

- Reliability in the blockchain
- Trust among unknown peers
- Only one block is accepted by all nodes

Hence, consensus algorithms are mainly responsible for bringing decentralization in the blockchain system.

The most known and used cryptocurrency consensus algorithms are Proof of Work (PoW) and Proof of Stake (PoS). Though these two are the most popular, there are more consensus algorithms. To list all

- Proof-of-Work
- Proof-of-Stake
- Delegated Proof-of-Stake
- Leased Proof-Of-Stake
- Proof of Elapsed Time
- Practical Byzantine Fault Tolerance
- Simplified Byzantine Fault Tolerance
- Delegated Byzantine Fault Tolerance
- Directed Acyclic Graphs
- Proof-of-Activity
- Proof-of-Importance
- Proof-of-Capacity
- Proof-of-Burn
- Proof-of-Weight

In our proposed model, we focused mainly on three of these algorithms, namely Proof of Work (PoW), Proof of Stake (PoS) and Proof of Elapsed time (PoET).

2.5.1 Proof of Work

Satoshi Nakamoto, still an unknown figure, designed and created Proof of Work (PoW), the first and the most popular consensus algorithm used by bitcoin to tackle the Byzantine faults [6].This algorithm is mainly about choosing the miner who is able to solve a complex mathematical puzzle/problem which requires a lot of computational power. The node who solves and gets a solution of the puzzle first, gets the privilege to mine the next block. And this consensus mechanism is the choice of majority of the cryptocurrencies currently in circulation [21].

To elaborate, in Bitcoin's Proof of Work, the miners stack up the transactions in a block and then try to mine it. To mine this, they are required to solve a hard-mathematical problem. The nonce, which is an integer value, is first appended to the hash of the block to be added in the blockchain. This appended value is rehashed and this rehashed value is the solution to the mathematical problem if this number is less than or equal to the target hash. The target hash is a difficulty restriction level that could be adjusted to ensure that the blocks are processed efficiently [22]. And the hash is a string of fixed data that is generated by the input of a string of data of any size to a hashing function (e.g. SHA256). However, the target hash is set by the cryptocurrency network and miners try to find it by incrementing the value of nonce trying out all the possible values. Besides, the lower a target is, the more difficult it is to generate a block. This target hash adjusts once every 2016 blocks [23]. This adjustment is based on the computational power and the average block creation time.

Two main advantages of PoW is that it is hard to find the solution for the mathematical problem and once found it is easy to verify it. On the other hand, the main issues of this protocol are that it is time and resource consuming, and takes a while for the transaction confirmation.

2.5.2 Proof of Stake

This consensus algorithm was introduced to overcome the drawbacks of Proof of Work. The method here is to use the coins in possession of the nodes instead of the computational power of the nodes. This means, the more coin one holds, the more mining chances one has.

The Proof of Stake process uses a pseudo random election process to select the validator of the next block based on a combination of factors: Staking age, Randomization and the nodes wealth. In Proof of Stake, the block validators are not called miners, instead, they are referred to as forgers or minters. However, the Proof of Stake process begins with pre-mined coins or by earned coins from Proof of Work and then switched towards Proof of Stake. To participate in the forging process, nodes need to put a certain amount of their coins at stake in the network. Based on

the percentage of the stake placed by each node, the chances of the node to be the next validator is determined. To avoid the rich from getting richer, Proof of Stake is used along with two methods, Randomized Block Selection and Coin Age Selection. In the Randomized Block Selection, the node with the lowest hash value and highest stake is selected as the validator. And in the Coin Age Selection, a parameter called Coin age is used to choose the node.

Coin age = Number of days the coin is held at stake × Number of coins that are staked.

Once the node forges a block, the coin age of that block rests to zero and the node has to wait for a certain time to be able to forge again. This system ensures fairness by avoiding the largest stake node to be selected.

The pros of PoS are that it is energy efficient by avoiding the usage of expensive high-power consuming hardware, secure by making it extremely expensive and risky for 51% attack, it is more decentralized and aids in keeping the bitcoin prices to be stable [24][25].

2.5.3 Proof of Elapsed Time

Proof of Elapsed Time also emphasizes on preventing the usage of high computation resources and excessive energy consumption. This process uses a lottery system to bring efficiency. Since this algorithm is used in a private network unlike PoW and PoS. In Proof of Elapsed Time, a node first has to identify itself in the network and get the permission from the network. The blockchains that such networks use is called permissioned blockchains, mainly preferred by centralized organizations. The nodes participating in the mining process is randomly given a certain time to wait and when this waiting time is over, the node gets the privilege to add the block to the blockchain. This random waiting time is generated by the nodes. Moreover, the node who wins to add the block, adds it to the network and broadcasts the required information to the entire network.

This mechanism requires to ensure the following:

- The nodes should generate a random time
- The waiting time is complete before a node wakes up

The process is almost similar to the Bitcoin's proof of work except for the need of power consumption. Furthermore the sleeping time of the nodes are making the system energy efficient [26] [27].

2.5.4 Related works concerning Consensus Algorithms

There have been several recent studies on improving the mining process of a block mainly by making changes in the consensus algorithms. In such a study [28], the authors tried to tweak the PoW algorithm and combine it with PoS. Their method was to use PoS to keep the honesty of a miner on stake instead of coins. Thus, this

is merely calculating the number of times a miner is successful in adding a mining block and is represented as Success Times. Each miner has different difficulty which is determined by the coefficient of the success times. That means, the chances for a miner to mine a block is easier, if the success times score for the miner is higher. Moreover, they have also tackled the problem of malicious nodes involvement by penalizing them as blacklisting them on the network.

In another study [29], the emphasis was made on the issue of centralization of power due to mining for which there is a high risk of tampering. To solve this, the authors proposed a fair mining system that evaluates the computing power of each node and based on this evaluation the difficulty as well as the reward for the node is adjusted. Here, the participating term is evaluated instead of evaluating mining costs. The higher the value of the participation term, the more resources are used by the node.

2.6 Mining Pool

Mining is a process of finding nonce to add a specific block to the chain. If a miner cannot find a nonce at the first time other miner will find it out eventually. So basically the work that first miner did is meaningless. Now a days a single miner has a lower chance to find a nonce and find the block. In order to win more and get reward more the miner unite together and form a mining pool [30].Large amount of miner nodes in Bitcoin system join as a mining pool to work on finding new blocks together and share the reward with each other based on the work of each nodes. A person or company owns a mining pool. The owner is called pool coordinator or manager. Pool coordinator takes a small amount of fee for his services.Different pools have different strategy to pay reward.A pool will always maximize their earning by selecting the optimal subset of transaction from the memory pool which increase the amount of fees but it keeps the block size same. This is a vaiation of 0-1 knapsack [28]. The transaction selection policy by default [31] works by selecting transactions from the mempool as follows:

- Transacetion are orderd in a descending order by Fee-Per-Kilobyte.
- Transaction which are not selected will be left in the memory pool for new blocks.

Previously in bitcoion system, there was a rule which was to save 50 kb of each block for high-priority transactions [32]. However getting some updates later on bitcoin changed this system. Important work to run a mining pool is to make sure the distribution is fair among the miners. At first miners used the getwork interface which gives them nothing but block header. So the miners had to generate so many hash and find the nonce. Before finding the final nonce no miner gets new work from the pool. After that bitcoin started getblocktemplate, where miners are provided a template. What they do is, they use the template to try and generate the next block. In this process the miners gets the freedom to choose transation but it takes more bandwidths. After that the timestamp comes which ensures that the workers are testing more and more combination to get the next work. In the Stratum protocol [31]the pool gives the miner a template that thehy can use to produce their own work. This make sures tha miners are requesting less. It is faster

than its previous protocols because it keeps a distance from HTTP protocol and it also reduces bandwidth. It also can manage new coming blocks which reduce stale work. Now a days most of the mining pools use Stratum Protocols as it make sure it is fast and proper workloads.

A non-extensive list of other available features includes:

- **Transaction Fee:** Fee of the transaction in satoshis. It is a one hundred millionth of a single Bitcoin (0.00000001BTC).
  Transaction Fee = Sum of Inputs - Sum of Outputs

- **Transaction Size:** Size of the transaction in bytes

- **Wallet Address:** A list of the wallet addresses involved in the transaction. A Bitcoin address is an identifier of 26-35 alphanumeric characters, beginning with the number 1 or 3.

- **Size of Previous Block:** The size of the previous block will affect the time it will take to be distributed through the network.

- **Transaction Load:** The number of transactions per second between the current block and the previous block. This provides an estimate of the load of the network [32].

For the reward distribution part among the miners the mostly used system is call Pay-Per-Last-Nshares, in short form PPLNS which distributes the reward according to the last N share reported by the miner [33]. When the miner report their shares and if the share is not in the N shares, the miner donot get anything.since different reporting strategies may get different rewards for the miners. However, in the literature, the share reporting problem has not got any attention from researchers [33].

2.6.1 Pool selection and Reward system

There area two types of pool for the miners. They could join to any one of them because they have the similar computing power but different reward distribution system. Both type the pool owner will take his share. The two different payment system is PPS and PPLNS. PPS means pay-per-share which is slightly different from PPLNS [34].

.

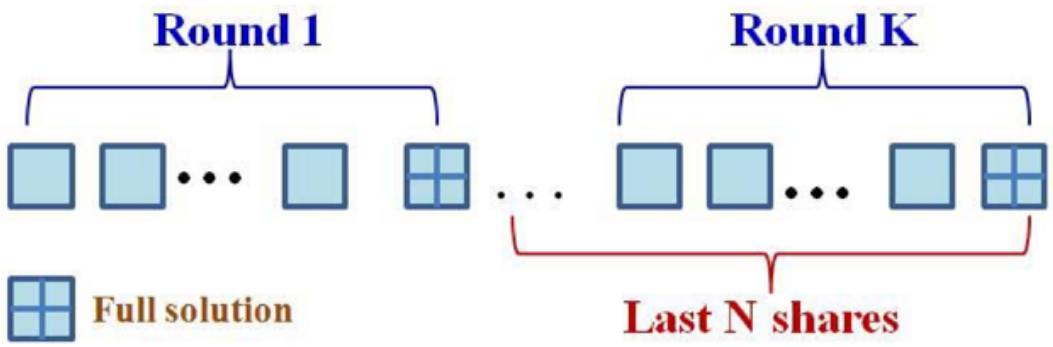

Figure 2.9: Demonstration of the PPLNS mechanism

SSuppose in PPS system, there is 100000 shares per block. If a miner gets to solve 10000 shares and quit doing anything more, he will get 10% of the full share as 10000 is 10% of 100000.

Suppose In PPLNS system, there is 100000 shares per block and there is something called round. After completion of a round only then miners can get rewards they owe. So suppose there are X rounds and in each round there are Y shares. If only 1 share is submitted by the miner from Y shares. The miner will get reward for only submitting one share.

So basically miners look for pools where they will find more reward based on the job. So that's why now a days PPLNS is much more popular as fraud people donot have to chance to do anything bad [34].

Chapter 3

Algorithm & Design of the Model

3.1 Motivation

In an era where communication and technology can demolish barriers between countries, currency is one of the few things that is still centralized and very private to each country. But with the introduction of bitcoin in 2009 and it's first transaction occurring in 2010, everything changed. People now have access to a decentralized currency that is available to them all around the world. Even though it might seem like a dream come true, bitcoin still has its disadvantages. As bitcoin network uses Proof of Work consensus algorithm and requires every miner node in the system to participate in the nonce solving process, it draws out a lot of energy. As of 2019, bitcoin is estimated to consume 66.7 Terawatt-hours per year, which is comparable to the energy consumption of Czech Republic, a country of 10.6 million people (where 0.2% of global electricity used) [35]. With such a large amount of energy consumption, carbon dioxide emission from the bitcoin network is as high as 22.9 million metric tons [36].

Also, the bitcoin network itself is getting power hungry day by day. As it requires miners to solve nonce and the difficulty of the nonce is decided by the total hash rate of the network, low or even medium configuration holding computers are almost declined from entering the competition. As of late with the introduction of Application Specific Integrated Circuit (ASIC), miners, even high configured computers are falling behind. So, the system is becoming unfair to a point where it is not mined by individuals anymore but rather by huge companies. Different centralized mining pools such as AntPool, BTC.com, BTCC Pool etc. are the primary miners right now. There is also the possibility of Quantum Supremacy where a Quantum computer might be able to solve nonce and add blocks at an extremely fast rate for two weeks (until target hash is changed) thus mining a huge amount of bitcoin in a very short time. It just might be the great hit that will destroy bitcoin.

In our proposal and system design, we have suggested solutions to these problems and adopted some of the great features bitcoin has to offer which will result in a system that can sustain in the future.

3.2 Registration

Before beginning with how to start with our proposed system. Let us get clear about the idea that there are many types of nodes in the cryptocurrency networks and each type of the nodes have their own vital role to play to function in the network [35]. Since our main focus is on the energy efficiency and fair system of reward distribution, we will describe the model of our system using the two main types of nodes [36]:

1. **General Users:** These nodes are just client nodes who use cryptocurrencies for their own convenience.

2. **Miners:** These nodes are the ones who are responsible for creating a block and adding it to the blockchain.

3.2.1 Becoming a FaircoinBD user

To use any cryptocurrency, an individual needs to install a client application or to be more precise, have access to a user interface to get started in the network. The user interface is more commonly known as the wallet. So, a user needs to install an application first. Then, running the application will automatically result in creating a wallet which contains a private key and a corresponding valid address that can be used in the network. Now, the user is ready to receive funds. However, at this point, this address is unknown to the network. This becomes known once it has been associated with a transaction. But, for a transaction to be propagated all over the network and added to the transaction memory pool, it has to be verified based on some defined rules mentioned previously in section 2.3.3.

Algorithm 1 Pseudo-code for Transaction verification:

```
1: procedure TRANSACTION_VERIFICATION
2:     loop:
3:     while (new trasaction) do
4:         if (satisties condition) then
5:             Propagate to adjacent nodes
6:             Add to temporary transaction pool.
7:         else
8:             Prompt user transaction unresolved.
9:     end while
10: end
```

3.2.2 Becoming a FaircoinBD miner

Again, to be a miner in the network, the miner has to install a mining software. All the process to be a miner is similar to a bitcoin miner except that miner of this network has an additional criterion to fulfil which also is very crucial for this network. And this criterion is being a staker.

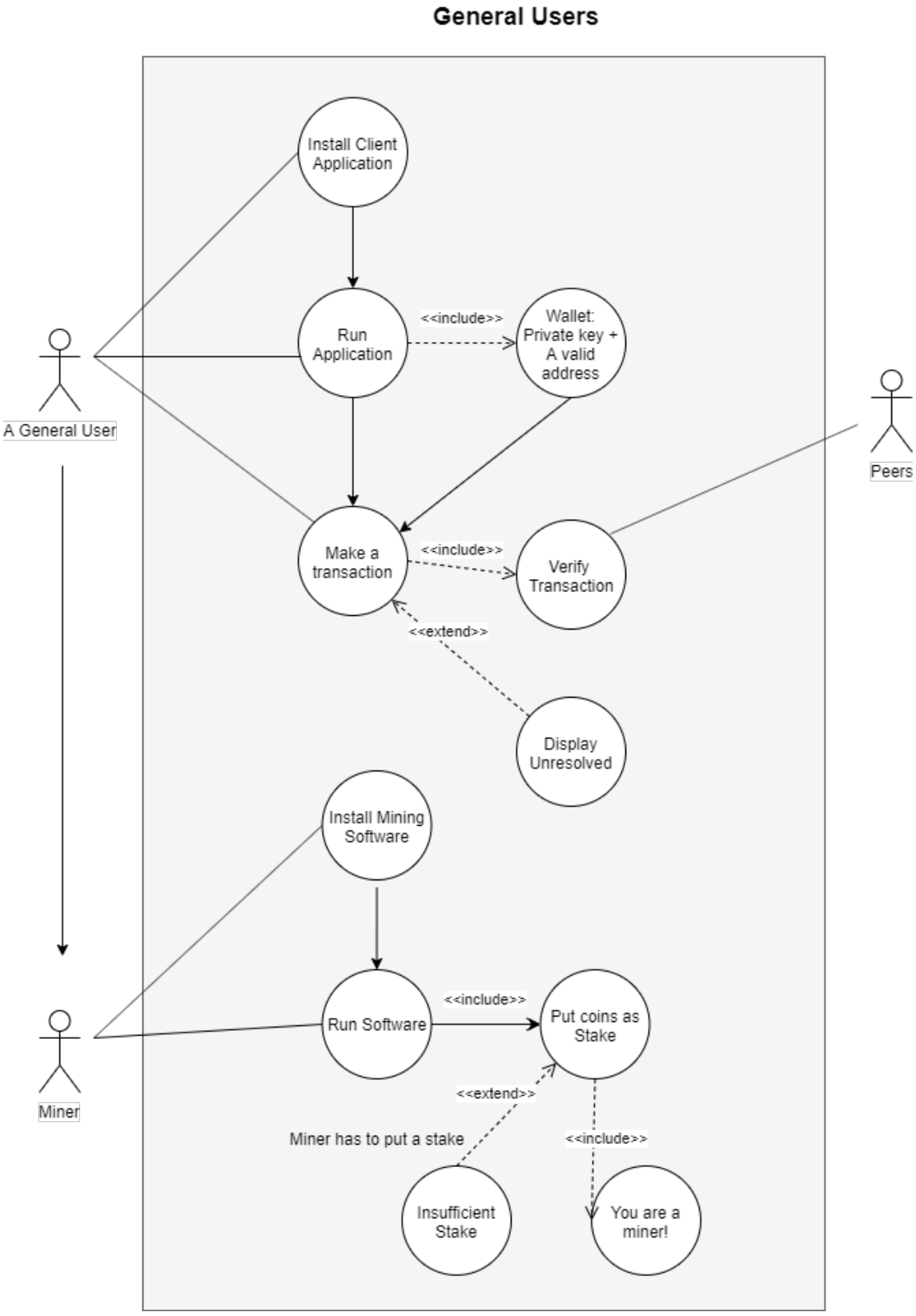

Figure 3.1: Use Case for User and Miner

3.2.3 Stake

A node to be allowed to mine in this network must put some coins on stake. More simply, the nodes need to lock up some of their coins in one place [37].

3.2.4 Addition to main pool

After the nodes put some of their coins in stake, they are allowed to participate in the block creation and adding a block to the blockchain. These allowed nodes are put in a main pool and the main pool contains all and only the nodes who wants to mine.

3.2.5 Sub pool Creation

A certain number of the total number of nodes from the main pool is selected randomly to create sub pools.

Pseudo code for Sub pool creation:

Algorithm 2 Sub-Pool Creation:

```
Number of total nodes in the main pool = T_N
Number of nodes in each pool = S_TN
Sub pool number = S_N
S_N = Floor(log(T_N))
S_TN = Ceiling(T_N ÷ S_N)
procedure CREATE_SUB_POOL
    remainder = S_TN × S_N
    Condition:
    if (remainder == 0) then
        Stop Creating Pools
    else
        Pool(S_N + 1) == remainder
end
```

Moreover, among all the sub pools generated, the sub pool with the highest computational power would be selected (So, it is basically randomly selecting a number of nodes and then selecting the best among the random sets of nodes). If by any chance, two or more sub pools have the same highest computational power, the sub pool will be selected randomly among them. In short, the sub pool with the highest computational power will get selected to participate in the mining process irrespective of what is each node's computational power and how much coin is each node putting on stake. Here, the selection of one sub pool contributes to wasting less energy by reducing the number of nodes using their computational power to solve the nonce. This is explained on the next page in more detail

Let the notations denote as follows:

N = Total number of nodes in the network.
E = Amount of energy wasted by the total number of nodes in the network.
X = Number of nodes in the selected sub pool.
So,

$$N \rightarrow E \tag{3.1}$$

$$X \subset N \tag{3.2}$$

$$X \rightarrow ((E \div N) \times X) = P \tag{3.3}$$

where,
P = Amount of energy wasted by the nodes in the selected sub pool.

Therefore,

$$\mathbf{P << E} \tag{3.4}$$

3.3 Transactions

Even though we are using the concepts of bitcoin in most of the areas of our system there is a slight change in terms of transactions. In our system as the transactions are coming into the network they get verified by each node in the main pool. They get added to their corresponding transaction pool also known as mem pool. Now as the whole process begins of creating a candidate block all the nodes in the system would take transactions from their mem pool to fill up their own version of a candidate block. While filling up the candidate block with transactions all the nodes would keep 20% of the block with high paying transactions and the rest would be filled up with others. As the candidate block is created, the process of block creation/nonce solving begins. The nodes that would start from the 0th second would work with their own version of the block however when a new node(s) arrive the system would assign any of the previous working nodes as a coordinator and all the other nodes that come after it would work on that particular block (candidate block of the coordinator). More on this in coordinator and block creation section. This whole process would work parallelly, that is, as the nodes are selected for creation of the block, they would also look for new transactions, validate it and add it to their mempool. Visualization for the task of mem pool and block creation is provided in figure 3.2 and 3.3.

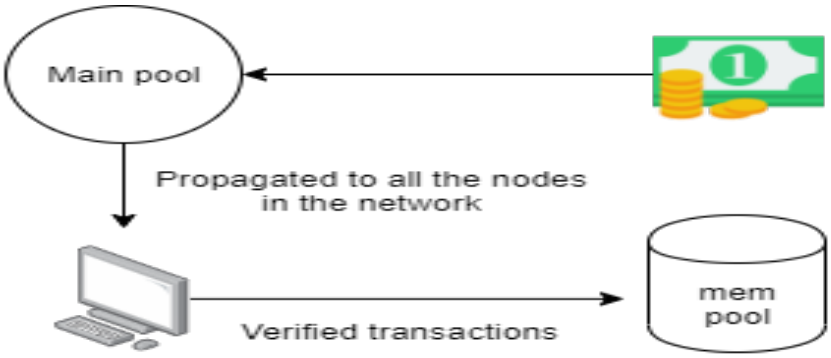

Figure 3.2: Task of Mempool

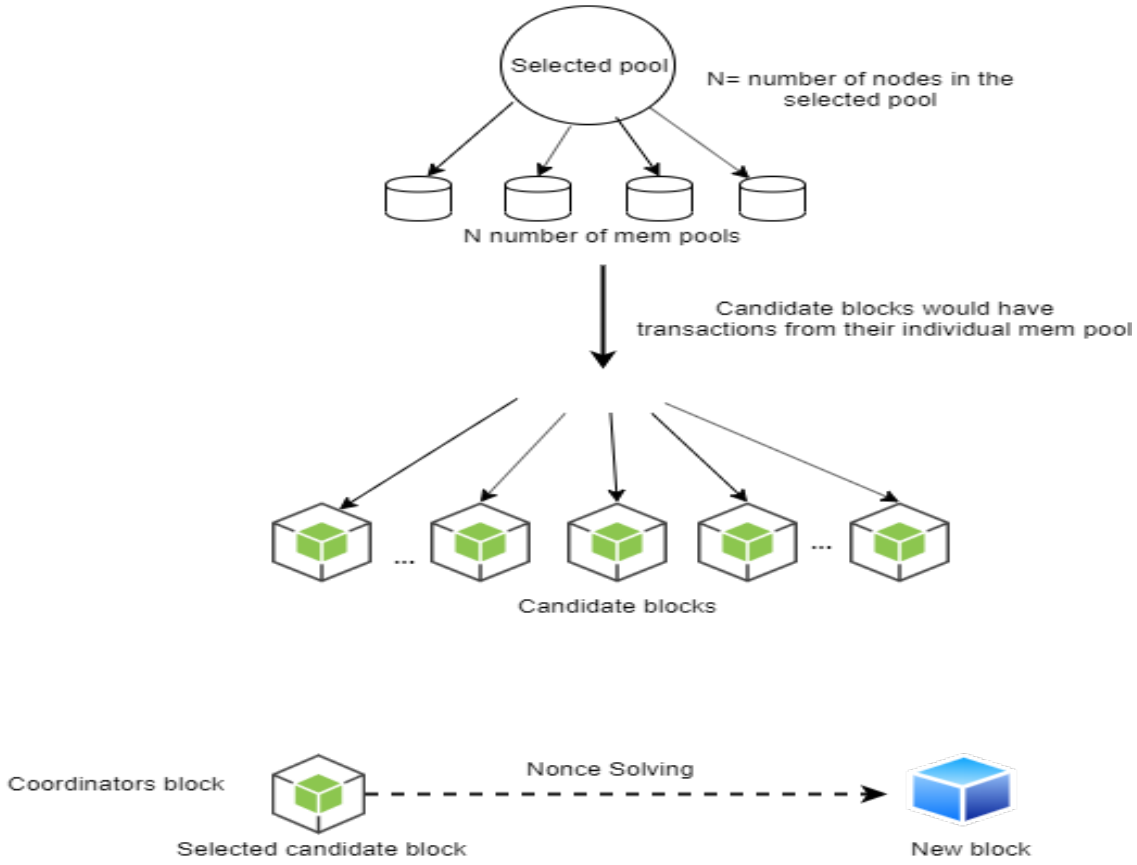

Figure 3.3: Block Creation

3.4 Proof of Segmented Work

In the previous sections, we have discussed how the registration and sub-pool creation will operate. In the last section, we observed the stake based segmentation which will leave us with two types of nodes. Let us consider,

P = Selected Pool
X = 10% Nodes with the highest Stake
(100-X) = Remaining 90% Nodes

X nodes or X+m (m = Nodes who were randomly assigned 0.0 wakeup time) will start solving the nonce together at the beginning and keep solving till any node other than the already competing nodes wake up. The remaining (100-X-m) nodes will be given a random wakeup time which will fall under a pre-defined criterion. When the next node(s) wakes up, the system will calculate the hash solved by each node during this time using the formula,

$$S = H/T, where \tag{3.5}$$

S = Hash rate
H = Number of Hash solved
T = Time Awake

The node with the highest value of S will be considered as the winner among these nodes and will compete with the recently awoken node(s) for solving the next part of the nonce. In the unlikely scenario, where multiple nodes have the same value of S, one of them will be randomly selected. This process will be repeated until the target hash is reached.

Example- let's say 3 nodes Node-1, Node-2 Node-3 have the highest stake in the pool and fall under the 10%. They will start generating hashes trying to solve the nonce from 0.0 sec. If Node-4 and Node-5 wake up at 15.0 sec. The hash rate of each node will be calculated using formula(3.5) and the winning node will be declared as the Coordinator. Suppose, Node-2 was the winning node. This node will then forward the computed hash range to the newly awakened nodes and compete with them as well. So, for the duration of 15.0 to 30.0 seconds, Node-2 will be competing alongside Node-4 and Node-5. Again, the winner node will be decided using formula (3.5) and that node will be allowed to compete in the next stage. If there is no newly awakened node then the winning node from last stage will keep trying to solve the nonce for that duration.

The Coordinator node in the system will have 4 primary jobs-

1. Forwarding the Hash range.
2. Keeping track of the winner in each stage and their generated Hash amount.
3. Calculating the division of prize among the winner nodes.
4. Adding the block

A simple visualization following the above-mentioned example of the system is given in figure 3.4.

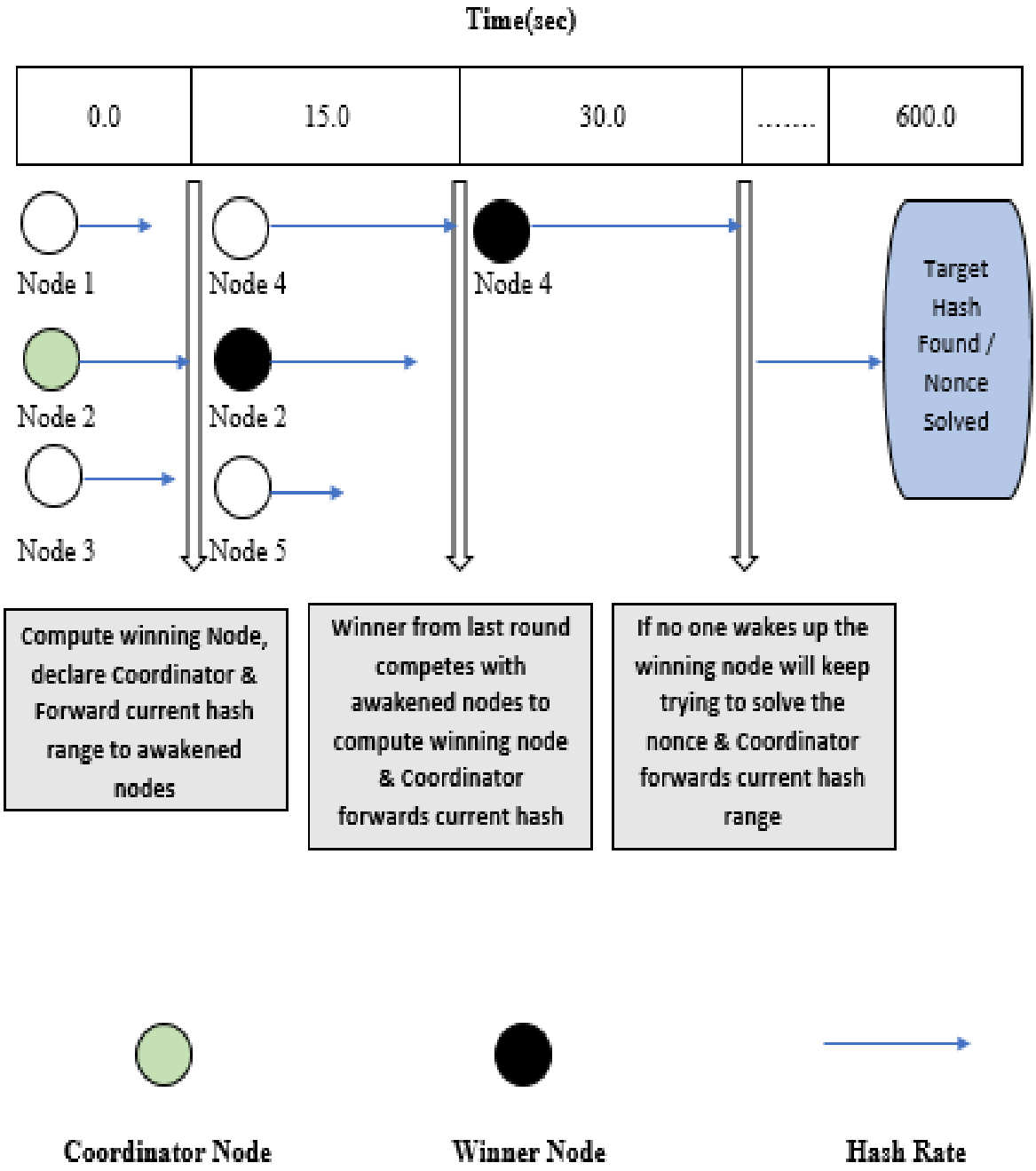

Figure 3.4: Node selection and Nonce solving

Pseudo-code for Stake and wake up time assignment:

Algorithm 3 Stake and Wake up Time Assignment:

```
1: Main pool = M_N
2: selected stake nodes H_STN =M_N × 0.10
3: Wake up time = W_T
4: procedure STAKE_WAKEUPTIME
5:     loop:
6:     while (M_N) do
7:         if (H_STN) then
8:             W_T = 0
9:         else
10:            W_T = Wake_Up_Time_Generator (0,600)
11:    end while
12: end
```

3.4.1 Coordinator selection

As we have seen in section 3.3 above, the system gives priority to the nodes having the highest stakes meaning it will check the stake of every node in the system and give the highest 10% an early start. Among the early starting nodes, there will be one winning node who will be designated the role of coordinator. The coordinator will keep track of the winners and their amount of hash solved and at the end decide on the prize distribution. After each iteration, the winning node will forward it's solved hash range to the coordinator and in turn the coordinator will relay the range to the newly awakened nodes. The coordinator will keep track of these ranges and their corresponding winner nodes. Finally, when the nonce have been solved, the last node will return the block to the coordinator and the coordinator will compute the contribution of each winning node using the following equation-

$$C = \frac{W^n}{T^n} \times 100 \tag{3.6}$$

where, T^n = Total number of hash generated or Number of iterations
W^n = Amount of hash generated by Node n

and according to their contribution allocate prize keeping 2% of the total reward as his own reward for coordinating the block. The coordinator will also add the block to the blockchain and start propagating the block within the network.

3.4.2 Random Function

The random function in our system is responsible for generating random wake up times for different nodes in the selected pool. The process involves 3 criterias;

- **The number of nodes in the selected pool**: This number represents how many nodes would be assigned random values from the sequence.
- **The difference between the closest random time:** In the worst case, the closest number between two nodes would be a minimum of 15 seconds upto 30 seconds. Which enables each node to at least contribute a good amount of time in solving the nonce.
- **The randomness range:** The random numbers would always be between 0 to 600(10 minutes) thus enabling non high stake nodes to have the opportunity to start from the beginning and also be in the situation where they wouldn't be able to contribute to the nonce solving process at all.

Pseudo-code for Random Function:

Algorithm 4 Random Function:

```
Selected Pool = S_P
procedure WAKE_UP_TIME_GENERATOR(STARTING_TIME, ENDING_TIME)
    sequence = i for in range (Starting_Time,Ending_Time, randint(15,30))
    loop:
    for ( _ in range (S_P) do
        wake up time = choice(Sequence)
        N_WT = selection
    end for
end
```

However, there would be cases where the difference between two nodes (wake up time) is more than 30 seconds. This is completely random so there is a good amount of fairity in the system.

For example if the selected pool had 20 nodes. The function would generate a sequence of random numbers maintaining the criteria of 15 to 30 seconds difference.

[0, 17, 34, 51, 68, 85, 102, 119, 136, 153, 170, 187, 204, 221, 238, 255, 272, 289, 306, 323, 340, 357, 374, 391, 408, 425, 442, 459, 476, 493, 510, 527, 544, 561, 578, 595]

As we have 20 nodes , 20 numbers W Would be selected from here and assigned to the nodes as their wake up time.

These values would assigned to the nodes as their wake up time.

3.4.3 Nonce Solving

The system will have nonce solving system similar to that of bitcoin. Nonce is an abbreviation for "number only used once" meaning it is a number or string added to a hashed block in the blockchain which meets the difficulty level restrictions. Just like bitcoin, the system will have a block difficulty which will be updated every 2

weeks based on the hash rate of the entire network. This difficulty is kept same across the entire network, meaning all the mining nodes in the system will have the same opportunity to find the target hash. This hash is between 0 bit (smallest option) to 256 bits (largest option). In our system, the waking nodes will compete to find the target hash from the beginning and participate in the trial and error process following the Proof of Work algorithm. But for each division of time there will be only one winner who will be awarded for generating the greatest number of hashes. As each iteration is effectively contributing in reaching the final target hash. The coordinator will keep track of the number of trial and errors conducted by each winning node and once the target hash is found it will distribute the earnings (Mining fee + Transaction fee) among all the winners.

Pseudo-code for Nonce Solving:

Algorithm 5 Nonce Solving:

```
Main pool = M_N
High stake nodes H_STN =M_N × 0.10
Nodes selected with randomly assigned waking time of zero = m
High stake nodes H_SN = H_STN + m
Wake up time = W_T
procedure SOLVE_NONCE
    loop:
    while (GeneratedHash > TargetHash) do
        if (New node wakes up) then
            call Selection
            P_C Forwards hash range
            P_C Forwards block information
            Resume hash generation
            if (previous node W_T == 0) then
                declared coordinator P_C
        else
            call Selection
            continue generating hash
    end while
    P_C Adds the block to the blockchain
end
procedure SELECTION
    compute and compare hash rate of nodes
    if (Highest Hash Rate) then
        don't sleep and compete with newly awoken nodes
    else
        sleep
    return node
end
```

3.4.4 Switching at Intervals

The competing nodes in the system will try to solve the nonce themselves and as each ranged interval approaches, they will check the pool for waking nodes. If waking nodes are found, they will provide the iterations conducted by each node to the coordinator and the coordinator will then declare the winner. Switching in each interval will have a small lag time where the coordinator will make decisions and forward the hash range to the newly awoken nodes.

3.4.5 Forwarding Hash Range

As nodes in the pool might be located all around the world propagating the hash range would be inefficient and time consuming. There might be a scenario where nodes are in the farthest corners of the world. So the hash range will be forwarded to the recently awoken nodes using a direct method of communication. As they are all inside the same pool communicating with each other without interruption can be ensured. As nodes wake up, the coordinator will forward the hash range to them using a one-way communication protocol.

3.4.6 Block Structure

The system will follow the segregated witness (Segwit) implemented bitcoin block structure meaning each block will contain two parts. One being the base transaction block which will only contain the inputs and outputs of the transaction and the other being the extended block which will contain witness data (signature + scripts). The reason behind using Segwit blocks from the beginning is because it solves the Transaction Malleability issue that occurred in bitcoin and allowed more transactions to be stored together in each block. By allowing more transactions inside a block the amount of transaction occurring in each second (Tx/sec) increases.

3.4.7 Adding the Block

Once the generated hash is less than or equal to the target hash only then the coordinator will add the block to the already existing blockchain. Adding the block means the hash generated by the miners are less than or equal to the hash used in the most recent block. If the target hash is set to a higher difficulty level than the capability of the nodes in the network, then the miners will take longer time to solve the nonce and block addition time will increase. Similarly working the other way around can speed up block addition (decrease block addition time). The system will maintain difficulty of the nonce in such a way that block addition time is kept around 600 seconds or 10 minutes.

3.4.8 Propagation

New transactions are propagated to all nodes and each node collects those transactions into a block. As transaction propagation is not uniform throughout the network (i.e. a node in China might get a transaction information from India earlier than a node in United States), Each node will have its own candidate block. As the nodes with the highest stakes will wake up at 0.0 second, they will immidietly start working with the incoming transactions and their own candidate block. They will take the new transactions from their memPool and validate it. Then they will put those validated transactions on their candidate block. One of the high stake nodes will be chosen as the pool coordinator. The pool coordinator will keep track of contribution, hash range and reward of other nodes and forward his candidate block after each interval. Pool coordinator will never be eliminated and there will be a comparison of contribution between the nodes each time a new node awakes. So, whenever a new node awakes it will import the candidate block of the coordinator and resume finding the target hash. When a node finds solves the nonce, it returns the block to the pool coordinator and the pool coordinator propagates the block to the network. It is essential that all nodes accept the block only if all transactions in the block are valid. Nodes express their acceptance of the block by working on creating the next block in the chain, using the hash of the accepted block as the previous hash.

New transaction broadcasts do not necessarily need to reach all nodes. As long as they reach majority of the nodes, the transactions will get into a block before long. Block broadcasts are also tolerant of dropped messages. If a node does not receive a block, it will request it when it receives the next block and realizes it missed one.

Our proposed system will have a similar broadcasting protocol to that of bitcoin. Bitcoin's P2P network is formed of miner nodes where the nodes randomly connect with each other. Transactions and blocks are transmitted over this network by the nodes, until each has received the message. For a message to be spread through the network, the transaction travel in hops. With each iteration a set of 2 nodes get the massage, and the network diffusion grows by a factor of $2\hat{n}$. The diffusion increases exponentially as the hops increase, and usually after 12–15 hops, the entire network receives the message

3.4.9 Rewards Distribution

Following the previous sections the pool might get the solved nonce after N number of hash solved. After the nonce has been solved the coordinator node will divide the (mining fee + transaction fee) among everyone based on their hash solved keeping 2% of the total earning as extra reward for working as the coordinator.

Assuming,

$$\text{N} = \text{Total hash generated till Target hash is found}$$
$$H_N = \text{Hash Generated by coordinator}$$
$$\text{M} = \text{Mining fee}$$
$$\text{T} = \text{Transaction fee}$$
$$C_C = H_N \div \text{N [Contribution of coordinator]}$$
$$N \rightarrow (M + T)$$
$$\text{So, Coordinator node will get}$$

$$((M + T) \times 0.2) + ((M + T) \times C_C) \tag{3.7}$$

If there are 3, Nodes involved till the target Hash is found and they have each solved Q, W ,R amount of hashes then,

$$Q + W + R = N \tag{3.8}$$

So, Node- 1 will be awarded,

$$C_Q \rightarrow (Q \div N) \times ((M + T) \times 0.98) \tag{3.9}$$

Node- 2 will be awarded,

$$C_W \rightarrow (W \div N) \times ((M + T) \times 0.98) \tag{3.10}$$

Node- 3 will be awarded,

$$C_R \rightarrow (R \div N) \times ((M + T) \times 0.98) \tag{3.11}$$

Pseudo-code for Rewards Distribution:

Algorithm 6 Reward Distribution

```
Total reward = R
Percentage of reward = R_P
Reward of node n = R_N
Total Hash generated = H
Hash generate by node n = H_N
procedure DISTRIBUTE_REWARD
    loop:
    while (Each winning node participating in solving nonce) do
        if (node==coordinator) then
            R_P = (H ÷ H_N) × 100
            R_N = (R × R_P) + (R × 2%)
        else
            R_P = (H ÷ H_N) × 100
            R_N = (R × R_P)
    end while
end
```

3.5 Flowchart of the proposed model

Process of our whole system is given in figure 3.5.

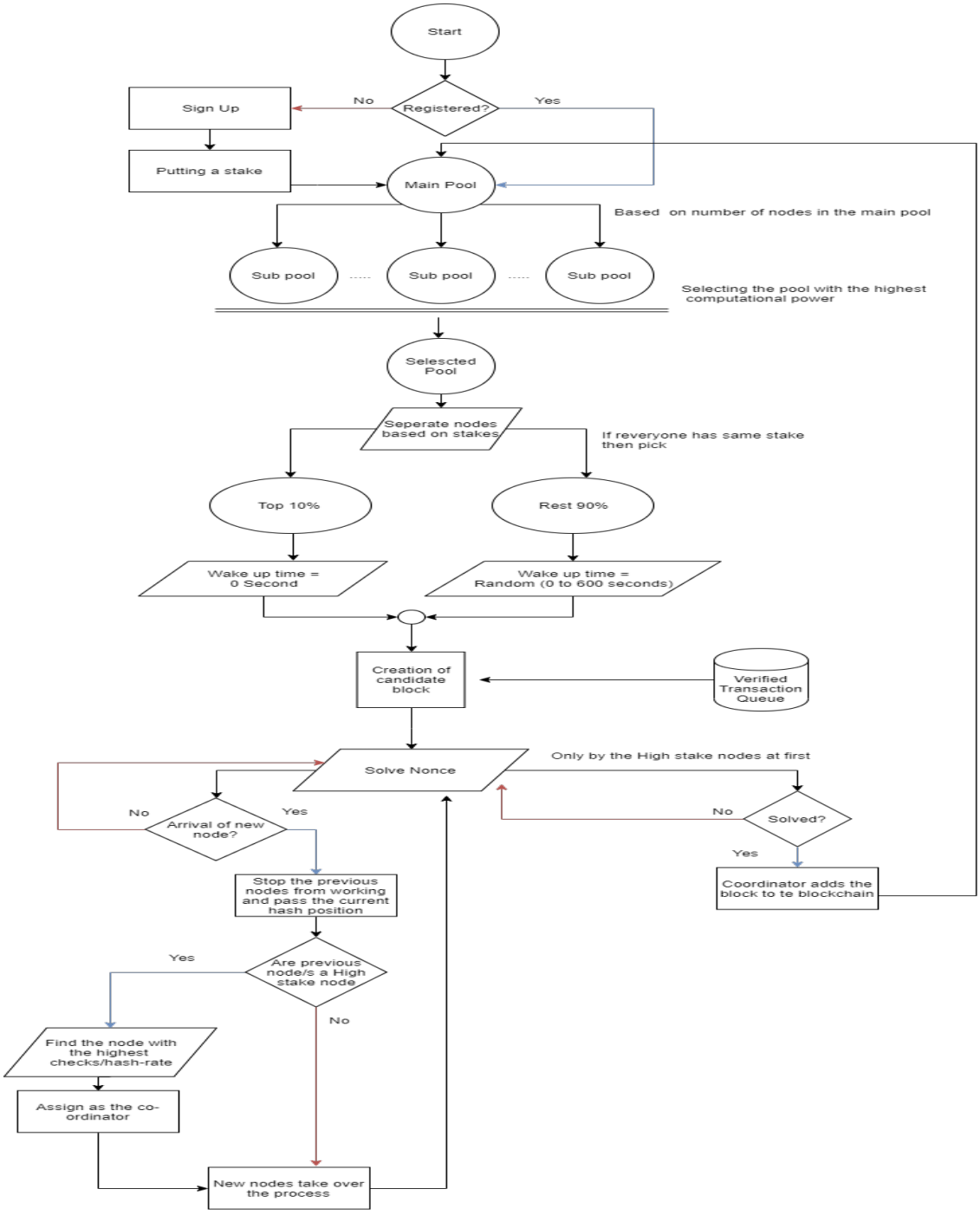

Figure 3.5: Flowchart of the proposed model

3.6 Final thoughts

Our system would be partially tackling a situation, as nodes are randomly selected and a difficulty is set based on that newly created pool so the quantum computer would not always be selected, thus stopping the domination of one node all the time, though, whenever a quantum node is selected it would be the only winner. So, our system would be partially tackling the problem of quantum computers as it would not make the currency obsolete.

Chapter 4

Comparison and results

4.1 Comparison with similiar networks

Since many such similar works have been researched previously and many crypto currencies and protocols have been introduced, the most popular crypto currencies till this date is Bitcoin and Ethereum. Hence, we tried to explain our energy efficiency of our proposed system by showing some calculative and demographic representations with comparisons.

4.1.1 Comparing our system with the Bitcoin network

In the second quarter of the calendar year 2019 (May- August), bitcoin had an average of 38,964,916 active wallet users [38] and it is estimated that there are about 100,000 to 150,000 miners in the bitcoin network [39], [40] and they have been estimated to have used about 65.7328 TWh so far. Moreover, based on a report published by International Energy Agency (IEA), bitcoin has surpassed many countries in terms of energy consumption [41] which is presented in Figure 4.1.

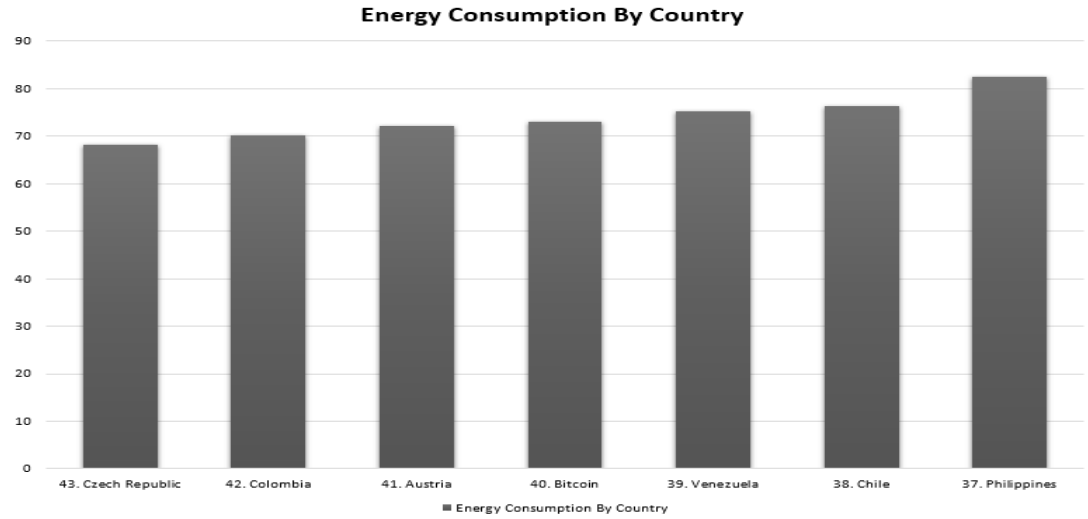

Figure 4.1: Energy consumption by country (BITCOIN)

The amount of energy waste and carbon foot print that bitcoin generates is something to be deeply concerned about. However, many cryptocurrencies are trying to lower their energy consumption via using different consensus protocols and being more energy efficient in terms of generating new coins.

Assuming that there were 150,000 miners during Q2, 2019. Our system would divide the whole network into 6 sub pools containing 25,000 nodes each. And then, the system would pick one of these sub pools. More specifically, unlike in bitcoin where all 150,000 miners would compete to solve the nonce, in our proposed system only a randomly selected portion of 25,000 nodes would compete to find a solve for one block.

To show by calculations:

According to the records, in bitcoin, 150,000 miners consumed = 65.7328 TWh

Therefore,

$$\begin{aligned} 25000 \text{ miners shall consume} &= ((65.7328 \times 25000) \div 150000) \text{ TWh} \\ &= 10.9554 \text{ TWh} \end{aligned}$$

Thus, it means that our system would be consuming **83.33%** less energy than bitcoin.

4.1.2 Comparing our system with the Ethereum network

As mentioned before, other crypto currencies are trying to solve this energy problem and one of them is Ethereum. They have comparatively better results than bitcoin in terms of energy consumptions. According to another report published by International energy agency, Ethereum ranks 103 compared to bitcoins that rank 40 in energy consumptions which is arguable better [42].

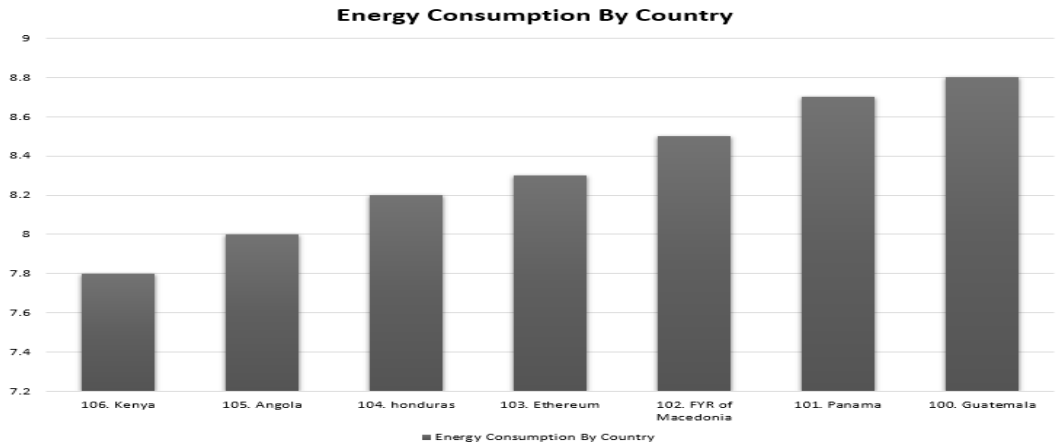

Figure 4.2: Energy consumption by country (ETHEREUM)

As of now, Ethereum has 50,744 active miners [43] and an average of 8.3456 TWh energy consumption. If Ethereum used our system, then the scenario would have been as in Figure 4.3. According to our proposed system, for 50,744 miners there would be 6 sub pools generated.

Figure 4.3: Different Computational Power of Pools

Based on the computational power of the sub pools, it chooses the one with the highest power. It is most likely that one of the 5 pools containing 10,148 nodes would be selected. However, their total power consumption would be as follows when calculated-

According to the records,

$$50744 \text{ nodes in Ethereum have a consumption of} = 8.3456 \text{ TWh}$$

therefore, 10148 nodes shall have a consumption of,

$$(8.3456 \div 50744) \times 10148 \text{ TWh} = 1.66898 \text{ TWh}$$

Hence, based on these calculations, it could be easily concluded that our system would consume 80% less power than Ethereum.

4.1.3 Comparing our proposed model with Bitcoin and Ethereum

Let us assume that each of the three networks, Bitcoin, Ethereum and FaircoinBD, the network using our proposed model, have 50,744 nodes.

Then mathematically:

According to the records, to solve the nonce for one block.

1 bitcoin node consumes 0.0004382 TWh
And, 1 ethereum node consumes 0.0001644 TWh

therefore, bitcoin network will consume = 0.0004382 TWh x 50744 = 22.24 TWh
and, Ethereum network will consume = 0.0001644 TWh x 50744 = 8.34 TWh

Now, if we assume that one node in the FaircoinBD network consumes the same amount of energy as in bitcoin, then for 50744 nodes, only 10148 nodes would be

mining in FaircoinBD. Thus, to solve the nonce for one block in the proposed network will consume 0.0004382 TWh X 10148 = 4.447 TWh, which is

$\frac{22.24-4.447}{22.24} * 100 = 80.00\%$ more efficient than Bitcoin network and,

$\frac{8.34-4.447}{8.34} * 100 = 46.68\%$ more efficient than Ethereum network.

This is illustrated in Figure 4.4.

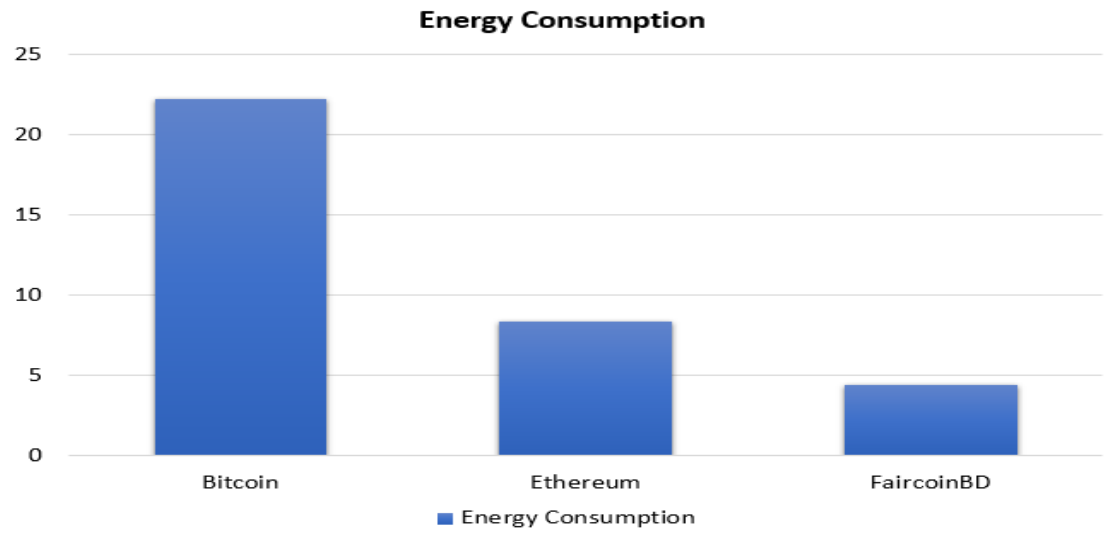

Figure 4.4: Comparison of Energy Consumption by Bitcoin, Ethereum and FairCoin if each node of FairCoin consumes same energy as in Bitcoin.

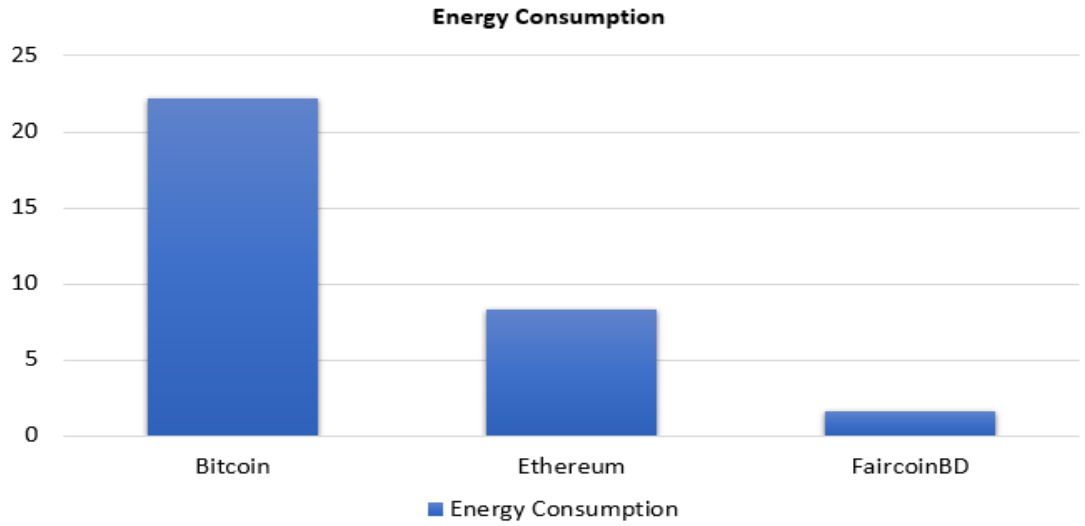

Figure 4.5: Comparison of Energy Consumption by Bitcoin, Ethereum and FaircoinBD if each node of FaircoinBD consumes same energy as in Ethereum.

And, if we assume that one node in the FaircoinBD network consumes the same amount of energy as in ethereum, then for 50744 nodes, again only 10148 nodes would be mining in FaircoinBD. Thus, to solve the nonce for one block in the FaircoinBD network will consume 0.0001644 TWh X 10148 = 1.668 TWh which is

$\frac{22.24-1.1688}{22.24} * 100 = 92.41\%$ more efficient than Bitcoin network and,

$\frac{8.34-1.688}{8.34} * 100 = 79.76\%$ more efficient than Ethereum network.

This is illustrated in Figure 4.5.

Chapter 5

Conclusion

5.1 Accomplishments

5.1.1 Provides chance to participate for low configuration computers

As the proposed system will have random pool creation containing all sorts of nodes, low and medium configured computer owning miners will also get a chance to be a part of the mining process. They can even put high stakes and become the coordinator node. The selected subpool will contain different types of nodes with different computational capacity. Even though the system will choose the highest hash rate generating node as the winner at each interval, there is still the possibility of a low capacity containing node to contribute and earn FaircoinBD.

5.1.2 Possibility of Fork is minimal

In FaircoinBD, the selected pool will be participating in the nonce solving process. Even though all nodes in the network are making candidate blocks, only the coordinator's candidate block is being added to the block. As for each block, only one pool is selected and only one verified candidate block is added to the network. There is little to no possibility that two chains are created. In Bitcoin, forks often occur and Bitcoin Cash is a result of that, but in our system the possibility of such forks is non existent.

5.1.3 Energy Consumption is minimal

Comparing to other cryptocurrencies using Proof of Work consensus algorithm for their nonce solving process, such as Bitcoin and Ethereum, FaircoinBD will have a very low Energy Consumption rate. In FaircoinBD, the nonce solving process is contained within the selected subpool. This will tackle the argument of cryptocurrencies in general being a power drain. FaircoinBD's efficiency allows it be mined in economically weaker countries or countries with high electricity cost.

5.1.4 Carbon Footprint is low

Carbon Footprint refers to the effect of a technology or event on earth. It is estimated that bitcoin has a carbon footprint between 22 to 22.9 mega tonnes per year [44]. In a world, where climate change is a burning issue that concerns all its people, low carbon footprint is a blessing. As our system has low energy and power consumption, it will leave a carbon footprint much lower than the traditional cryptocurrencies.

5.2 Drawbacks

5.2.1 Quantum Supremacy

One of the major concerns about bitcoin right now comes from the development of Quantum Computers. Google has recently declared quantum supremacy with their introduction of the Sycamore quantum computer and since then bitcoin has taken a hit in its price. The price of bitcoin dropped from nearly $8000 to $7000 [45] [46]. This is because people are fearing that this could eventually mean the end of bitcoin, as quantum computers can easily hack millions of dollars. The transaction in the bitcoin are encrypted with RSA, however, quantum computers can easily break this encryption and get all the information. According to Microsoft research director Dr. Krysta Svore, "The RSA-2048 challenge problem would take 1 billion years with a classical computer. A quantum computer could do it in 100 seconds." [47].

From the previous discussion, we know that the difficulty of bitcoin changes every 2016 blocks or 2 weeks. However, as quantum computers have started to become a reality, if it appears in the bitcoin network, it could solve the nonces within seconds, thus making that node earn a staggering 25,200 bitcoins which as of now, means $179,020,800 after all the 2016 blocks are completed and the difficulty of the system changes and adapts to the computational power of the network. As the quantum computer would have a lot of computational power, the system would generate a puzzle that only the quantum computer would be able to solve, thus, eliminating all sorts of competition. However, the bitcoin network yet is not capable to produce a difficulty of this level [48]. As our system has a similar nonce solving process to that of bitcoin, it is also at risk of facing the high computational power of a quantum computer.

5.2.2 Time consumed at each interval

As our proposed system has an interval time at which the already competing nodes will stop generating hashes and compute their current hash amount, using this hash amount and their time awake, the winner node will be selected. At this time the coordinator node will also forward it's candidate block and the new hash range. Even though in a high configured environment this process takes very little time, it is still taking time where the nonce solving process is halted.

5.2.3 Bandwidth consumed by the coordinator

In our proposed system, even though each node in the system will create its own candidate block, only the coordinator's block will be worked on. So, at each interval, the coordinator will have to forward it's candidate block to the waking nodes. Even though the base block will have the size of 1MB only, it will still add up as the process goes on.

5.3 Future Work

Even though our system has tackled some of the most argued topics of bitcoin, it still has a lot of places to improve. As mentioned before, there are a few things even other successful crypto currencies aren't capable of solving and are coming together as a community to tackle the problems like quantum computers. This is one of the places we can improve.

Furthermore, we made our system on a theoretical basis and proved the efficiency of our system through mathematics, however, we need to implement the whole concept into a real life situation through making our coin and there isn't any doubt that whenever we are implementing the system we would face problems or find ways to make the system even better, thus, in the future we would be focusing more on implementation.

Moreover, as of August 2019, bitcoin has updated their system to implement lighting network and they have been updating bitcoin for quite a while now. A massive crypto currency like bitcoin is updating itself with new technologies to make transactions faster and more secure. Similarly, we would also try to update our system in terms of making the propagation of block, transaction and block information with the selected pool much faster so that time and bandwidth both can be saved.

Finally, we would implement the concept of coinage to reduce the possibility of a single node dominating the system. This would give a limit to how many times a node can be a coordinator so that they won't be able to hog the rewards all the time thus increasing the chances of others and in the end making our system more fair.

5.4 Conclusion

We have discussed several possibilities of cryptocurrency, as well as, the incredible implementations of blockchain and cryptography that has made all of this possible. The era of cryptocurrency is just beginning and every day new concepts, ideas and research topics are being introduced. In our paper, we have proposed several ideas that might be implemented as a whole or be used only as a subpart of a system. The paper has shown how this implementation will prove beneficial by showing fairity in reward distribution and low energy consumption. It will also be able to solve the multi-chain problem by essentially decreasing the chances of fork. We have

also acknowledged our limitations and proposed possible solutions for them. The research on blockchain and cryptocurrency is still at a very early stage but we believe that, in time the whole world will make transactions without needing a trusted third party that will go beyond borders.

Bibliography

[1] CoinMarketCap, *All cryptocurrencies*, https://coinmarketcap.com/all/views/all/, [Accessed: 08-Nov-2019], Nov. 2019.

[2] E. Macauley, *What are the most popular cryptocurrencies?*, https://sba.thehartford.com/finance/cryptocurrency/what-are-the-most-popular-cryptocurrencies/, [Accessed: 08-Nov-2019], Aug. 2019.

[3] N. Chong and M. Young, *What are the most popular cryptocurrencies?*, https://www.newsbtc.com/2019/09/04/twitter-ceo-bitcoins-longevity-and-resilience-make-it-prime-currency-for-the-internet-candidate/., [Accessed: 08-Nov-2019], Sep. 2019.

[4] A. Lucian, *Analyst warns against a bullish bitcoin bias after china surge*, https://beincrypto.com/analyst-warns-against-a-bullish-bitcoin-bias-after-china-surge/, [Accessed: 08-Nov-2019], Oct. 2019.

[5] C. Rose, "The evolution of digital currencies: Bitcoin, a cryptocurrency causing a monetary revolution", *International Business & Economics Research Journal (IBER)*, vol. 14, no. 4, pp. 617–622, 2015.

[6] C. Metz, *Bitcoin in japan*, https://www.wired.com/2013/10/bitcoin-in-japan/., [Accessed: 16-Nov-2019], 2013.

[7] J. FRANKENFIELD, *Cryptocurrency*, https://www.wired.com/2013/10/bitcoin-in-japan/., [Accessed: 17-December-2019], 2019.

[8] bitcoin.it, *Secp256k1*, https://en.bitcoin.it/wiki/Secp256k1, [Accessed: 18-September-2019], 2019.

[9] A. M. Antonopoulos, *Mastering Bitcoin: Unlocking Digital Crypto-Currencies*, 1st. O'Reilly Media, Inc., 2014, ISBN: 1449374042, 9781449374044.

[10] Coinbase, *Coinbase commerce, "commerce.coinbase.com/docs*, www.coinbase.com, [Accessed: 18-September-2019], 2018.

[11] T. Be'ery, *A brief intro to bitcoin schnorr multi-signatures*, =https://hackernoon.com/a-brief-intro-to-bitcoin-schnorr-multi-signatures-b9ef052374c5, Jul. 2018.

[12] G. Maxwell, A. Poelstra, Y. Seurin, and P. Wuille, "Simple schnorr multi-signatures with applications to bitcoin", *Designs, Codes and Cryptography*, pp. 1–26, 2018.

[13] H. und Paola Mayer, "Ecdsa security in bitcoin and ethereum : A research survey", 2016.

[14] BTC.com, *Bitcoin block explorer - btc.com*, https://btc.com/, [Accessed: 08-Nov-2019], Nov. 2019.

[15] A. M. Antonopoulos, *Mastering bitcoin: unlocking digital crypto-currencies*, 1st ed., ser. 10. The address: O'Reilly Media, Inc, Dec. 2010, vol. 2, An optional note, ISBN: 1491902647.

[16] CryptoCompare, *What is bitcoin transaction locktime?*, https://www.cryptocompare.com/coins/guides/what-is-bitcoin-transaction-locktime/, [Accessed: 15-Nov-2019], Feb. 2015.

[17] B. T. Fees, *Bitcoin transaction fees*, https://bitcoinfees.info/, [Accessed: 15-Nov-2019].

[18] B.Asolo, *Transaction malleability explained*, https://www.mycryptopedia.com/transaction-malleability-explained/, [Accessed: 15-Nov-2019], Oct. 2018.

[19] GitHub, *Bitcoinbook/bitcoinbook*, www.coinbase.com, [Accessed: 17-November-2019], 2019.

[20] B. Academy, *What is a blockchain consensus algorithm?*, https://www.binance.vision/blockchain/what-is-a-blockchain-consensus-algorithm, [Accessed: 16-Nov-2019], 2019.

[21] GeeksforGeeks, *Consensus algorithms in blockchain*, https://www.geeksforgeeks.org/consensus-algorithms-in-blockchain/, [Accessed: 16-Nov-2019], 2019.

[22] Investopdia, *Target hash*, https://www.investopedia.com/terms/t/target-hash.asp, [Accessed: 16-Nov-2019], 2019.

[23] GeeksforGeeks, *Proof of work (pow) consensus*, https://www.geeksforgeeks.org/proof-of-work-pow-consensus/, [Accessed: 16-Nov-2019], 2019.

[24] B. Academy, *Proof of stake explained*, https://www.binance.vision/blockchain/proof-of-stake-explained, [Accessed: 10-Nov-2019], 2019.

[25] H. Anwar, *Algorithms: The root of the blocconsensuskchain technology*, https://101blockchains.com/consensus-algorithms-blockchain/, [Accessed: 16-Nov-2019], May 2019.

[26] investopedia, *Proof of elapsed time (cryptocurrency)",* https://www.investopedia.com/terms/p/proof-elapsed-time-cryptocurrency.asp., [Accessed: 16-Nov-2019], 2019.

[27] Blockonomi, *What is proof of elapsed time consensus? (poet) complete beginner's guide*, https://blockonomi.com/proof-of-elapsed-time-consensus/, [Accessed: 16-Nov-2019], 2019.

[28] T. Xue, Y. Yuan, Z. Ahmed, K. Moniz, G. Cao, and C. Wang, "Proof of contribution: A modification of proof of work to increase mining efficiency", in *2018 IEEE 42nd Annual Computer Software and Applications Conference (COMPSAC)*, IEEE, vol. 1, 2018, pp. 636–644.

[29] R. NAKAHARA and H. INABA, "Proposal of fair proof-of-work system based on rating of user's computing power", in *2018 IEEE 7th Global Conference on Consumer Electronics (GCCE)*, Oct. 2018, pp. 746–748. DOI: 10.1109/GCCE.2018.8574499.

[30] Y. Liu, X. Chen, L. Zhang, C. Tang, and H. Kang, "An intelligent strategy to gain profit for bitcoin mining pools", in *2017 10th International Symposium on Computational Intelligence and Design (ISCID)*, vol. 2, Dec. 2017, pp. 427–430. DOI: 10.1109/ISCID.2017.184.

[31] investopedia, *Stratum mining protocol*, https://en.bitcoin.it/wiki/Stratummining\protocol, [Accessed: 25-Nov-2019], 2017.

[32] B. B. F. Pontiveros, R. Norvill, and R. State, "Monitoring the transaction selection policy of bitcoin mining pools", in *NOMS 2018 - 2018 IEEE/IFIP Network Operations and Management Symposium*, Apr. 2018, pp. 1–6. DOI: 10.1109/NOMS.2018.8406328.

[33] M. Rosenfeld, *Analysis of bitcoin pooled mining reward systems*, 2011. arXiv: 1112.4980 [cs.DC].

[34] R. Qin, Y. Yuan, and F. Wang, "Research on the selection strategies of blockchain mining pools", *IEEE Transactions on Computational Social Systems*, vol. 5, no. 3, pp. 748–757, Sep. 2018, ISSN: 2373-7476. DOI: 10.1109/TCSS.2018.2861423.

[35] M. Beedham, *All you need to know about bitcoin network nodes*, https://thenextweb.com/hardfork/2019/03/01/bitcoin-blockchain-nodes-network/, [Accessed: 17-November-2019], 2019.

[36] Unocoin, *Bitcoin miners vs bitcoin nodes*, https://blog.unocoin.com/bitcoin-miners-vs-bitcoin-nodes-6a4d35be9712, [Accessed: 15-November-2019], 2018.

[37] R. Mitra, *What are proof of stake coins: Ultimate guide - blockgeeks*, https://blockgeeks.com/guides/what-are-proof-of-stake-coins-ultimate-guide-blockgeeks/, [Accessed: 15-November-2019], 2019.

[38] blockchain.com, *Blockchain wallet users*, https://www.blockchain.com/en/charts/my-wallet-n-users?timespan=1year, [Accessed: 15-November-2019], 2017.

[39] S. Bose, *How many bitcoin miners are there*, https://www.btcwires.com/round-the-block/how-many-bitcoin-miners-are-there/, [Accessed: 12-November-2019], 2019.

[40] E. D. G. Weinberg, *How many bitcoin miners are out there*, https://www.quora.com/How-many-bitcoin-miners-are-out-there, [Accessed: 12-November-2019], 2019.

[41] Digiconomist, *Bitcoin energy consumption index*, https://digiconomist.net/bitcoin-energy-consumption, [Accessed: 12-November-2019], 2017.

[42] Digiconomist1, *Ethereum energy consumption index (beta)*, https://digiconomist.net/ethereum-energy-consumption, [Accessed: 12-November-2019], 2017.

[43] Bitfly, *Ethereum energy consumption index (beta)*, https://ethermine.org/, [Accessed: 12-November-2019].

[44] J. Bhosale, *Bitcoin use causing huge co2 emissions: Study*, https://economictimes.indiatimes.com/news/science/astronomers-use-the-upgraded-gmrt-to-measure-the-gas-mass-of-galaxies-in-the-distant-universe/articleshow/72185368.cms, [Accessed: 12-Nov-2019], Nov. 2019.

[45] Y. ROYER, *Google lays claims to quantum supremacy, sending bitcoin tumbling*, https://www.france24.com/en/business/20191024-google-lays-claims-to-quantum-supremacy-sending-bitcoin-tumbling, [Accessed: 15-November-2019], 2019.

[46] J. Shieber, *Bitcoin and cryptocurrencies had a very bad day*, https://www.cryptoglobe.com/latest/2019/11/could-google-s-qauntum-computer-mine-3-million-bitcoin-in-2-seconds/, [Accessed: 15-November-2019], 2019.

[47] A. S. Agapiev, *Bitcoin just passed its biggest test to date*, https://medium.com/datadriveninvestor/bitcoin-just-passed-its-biggest-test-to-date-eb308a8a5d82, [Accessed: 15-November-2019], 2018.

[48] W. Heasman, *Could google's quantum computer mine 3 million bitcoin in 2 seconds*, https://www.cryptoglobe.com/latest/2019/11/could-google-s-qauntum-computer-mine-3-million-bitcoin-in-2-seconds/, [Accessed: 15-November-2019], 2019.