Analysis of Blockchain consensus mechanisms

Proof-of-Work vs Proof-of-Stake

Subject/Department: Faculty of Science.
Master's thesis

Author(s):
Saba Saif

Supervisor(s):
Professor Ion Petre

12.09.2022
Turku

Master's thesis

Subject: Master of Science
Author(s): Saba Saif
Title: Analysis of blockchain consensus mechanisms
Supervisor(s): Professor Ion Petre
Number of pages: 50 pages
Date: 12.09.2022

The objective of this thesis is to understand and evaluate the two popular consensus mechanisms of blockchain: Proof-of-Work (PoW) and Proof-of-Stake (PoS), especially in terms of their cost effectiveness. This study attempts to answer one significant research question: "Researchers assume that blockchain cannot takeover computer networks, as it requires excessive computation power. If blockchain moved to a Proof-of-Stake (PoS) consensus algorithm would takeovers remain equally difficult?"

The thesis uses qualitative desk research approach by utilizing the existing research papers and published reports related to the topic. It attempts to draw comparison between both consensus algorithms and extracts reasonable conclusions based on the simulation experiment results. The three main comparison points discussed among the consensus protocols are energy consumption, decentralization, and security of blockchain.

This study concludes that Proof-of-Stake (PoS) consumes less energy than the Proof-of-Work (PoW) and also shows better results in providing decentralization and security as compared to Proof-of-Work (PoW). Hence, takeovers are easier with PoS over PoW, but PoS still has room for improvement to reduce the required energy resources and further research studies are needed to analyse it.

Key words: Blockchain, Consensus Mechanism, Proof-of-Work, Proof-of-Stake, Energy Consumption, Cost Efficiency.

Table of Contents

Table of Figures

Table of Tables

1 Introduction

1.1 Background and Motivation

What is worth more to us, money, or security? It is the biggest dilemma of this modern world. According to a research survey conducted at University of Cambridge, Bitcoin uses more electricity yearly i.e., 121.36 terawatt hours/year than the whole Netherlands (108.8 TWh) and Argentina (121 TWh) (Criddle, 2021). Bitcoin is one of the utmost widespread crypto currencies based on Distributed Ledger Technology (DLT), commonly known as Blockchain Technology. Furthermore, bitcoin employs Proof-of-Work (PoW) as consensus algorithm through which all participants/ nodes of blockchain reach to the common agreement of blockchains' state. Huge amount of electricity consumption by bitcoin is also due to PoW mechanism but in return it provides secure means of record keeping. According to consensus, 0.5% people on earth is using blockchain, means applicability of blockchain is quite less as compared to it should be since it is an expensive solution to our problems. Thus, a detailed investigation is needed to understand the fundamental principles of blockchain technology and its underlying consensus algorithm to shift focus towards efficient ways of implementing. This approach will help to save environment by highlighting the ways of reducing the electricity consumption.

This research is based on the core differences between the two consensus algorithms Proof-of-Work (PoW) and Proof-of-Stake (PoS), both are practically used in the blockchain technology and have the capability to change the financial and other record keeping systems, with various practical implementations. Hence, the research to find a cost-effective solution which can overtake technological systems is equally important to address the problem of infeasibility of blockchain.

1.2 Related work and research contribution

In basic terms, blockchain is a distributed ledger which works as a record keeping system or in other words, it is a chain of data storage blocks, and every block is linked with the previous block cryptographically by storing its hash, as shown in Figure 1.

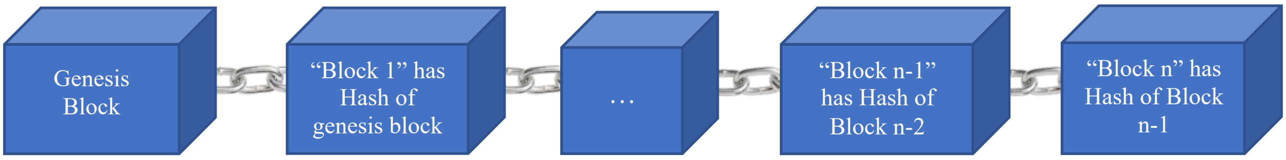

Genesis Block
"Block 1" has Hash of genesis block
…
"Block n-1" has Hash of Block n-2
"Block n" has Hash of Block n-1

Figure 1: A basic "blockchain" (cryptographically linked n+1 blocks).

The topics of this thesis are the basic concepts which are already under discussion in the past literature works such as blockchain, consensus algorithms, security of blockchain, blockchain's cryptography (hash functions, digital signatures, time-stamping techniques) back in 1990 by Haber and Stornetta (Haber & Stornetta, 1990). However, this study is providing analysis of blockchain consensus algorithm on a larger scope. This thesis attempts to address one significant research question which is, researchers assume that blockchain cannot takeover computer networks, as it requires excessive computation power. If blockchain moved to a Proof-of-Stake (PoS) consensus algorithm would takeovers remain equally difficult? The study focuses on public blockchain systems which are implemented on Proof-of-Work (PoW) and Proof-of-Stake (PoS) algorithms and their implications.

For this study, Proof-of-Work (PoW) and Proof-of-Stake (PoS) are studied with a pragmatic desk research approach which focuses to answer the under-discussion research question with best workable solution, as the subject is distinct and relatively young. They are picked as consensus algorithms due to their major divergent implementations regarding transaction verification of a new block into blockchain. This enabled obtaining an in-depth understanding of consensus mechanisms and their impact on blockchain as well as the justification behind their choices and feasibility of their cost-effectiveness.

This analysis provides holistic view of both popular consensus algorithms in blockchain technology, and thus amalgamated research that can be utilized to grasp the firmer knowledge of blockchain's main consensus protocols. Hence, the audience will be able to positively influence systems of blockchain technology and participate in their cost performance analysis. This study targets to provide and evaluate the standards used in the consensus mechanisms, essentially to consider the cost-efficiency of blockchain technology which in return can help in blockchain's scalability.

1.3 Structure

There are six main chapters of this thesis. In chapter one, research motivation and contribution's summary are provided. In the second chapter, the origin of blockchain technology, along with the brief overview of the blockchain structures and basic concepts which are important to understand the working of blockchain consensus algorithm. They stipulated a concrete fundamental understanding which is necessary to grasp further views. Likewise, a concise overview of the former blockchain technology related literature works concerning was stipulated in second chapter's later sections and aided as a foreword to the key blockchain subtopics. In third chapter, a brief justification of the methods selected for this study is provided.

In fourth chapter of the thesis, a preliminary introduction, innerworkings, properties, governing algorithm, block generation scheme, advantages, disadvantages, and applicability of both consensus algorithms are presented. Similarly, a detailed comparison of Proof-of-Work and Proof-of-Stake is given in the fifth chapter, which form the core of this thesis and key points which play a huge role in the cost-effectiveness and reliability of consensus mechanism were explained. Both consensus mechanisms were compared to a larger scope and the basic purpose of the fifth chapter is to draw reasonable conclusions by keeping in mind the statistics and results from realistic and simulation studies, which could then be generalized for other blockchain based systems while choosing the consensus algorithm. Thus, this study answers the question whether taking over becomes possible with Proof-of-Stake (PoS) or not.

2 Theoretics of Blockchain

In this section, the overview, and basic understanding of blockchain concepts will be discussed which is required to lay the foundations of our core topics and to examine them in detail later in this study. The knowledge of blockchain structure, innerworkings and cryptography is a pre-requisite to grasp the complexity of blockchain's functions.

2.1 Origin

According to Stuart Haber and W. Scott Stornetta, the concept of a secure cryptographic chain of blocks was introduced (Haber & Stornetta, 1990). After eight years, Nick Szabo; a computer scientist worked on "bit gold-decentralized digital currency" in 1998 (Szabo, 1998). Then in the year 2000, theory and implementation ideas of cryptographic blocks of chain were written by Stefan Konst (Konst, 2000). Later on, after eight years, in 2008, on the model of blockchain a white paper was published by Satoshi Nakamoto (Nakamoto, 2008). Then in 2009, he implemented blockchain for his cryptocurrency, known as "bitcoin" (Nakamoto, 2009). Further on, during the year 2014, finances were separated from the blockchain technology, and its applications were introduced in the other industries beyond cryptocurrency (Ulieru, 2016).

2.2 Definition

According to Niranjanamurthy, Nithya and Jagannatha, blockchain is defined as a data structure that stores all the transactions online on a peer-to-peer computer network in a digitally distributed ledger (Niranjanamurthy *et al.*, 2019). It gives the users freedom to create and validate these online transactions without the need of central authority. Thus, blockchain creates a trust-free environment. Blockchain contains the following key properties to safeguard the confidentiality, integrity, and availability of secure system:

- **Immutability:** Blockchain offers this property by ensuring that no record can be deleted, added, or updated after creation in the blockchain's database unless 51% of the nodes agree on it. Public blockchain transactions are stored on the distributed nodes, that makes the tampering of blocks difficult. Therefore, all subsequent blocks need to be changed even any slightest of change will happen in the block (Zheng *et al.*, 2018).
- **Anonymity:** All the transactions in blockchain are stored anonymously without the sender's name and validation only requires the address of sender in the blockchain. Blockchain also gives the user ability to generate multiple addresses and they can interact

with blockchain by the produced addresses. But blockchain cannot offer perfect privacy as the public key of transactions is open to public and can disclose user's personal information when linked for example to IP address (Zheng *et al.*, 2018).

- **Transparency:** Blockchain is an open-source platform, everyone can contribute and verify the blocks publicly by the help of timestamp that each transaction has on distributed network of blockchain (Zheng *et al.*, 2018). Each node can participate in updating process of blockchain's data which makes it transparent. Hence, blockchain has the capability to provide a single true aligned copy to the whole network nodes.
- **Decentralization:** Conventionally, there is always a central authority who is responsible for the ingoing and outgoing transactions within the system for example central bank. All the load has been put on these central servers which results into performance and cost issues. Differently, blockchain gives platform for the transaction authentication within the two peers without involving any central authority rather authority is distributed among multiple nodes. In this way, blockchain can tackle the challenges of performance and cost bottlenecks that can occur at central server (Zheng *et al.*, 2018).
- **Autonomous:** As mentioned, blockchain creates a trustless environment. In such a distributed environment, some protocols are needed that can ensure consistency (Zheng *et al.*, 2018) and make the process autonomous. Thus, consensus algorithms in blockchain like Proof-of-Work (PoW) or Proof-of-Stake (PoS) makes blockchain autonomous by making transference, updating or alteration of data processes safe without relying on any trusted party. These consensus mechanisms are the source of validating the transactions entering the blockchain network (more on consensuses mechanism in chapter 4).

2.3 Structure

Blockchain is defined as the chain of decentralized and distributed blocks linked together with a cryptographic mathematical function. Generally, a block reference exists to link with the previous block which is used as a verification means of a new block, that it is not from an attacker. This tight referencing of each block to other between the blocks makes blockchain immutable.

For instance, a group of students working on a same assignment that is stored on the blockchain, each page added is one block, and a mathematical function is linking all the blocks or pages. Whenever a new page needs to be added to assignment one student solves a puzzle. If he or she is successful in solving the puzzle that new page is broadcasted to the chain and will be linked to existing pages.

When all previous blocks in the particular chain are broadcasted as well as verified then that chain would be considered as authentic main chain.

Monrat *et al.* described blockchain as a sequence of blocks that contains all transactions information (Monrat *et al.*, 2019) and according to Malik *et al.*, every block consists of the reference of preceding block, transactions data as Merkle tree root hash, and timestamp (Malik *et al.*, 2019). In few blockchains, like Ethereum, hash of the next linked block is also included in the block header. A block includes a header and the body, as shown in the Figure 2. The first block is usually, termed as the genesis block and creates a Merkle tree root hash of the set of transactions it has according to Merkle tree structure. That hash is included in the genesis block and also passed to the subsequent block.

Genesis Block
-header
-body
Block 01 …
-header
-body
Block n
-header
-body

Figure 2: A basic layout of "blockchain".

A complete copy of blockchain and its transactions are provided to the new use whenever he or she enters the network of blockchain for the first time. These transactions include all the verified transactions with the respective blocks. It means, these blocks then get copied to the user's personal machine and there he or she can validate them with the help of Merkle tree root (MTR) hash and the header hash of previous block.

Usually, the block has following components either in the block header or in the header body, also shown in Figure 3.

- Block number
- Block version
- Current block hash value
- Previous block hash
- Timestamp
- Nonce
- nBits
- Merkle tree root hash
- Transactions set

Four components i.e., timestamp, previous block header hash, Merkle tree root hash and nonce are present at least in every block header.

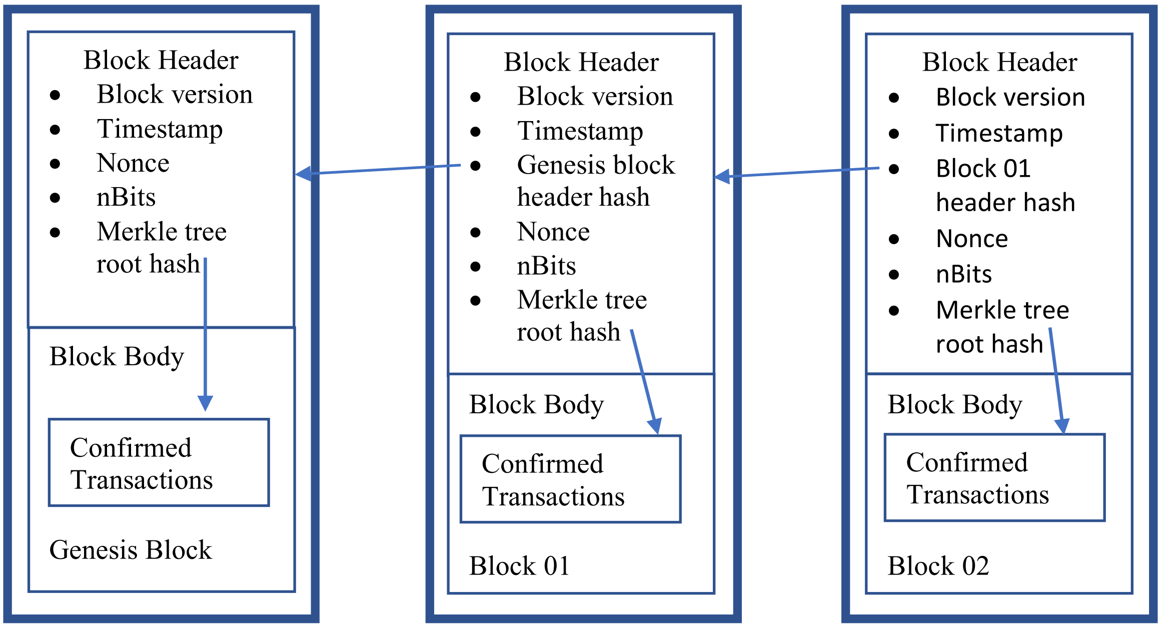


Figure 3: Structure of blockchain "Block".

A block header contains a version number to identify the validation rules implemented on it, Merkle tree root (MTR) hash which is the hash of all the transactions present in the block, timestamp specifies the current time in UTC as seconds, nonce which is a four bytes field generally initialized with 0 and incremented with the progression of blocks, parent block hash (256-bit) or previous block hash and nBits is used in mining the block, it gives the targeted threshold to meet for the validation of a block (Niranjanamurthy *et al.*, 2019). Further, a block includes transaction number and all the transactions.

As stated previously, block header includes the Merkle tree root hash, it is the combined summary of all verified transactions merged into one hash inside the block as displayed in the Figure 4. It applies the Merkle-Damgård compression function to join all the transactions hashes into one (Szydlo, 2004). This means Merkle tree root hash is part of the current block header, forms the basis of the previous block in chain. Furthermore, this block header is hashed into a single hash value and used in the next block in chain. Most importantly, all the contents of block are encrypted into one hash value. Therefore, if any of the block's transaction is tempered by illicit means, Merkle tree root hash will automatically invalidate the following block header. Hence, as we mentioned earlier this referencing within blocks ensures the immutability of blockchain.

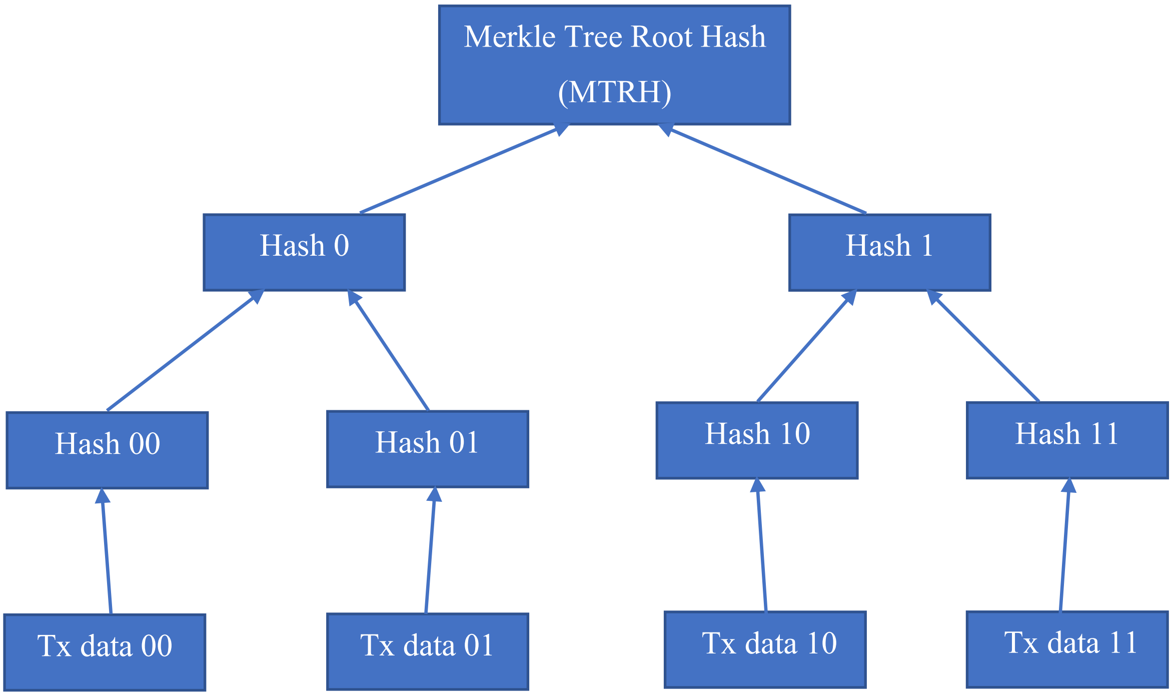


Figure 4: An example of Merkle tree.

2.4 Blockchain's architecture

The digital ledger technology (DLT) or blockchain comprises of different subjects such as computer networks, math, cryptographic structures etc. The architecture of blockchain has multiple layers (Lu, 2018), these layers are responsible for generating, validating, and storing information/data.

- **Application layer:** This layer includes all the services and applications for example blockchain based applications in healthcare etc.
- **Service layer:** Blockchain uses SaaS (Software as a Service). Some of the popular blockchain services are Ethereum and Hyperledger.
- **Contract layer:** It comes before consensus layer, network, and data layer and comprises of smart contracts which develops the basic strategy or logic of blockchain's core, implemented by adaptable coding. Also, they bridge the upper and lower layers of blockchain. For instance, smart contracts are the mutual agreements which are self-assured, and both the parties agree on these set of rules to proceed with the transactions.
- **Consensus layer:** Consensus layer comes as the third last layer in blockchain's architecture. It uses consensus algorithm to ensure that the data stored in blockchain is consistent and accurate. The consensus algorithm has the power to accept and reject the transactions based on the mining process, which involves solving of cryptographic puzzle and verification of the

transactions. With the passage of time, different consensus algorithms are innovated for the improvements in blockchain's performance with respect to resources. Notable among them are Proof-of-Work (PoW), Proof-of-Stake (PoS), delegated Proof-of-Stake (DPoS) and others. PoW and PoS will be discussed in detailed later as the focus of this study.

- **Network layer**: As mentioned earlier, that blockchain is a distributed system and works under peer-to-peer broadcasting protocol. Each node in the blockchain has the full control to check the correctness of data, keeping the copy of data and can reject the transaction by not sending validation message to sender.
- **Data layer**: It processes the data from blockchain and stores it in blocks along with the timestamp, Merkle tree root (MTR) hash without the hash of previous block, which is only in the logical layer. Data layer does not have any information or identification of the sender or receiver, thus ensures the property of anonymity.

2.5 Types

The blockchain system is composed of several nodes, few of them can have the arbitrary or Byzantine (untruthful) behavior. Therefore, blockchain transactions follows the same set of operations as in the typical database and adhere to fulfil ACID (Atomicity, consistency, isolation, and durability) properties for data validity (Dinh *et al.*, 2018). According to Andreev *et al.* (2018), there are three main types of blockchain technology based on the access privileges given to them. Mainly named as permissionless blockchain (Public) and permissioned blockchain (Private and Consortium) (Andreev *et al.*, 2018).

2.5.1 Public blockchain

Public or permissionless blockchains are open for everyone. They are considered as uncontrolled blockchain as the access privileges to this type of blockchain is not restricted. From running a node, accessing wallet, writing data to transactions to reviewing transaction and contributing to consensus protocol is for all, if you are abiding by the principles set by the blockchain (Dattani *et al.*, 2019). Since anyone can contribute to the public blockchain, they are vulnerable to attackers who can manipulate it by illicit means. Therefore, consensus or a joint agreement algorithm is used to impose certain set of rules (Yaga *et al.*, 2019). Most of the public electronic ledgers imply Proof-of-Work consensus for transaction verification. The most popular public blockchains are Bitcoin and Ethereum. However, both differ in the workings and uses (more details in the chapter 4).

2.5.2 Private blockchain

On contrary to the permissionless blockchain network, private or permissioned blockchain network only authorizes specific users which can interact with the ledger. Blockchain's permissioned network can restrict even read and transaction issuing access of the user. This type of network is usually used inside the organizations who wants to enforce strict rules and regulations, have multiple business partners and they want to create a trust-free or transparent system (Yaga *et al.*, 2019). This type of controlled access can be categorized into two, either private or consortium. The former is fully restricted, you need to take access right from the one single administrator/entity to participate or act as a validator for example, ripple blockchain and the latter is known as semi-decentralized network. This network is controlled by the more than one administrator inside the organizations, such group of administrators are known as federation or consortium. Notable example of consortium blockchain network is Hyperledger (Dattani *et al.*, 2019).

2.6 Uses of blockchain

Many authors emphasized on the fact that blockchain can be an integral part of our lives and can effectively change the process of transactions and their storage system. Blockchain technology has various applications in the different areas of technology. As it is not just a tool for storing virtual currencies in a decentralized system but is applicable to many other industries in which, it has shown extensive in-depth implementation. Following is few of them:

- **Smart Contracts:** An essential part of Ethereum blockchain is smart contracts and are defined as the small pieces of code with if-then logic, where the users deploy them according to their need. For example, if someone wants to write their inheritance will into the blockchain based smart contract, this contract will be executed after the person dies and cannot be intervened from any third party. Similarly, other applications of smart contracts exist in the notarization of real estate, betting or where users want to establish a mutual agreement without involving central authority (Foroglou *et al.*, 2015).
- **Supply Chain:** Supply chain as well as logistics had a huge stir due to the emergence of blockchain technology as it offers characteristics such as immutability and transparency. Most important applications of blockchain like timestamps, public-private (asymmetric) key encryption, digital ledger, and smart contracts are beneficial in the field of supply chain management and logistics (Korpela *et al.*, 2017). For instance, the consumers want guarantee that the good being delivered to them are derived from the legal means and blockchain

provides the transparent chain of transactions which are added to the blockchain by distributed consensus protocol (Francisco *et al.*, 2018).

- **Voting:** Traditional voting procedure has always been a controversial topic in many countries, incidents like rigging, invalid votes and multiple registrations are producing the inaccurate results. Therefore, to increase authenticity and reliability of votes Foroglou *et al.* discussed that blockchain technology has proposed the electronic voting systems where users authenticate themselves (biometric or any other technique), cast vote by using public-private key pairs and votes are stored in distributed ledger anonymously (Foroglou *et al.*, 2015). Example of such electronic voting systems are Votecoin, Remotengrity, AgoraVoting and BitCongress.

2.7 Blockchain's cryptographic security

Generally, unconditional security is not provided by any practical system which relies over cryptographic solution. But existence of certain conditions such as limited computation capacity or the hardness of cryptographic problem, can lead to conditional security (Maurer & Wolf, 1997). There are multiple factors which can affect the security of the system for instance, the organization of network, working of consensus, methods of transaction verification and storage of cryptographic keys etc. Many cryptographic techniques and concepts have been used in blockchain technology. The emphasis of this thesis will be on the digital signatures, zero-knowledge proofs, and hash functions for the purpose of founding the base of analysis and technical details presented in the next sections:

- **Digital signatures:** A digital signature, as Maurer and Wolf noted, safeguards the message integrity (Maurer & Wolf, 1997). They are based on public-key cryptography and are used to protect against forgery and tempering. They are short codes generated with the help of a private key and are verifiable with the corresponding private key. Every time transaction is created, it is digitally signed and sent to the receiver which can be publicly verifiable (M. Raikwar *et al.*, 2019).
- **Zero-knowledge proofs (ZKP):** Zero-knowledge proofs or ZKPs are used for verifying that the "transfer of an asset is valid" without revealing any information about the asset (Goldreich & Oren, 1994). This concept is implemented in the Zerocoin blockchain for untraceable and anonymous transaction data, it is the extension of bitcoin. A variant of zero-knowledge proof has also been used in zerocash protocol, known as zk-SNARK. It reduces the computational effort and size of the proof.

- **Hash Functions:** Importance of hash functions to the security of blockchain can be comprehended by the previous sections of this study. Proof-of-Work and Proof-of-Stake are also hash based consensus algorithms and in the later part of this thesis it will be discussed how the hash functions are utilized in the building of consensus algorithm and why they are important. Therefore, taking a closer look on the definition, background and properties of hash functions is an essential part of this writeup.

  In the past, with the growth of information systems, this process of hashing was introduced that maps the larger data storages to the short, fixed length "key", for smooth and quick data operations. Hashing techniques also reduce the resources consumed for the data representation. Furthermore, hashing techniques are divided into data and security-oriented hashing techniques (Chi & Zhu, 2017).

  Cryptographically, when a fixed length "output" is generated by the arbitrary length input, is known as hash function. A cryptographic hash function should be *one-way* that means it should have the following properties (Preneel, 1998):

  - **Collision resistant:** Collision means having same hashed output for the different input values. Thus, collision resistance is an important property of a hash function which means having two distinct hashed inputs $\mathbf{x_0}$ and $\mathbf{x}$ for the same output is "hard", such that:

    $\mathbf{hash\ (x_0) = hash\ (x)}$
  - **Preimage resistance:** Preimage resistance refers to computational infeasibility of finding a hashed input $\mathbf{x}$ that matches to the given output $\mathbf{y}$, such that:

    $\mathbf{hash\ (x) = y}$
  - **2nd preimage resistance:** Second preimage resistance also follows the same concept as preimage resistance with a little difference, that it is computationally not possible to find the second input $\mathbf{x_0}$ which has the same hashed output for given input of $\mathbf{x}$, such that:

    $\mathbf{hash\ (x_0) = hash\ (x)}$

    All these three properties should be fulfilled for a hash function. Property of 2nd preimage resistance is implied by the collision resistance property. While preimage resistance is implied by the 2nd preimage resistance. Preimage resistance is also known as the one-way hash function (Preneel, 1998).
- **Encryption scheme:** As blockchain creates a trustless system, a need for the secure means of communication was required. Hence, encryption scheme provides the platform for encoding

data to authorize only legitimate parties. Multiple encryption schemes were developed and throughout time in blockchain. For example, symmetric-key encryption is used in blockchain based smartly designed home devices (Dorri *et al.*, 2017) and in Hyperledger fabric to restore confidentiality of the smart contracts (Androulaki *et al.*,2018).

2.8 Interoperability

According to Wegner, "interoperability is the ability of two or more software components to cooperate despite differences in language, interface, and execution platform" (Wegner, 1996). Interoperability is a concept of supporting one blockchain to other for transferring assets or information. One of the notable applications of blockchain interoperability is in the field of healthcare, which can help in delivering patient data safely, enabling the useful user interactions with the medical applications and can enhance the entire workflow of healthcare.

2.9 Energy Consumption

As Sedlmeir *et al.* pointed out, the applications of blockchain especially Bitcoin, Ethereum and Hyperledger fabric, are raising since this last decade due to the decentralized environment blockchain proposes (Sedlmeir *et al.*, 2020). However, according to De Vries (2018), Bitcoin uses a lot of energy. The elevated costs of energy consumed by the blockchain have always been a challenge for blockchain technology since its invention. Proof-of-Work (PoW) consensus used in Bitcoin is reported to be high energy-consuming, according to the "Bank for International settlement (BIS)" (BIS, 2018). Furthermore, considering sustainability and climate change's ongoing discussions, these declarations can consequently halt the growth of blockchain technology (Sedlmeir *et al.*, 2020). Hence, this writeup is aimed to provide the detailed analysis of the energy consumption by the two most popular consensus algorithms Proof-of-Work (PoW) and Proof-of-Stake (PoS) and then a comparison on both consensus mechanisms to deeply understand the advantages and disadvantages of one over the other in terms of implementing blockchain technology on a wider scale.

2.10 Scalability

Scalability and cost challenges are always discussed side by side whenever we mention the demerits of blockchain technology. The expense of having and maintaining the blockchain based application increases as the blockchain network grows, as it has been seen according to Zheng *et al.*, with the Bitcoin that the transactions are taking nearly 10 minutes each and the size of one block is nearly 1 MB that ends up taking 100GB of space in database (Zheng *et al.*, 2018). This means, larger the block size the slower is its transmission within the network, for example, Bitcoin can only process 7 transactions per second due to low latency and throughput, results in delaying millions of transactions. Usually, consensus mechanism like Proof-of-Work (PoW) can deal with the issue of scalability but it causes high latency (time needed for block addition in blockchain) and low throughput (transactions per second). The reason for low throughput again is its computational expensiveness and puzzle difficulty for mining a block (Monrat *et al.*, 2019).

On contrary, Ethereum utilizes the PoW algorithm with a different approach of designating specialized hardware only for mining, which costs a lot of electricity. Thus, scaling along the challenges of computation and storage resources, cryptographic puzzle difficulty, management of network complexity is extremely difficult task despite having blockchain's great potential of changing the futuristic world of networking systems. Many optimizations and blockchain redesign efforts have been proposed as well as ideas like division of blocks at the time of sharing and verification but all are still under construction.

2.11 Forking and Double Spending

Another challenge blockchain faces is forking. In simple terms, when a single block in the blockchain is pointing towards the two child or subsequent blocks, is known as forking. Technically, this condition happens when two nodes for example A and B, both publish their block at the same exact moment from same original block as shown in the Figure 5. Then, there are two valid chains of blockchain exists at same time and the miners can add the newly mined blocks to any of the chain, of course it will trigger problem of contradiction as both the chains will have distinct transactions in the respective blocks.

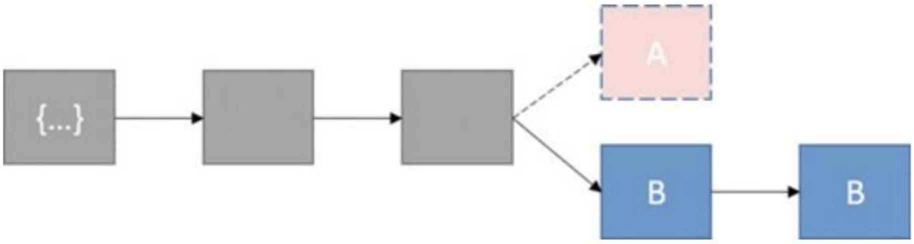


Figure 5: An example of forking. Source: (Sriman *et al.*, 2021).

Forking is divided into soft and hard forking. Soft forking enables nodes to trace back and update, while hard forks are incompatible. All in all, this condition creates space for the attackers to do diverse attacks for example double spending. Double spending is a situation when attacker utilizes same coin twice (more will be discussed in chapter 5). Forking and double spending are directly related as forks can be used to effectively do this kind of attacks. Usually, to resolve forking a longest chain with a greater number of blocks is considered as an authentic chain and all other chains are rejected. Then the miners have to submit the transactions again which were rejected previously.

3 Research methodology

3.1 Goals of research methodology

Research methods are considered as to provide you a roadmap and guideline for your research journey to solve a problem (Dresch *et al.*, 2015). Blockchain technology is one of the newly emerging technologies and the studies or researches on it are still in the early phases. In addition, it has a diverse scope, a thorough, qualitative, and deep study is required to explore the unique nature of this technology and to get advantage from its full potential. Therefore, this thesis has been devised to apply the explorative research methods to identify whether the new protocols introduced can spread the blockchain as general-use system in the world or not. To understand the subject, this study will provide a detailed comparison between the consensus algorithms and a concise conclusion of what works and what does not.

3.2 Reflection on methodology

Chosen research method plays a vital role in the whole process of research and impacts how the problem in question is answered. According to Dresch *et al.*, most efficient, and useful research approach should be selected, according to the relevance of research problem to the research method and the legitimacy scientifically (Dresch *et al.*, 2015).

Creswell (2009) point out that the secondary methods of doing research and gathering data beforehand can contribute to saving resources and time drastically (Creswell, 2009). Therefore, a qualitative desk research, defined as exploring the problem with the help of published materials such as reports, research papers etc. which is used to answer the research question to minimize the future costs related to blockchain based solutions and propose the cost analysis comparison of consensus algorithms.

This literary work has been built on the existing research studies and quantitative results derived from the simulation experiments.

3.3 Methodology of research

In the related literature workings, Zhang, R. *et al.* provided the agent-based model based on simulations to assess the performance of consensus mechanisms, in other words a quantitative framework for the cost analysis of blockchain consensus protocols while De Vries *et al.*, Mora *et al.* and Sedlmeir *et al.* has provided the qualitative frameworks to describe the technicalities of comparing the energy consumption of one protocol over the other (Zhang, R. *et al.*, 2020, De Vries *et al.*, 2018, Mora *et al.*, 2018, Sedlmeir *et al.*, 2020). While these postulated a relevant blueprint and complemented to this research, still a desk research approach was needed to portray a detailed comparative analysis between the two popular blockchain consensus mechanisms with enlisting the pros and cons of both approaches and addressing their ability for widespread. Hence, based on deciding a more cost-efficient solution and evaluating its candidacy for takeovers.

4 Consensus Mechanism

This section of thesis is aimed at to provide deep understanding of consensus mechanism. The insurance of reliability is an important aspect of distributed computing. The consensus or joint agreement between all parties is used for consistency in the network, and it is known as a consensus mechanism. This mechanism is guarded by a consensus algorithm to make a decentralized application trust-free. Therefore, the efficiency of the network depends upon the efficiency of its algorithm.

Many consensus mechanisms are presented over time such as Proof-of-Work (PoW), Proof-of-Stake (PoS), practical byzantine fault tolerance (PBFT) which revolutionized blockchain technology (Zhang, C. *et al.*, 2020). But for the purpose of this study, we will investigate the two most popular mechanisms in blockchain, PoW, and PoS along with their analysis of individual characteristics.

4.1 Proof-of-Work (PoW)

Proof-of-Work is one of the widely used security protocol in Digital Ledger Technology (DLT). It almost takes up to the 90% market capitalization of all the cryptocurrencies (Gervais *et al.*, 2016). The idea behind this algorithm was to restrict unauthorized access to the blockchain by taking vote from the blockchain nodes utilizing their "processing" power to solve PoW instances to construct legitimate blocks. It employs hash-based nonce that must be smaller than the target hash value (Gervais *et al.*, 2016). The verification of valid node's block is done by the process of mining, it is the process of solving a cryptographic puzzle to validate the transaction (Golosova *et al.*, 2018). Each miner has different hash rate or computation power, miners with higher hash rate have more chances to solve puzzle quickly, hence can earn more rewards as illustrated in Figure 6. Miners find out the nonce and push the block to the network layer for peer validation. Peers can confirm whether it is a valid block hash or not by checking the condition of being smaller than target value (Gervais *et al.*, 2016).

However, the interval of block is defined as the time it takes to complete from processing of block till adding it to blockchain. The more difficult the cryptographic puzzle to solve for miner the more will be block interval. Hence, less difficulty means more blocks in the blockchain network in less time and vice versa. Therefore, adjusting the complexity of PoW mechanism is crucial for safer transactions and avoiding the security attacks (will be discussed later also).

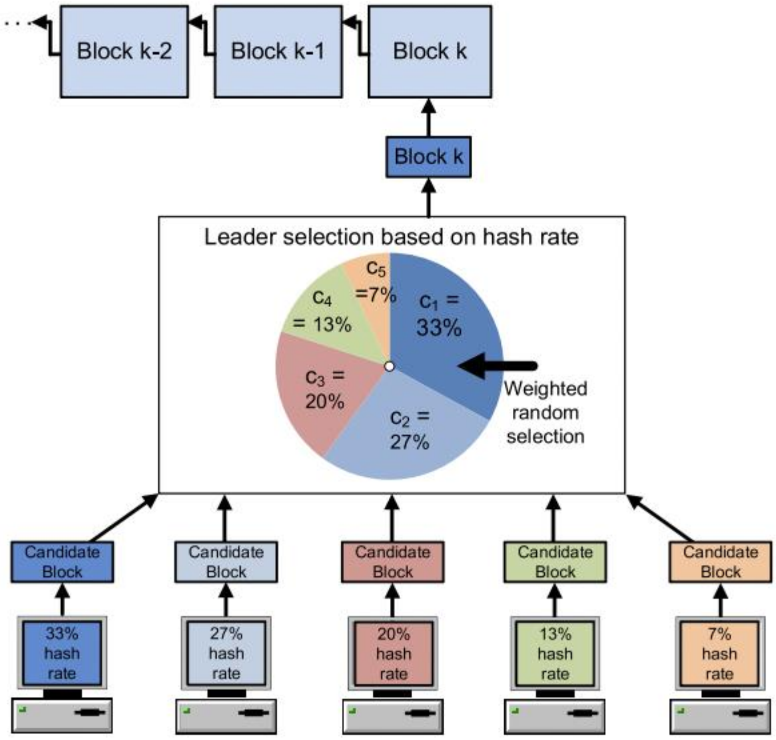


Figure 6: Proof-of-Work Consensus Process. Source: (Nguyen *et al.*, 2019).

4.1.1 Algorithm

According to Vashchuk *et al.* (Vashchuk *et al.*, 2018), if we take Bitcoin as an example, following are two halves of each Bitcoin's block:

1. Block header (time of block creation, previous block hash, Merkle root hash of transactions)
2. Block's transaction list

Condition

Proof-of-Work (PoW) protocol uses the block reference not exceeding specific threshold to check block's validity.

$$Hash(Block) \leq M/D \tag{A}$$

where

$D \in [1, M]$ is the targeted difficulty.

Therefore, first step to hash the block header two times using SHA-256 hash function (see SHA-256 section for details) to refer the definite block. This will give the value within the [0, 2^{256} - 1] interval.

All the key block header variables are iterated to find the valid block and it is directly proportional to the level of difficulty.

SHA-256

We already mentioned about the hash functions, informally, their computation is easy, but inversion is difficult (Gilbert *et al.*, 2003). Davies-Meyer construction and Merkle-Damgård (MD) construction are the basis of SHA-256 algorithm. Following is a fixed 256- bit formula, given that M is the arbitrary-length message and hash value V_n is computed (Yoshida *et al.*, 2005):

$$V_0 = IV$$

$$V_{s+1} = compress(V_s, M_s) = E_{M_s}(V_s) + V_s \, for \; 0 \leq s \leq n$$

where

1. $compress$ is compression function.
2. IV is initialization vector.
3. $E_{M_s}(V_s)$ is block cipher.

There are 64 rounds of SHA-256 compression function. This algorithm is considered invertible if the Davis-Meyer feed-forward function is removed. It has 256 bits size of digest. Generally according to Sriman *et al.* (Sriman *et al.*, 2021), digest is considered as:

$$digest = hash\ (data + nonce)$$

where

$Nonce$ is the initial random number.

Time

A miner equipped with specialized hardware would take exponentially distributed time to find a valid block with rate *k/D*:

$$P\ \{T(k) \leq t\} = 1 - \exp\ (-kt/D)$$

where

1. *k* is the no. of iterations
2. *T* is time period.

If we assume that in Bitcoin the hash rates are $k_1, k_2 \dots, k_n$ for n miners. Hence, the time period T required to mine a block is less than and equal to random variable value $T(k_i)$ considering found block is published by miner and it is broadcasted to other miners instantly. Therefore, as per the exponential distribution properties, T is also exponentially distributed:

$$P\,\{T \text{ def} = min\ \ (T_1, \dots, T_n) \leq t\} = 1 - \exp(-t\ D\ ) \sum_{n}^{i=1} k_i$$

$$P\,\{T\ = T_i\} =\ k_i / \sum_{n}^{j=1} k_j$$

Fairness

Proof-of-Work (PoW) algorithm mining is fair as we have seen in the above equation, each miner m would have probability p having computation power to find a block before the other miners.

4.1.2 Properties

In 2008, Satoshi Nakamoto proposed a consensus mechanism of Proof-of-Work for permissionless blockchain like Bitcoin (Nakamoto, 2008). Each block represents a group of transactions in a linear manner. The block is created through mining. The vital part of mining operations is "good connectivity", which gives advantage to miners with good connection.

PoW employs the "general purpose cryptographic hash function SHA-256" (Tikhomirov *et al.*, 2017).

Specialized hardware equipped with the application-specific integrated circuits and targeted GPUs are used for the effective implementation of PoW. However, puts the big miners into unfair advantage than others.

4.1.3 Transaction verification technique

In Proof-of-Work (PoW) setting, the core function is to make network resource available by solving the computationally hard problem. Users try to come up with the unique hash which comprises previous block hash, transactions, and proof. Hash computed by nodes should have leading zeros, is the network requirement. Initially to find the current block hash, proof is initialized with zero and a hash function is executed using previous block hash, transactions, and proof. As we can see from the Figure 7, if the resultant unique hash meets the network requirements it is added to block header otherwise the proof is incremented and the process is repeated until a suitable hash is found which matches the network requirements (Aljassas *et al.*, 2019).

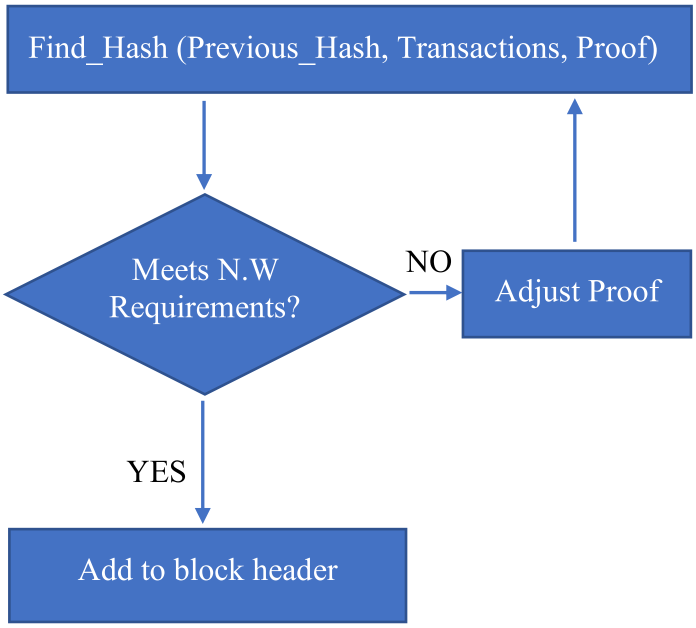


Figure 7: Proof-of-Work Model. Source: (Aljassas *et al.*, 2019).

A miner who successfully resolves the mathematical problem will be rewarded additional crypto coins and the probability of reward for a miner with the highest computational power is the highest. The average transaction confirmation time, known as block interval, as already stated in the case of bitcoin is 10 minutes, if the computational capacity of the network remains constant, and it will allow 7 transactions in one second (Koops, 2018). Therefore, after every 10 minutes, a new block is composed.

4.1.4 Advantages

In a decentralized environment like blockchain, adversaries can attack and exploit the system in many ways. To tackle this and make blockchain secure, Bitcoin introduced PoW and made sure that all nodes agree on the same blockchain's branch (Porat *et al.*, 2017). Moreover, Proof-of-Work (PoW) sets up the computationally difficult puzzles to avoid forking – condition when two nodes published a block at same time and both points to the same previous block.

The level of difficulty in PoW's cryptographic puzzles create a huge difference on the length of forks. Porat *et al.*, conducted the experiments on Ethereum based blockchain application, following results were obtained after setting the complexity of cryptographic puzzle to different values (Porat *et al.*, 2017). We can see that in Table 1 that average fork length has been reduced as we increased the complexity. That means, consistency of system gets reduced when length of fork increases, that makes the blockchain unreliable.

Table 1: Puzzle complexity on different levels. Source: (Porat *et al.*, 2017).

Problem Complexity	Average time to mine a block (in seconds)	Stale blocks mined	Average fork length
2.10^{-4}	0.03	302	21.47
2.10^{-5}	0.32	219	8.27
10^{-6}	2.62	42	2.61
2.10^{-7}	8.6	13	1

PoW helps to prevent the malicious or unauthorized access to the blockchain. It also gives protection against denial of service as only method for finding a none in hash-based PoW is brute-forcing and it is not economical.

4.1.5 Drawbacks

Proof-of-Work's mining process is often considered as the race. The miner, who has higher processing capacity wins the race and hence results in quick addition of nodes into blockchain which are unchangeable and immutable. The amount of power and electricity consumption this process takes is a major drawback of this protocol. Another reason of consuming large amounts of computation and energy is the signature verification of the blockchain, every transaction is signed cryptographically and requires resources to calculate signatures transaction. Furthermore, it can have negative impacts on the environment (Golosova *et al.*, 2018) and it is also a big hurdle for scalability of blockchain applications (Gupta *et al.*, 2018) as the need of computational resources increases with the increase in the network size for big open systems requiring security.

PoW has some major security drawbacks as well. When the energy costs are so high for security providing mechanism, it can create a selfish environment where people will try to reduce the cost and end up compromising the security (Gupta *et al.*, 2018). PoW is prune to 51% attack, if the 51% of validators vote towards a single block that it is valid, it will be considered a valid block. For example, if attacker accumulates 51% computation of network, then blocks can easily be added by him or her. Attacker can also do distributed denial of service (DDoS) attack after acquiring this much computation power and some other attacks that are discussed in last section.

4.1.6 Applications

As we discussed, Proof-of-Work (PoW) is the consensus which is widest deployed. It has different blockchain instances. For example, Bitcoin, Litecoin and Ethereum all implements the hash-based Proof-of-Work (Gervais *et al.*, 2016). In general, most of the public blockchain networks tend to use Proof-of-Work as their consensus algorithm. Two biggest implementations of blockchain are Bitcoin and Ethereum, both are public blockchains and users have unrestricted access to them. Let us have a closer look at both as they have separate uses and implementation approach.

- **Bitcoin:** Bitcoin is an online tool for communicating, 368m transactions are operated from Bitcoin, with market value of circulating $121 billion (Blockchain.com, 2015). It is a virtual protocol for communicating e-payments. It rewards the special nodes for verifying the transactions to be added into the block (Böhme, 2015).
- **Ethereum:** Ethereum is a full featured programmable platform that uses Proof-of-Work (PoW) as consensus algorithm like Bitcoin and provides the ability to implement complex business logic. It was designed over the Turing complete smart contracts, that are stored permanently on the blockchain and can respond to user requests to modify the value of digital units (Tikhomirov *et al.*, 2017). Thus, Ethereum is considered as a universal blockchain platform on which other applications can be founded with customized set of rules and formats stated in the smart contracts.

Following are the metrics of Bitcoin and Ethereum, we can see in the Table 2 that both of them have million dollars trading volume and market capitalization. Also, they have thousands of transaction transmission per hour, hence creates the huge size of blockchains. Still, Bitcoin is two folds bigger in size than the Ethereum. By looking at these numbers, we can say that Proof-of-Work base blockchains are widest spread globally.

Table 2: Ethereum and Bitcoin (Sept 2017). Source: (Tikhomirov *et al.*, 2017).

Metric	Bitcoin	Ethereum
Number of nodes	9428	22007
Blockchain size	158 GB	52 GB
Transactions per hour	8509	12406
Market capitalization ($ million)	62812	27200
Daily trading volume ($ million)	997	420

4.2 Proof-of-Stake (PoS)

Proof-of-Stake (PoS) is an arising consensus algorithm whose base algorithm is Proof-of-Work. It was first realized by concept of coin age in 2011. Coin age is the product of currency amount and holding period for example, if a person is holding 10 coins for 90 days, it has accumulated coin age of 900 coin-days (King & Nadal, 2012). The cryptographic challenge imposed by the PoS needs less consumption of energy to add records in blockchain by the trusted parties and voting among them (Golosova *et al.*, 2018). The main concept of PoS was to avoid mining power and user's mine and create blocks with probability, based on their ownership stake in circulation within the system as illustrated in the Figure 8. Users who have the highest share in the cryptocurrency have the highest interest to secure it otherwise value of cryptocurrency can depreciate as being vulnerable to attacks. Adversary can attack the system if has the majority of cryptocurrency (Vashchuk *et al.*, 2018).

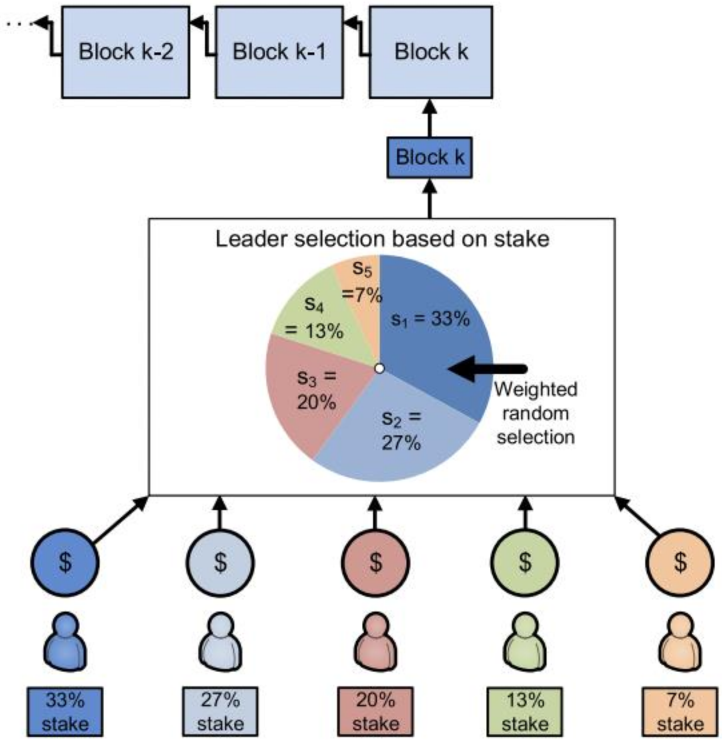


Figure 8: Proof-of-Stake Consensus process. Source: (Nguyen *et al.*, 2019).

4.2.1 Algorithm

As we have conversed earlier, the probability of creating the block depends upon the ownership of user stake rather on properties of block.

Condition

According to Vashchuk *et al.*, in Proof-of-Stake algorithm the main condition is to abide by the balance, so the condition would be as follows given that the user has address A and has balance (Vashchuk *et al.*, 2018).

$$Hash(Hash(Block_{prev}), A, time) \ \leq \ balance(A)\ M\ /\ D \tag{B}$$

where

- $D \in [1, M]$ is the targeted difficulty,
- $\text{Block}_{\text{prev}}$ is the previous block with which we are linking to,
- time is UTC current timestamp and can be changed by the user,
- balance(A) is locked, and user cannot change it.

Pre-requisites

Proof-of-Stake (PoS) involves no complex computations and has the following pre-requisites for user using the system:

- User must provide the address A, address’ proof of ownership and timestamp t meeting the requirements set by (B).
- User must have private key for the associated address A.

Time

For address A to find a block, time is exponentially distributed as:

$$bal(A)/D$$

And for the whole network to find a block, exponentially distributed time would be sum of all nodes time:

$$\Sigma\, a\ bal(a)/D$$

Fairness

The Proof-of-Stake (PoS) algorithm is fair, each user has the probability p to create a valid block based on the ratio of balance to the cryptocurrency they have in circulation of system.

4.2.2 Properties

Following are the properties of the Proof-of-Stake protocol:

- Proof-of-Stake is like the form of currency's ownership proof.
- The owners of cryptocurrency can participate in mining and contribute their few coins to secure network.
- It gives everyone chance to participate in the process of mining and thus reducing centralization.
- Proof-of-Stake is environmentally friendly.
- Special mining hardware is not needed.

4.2.3 Transaction verification technique

The transaction in Proof-of-Stake (PoS) is called coinstake transaction. This special transaction is mined by the owner of the cryptocurrency in which they are mining by utilizing coin age and in return they get the transaction fee as a reward (King & Nadal, 2012).

The hash target is met in the first input i.e., kernel input of the transaction that makes it stochastic like Proof-of-Work protocol, as shown in the Figure 9. The only difference is it is done on restricted search space that is single hash per unexpended wallet-output in one second instead of unrestricted search space as in Proof-of-Work. Hence, no meaningful computational power is needed.

Another key point in the kernel input is that hash target is not fixed like in Proof-of-Work, rather it depends upon the coin age consumed. For instance, if a person has 50 coin-years accumulated in the wallet-output and anticipates producing kernel in 3 days, then a second person can roughly anticipate from his/her 100 coin-years wallet-output producing a kernel in 2 days (King, & Nadal, 2012).

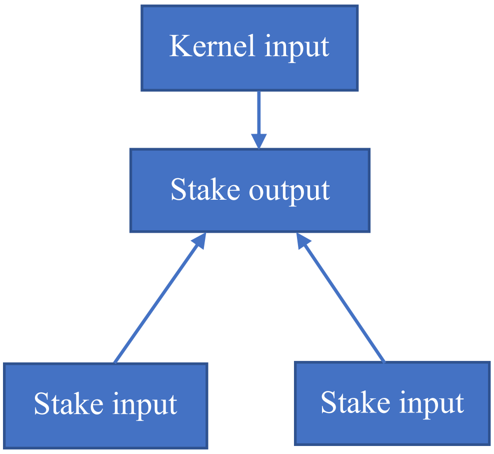


Figure 9: Proof-of-Stake transaction structure (coinstake). Source: (King & Nadal, 2012).

Proof-of-Stake is carried with every transaction within the network. Owner wants his transaction to get accepted while recipient validates it according to conditions of network. Every stakeholder has a contribution in the security of the network. Coin-days are defined as number of days since last transaction of the specific coin on the network, act as a proxy between the network and stake. They are destroyed whenever a transaction involves stake coins. In addition, coin-days-destroyed cannot be used again (Larimer, 2013).

4.2.4 Advantages

The main purpose of invention of Proof-of-Stake (PoS) was to deal with 51% attack. In Proof-of Work (PoW), attackers keep the chain secret and broadcast the longest secret chain to invalidate the transaction. The same strategy of maintaining secret chain that is longer than the original chain, is also used in the other attacks such as denial of service, selfish mining, and double spending. To prevent them, PoS implies to have current block hash and can credit the transaction's stake only in the blockchain. Thus, after committing of the transactions in the blockchain, best blockchain is picked up based on the coin-days-destroyed, instead of the total work (Larimer, 2013).

Proof-of-Stake (PoS) consensus is reached by a set of validators. Blockchain's cryptocurrency is deposited by them, and votes weighed by their stake are casted. No unnecessary amount of electricity is ingested during this process. Furthermore, it is fully decentralized as there is no cost of scaling it (Moindrot & Bournhonesque, 2017).

Another benefit of having Proof-of-Stake (PoS) as a protocol that user does not have to wait or being dependent on the miner for block confirmation, if you want to speed up you can use some of your coin-days and can confirm the transaction. Moreover, transactions can also be divided into the smaller parts and first half can be confirmed by the second half of transactions (Larimer, 2013).

4.2.5 Drawbacks

The blockchains powered by the Proof-of-Stake (PoS) consensus algorithm are accounted as less than 2% of the existing cryptocurrencies' market capitalization. Because it is vulnerable to the following security attacks (Li *et al.*, 2017):

- Nothing-at-stake: During this attack, the conflicting blocks in the blockchain can be mined without using the stake by the attacker. As a result, the forks and network time to reach consensus will be increased.
- Long-range attack: This attack enables the adversary to modify the entire history of the blockchain including the genesis block. To successfully execute this attack, adversary needs the access to older account's private keys having no stake but accumulated most of the stake at block height h of the previous block. Thus, adversary performs attack by utilizing these accounts and constructing the fork at block h.

Proof-of-Stake does not fully solve the problems of double spending and denial of service. Any adversary who has accumulated enough coin-days and can execute the double spending attack.

It limits the number of people mining in Proof-of-Stake as well as the cryptocurrency supply, available to protect the network. The miners get only 1% return on their stake, which is minimized by 8% inflation rate of Proof-of-Work (PoW) miners (Larimer, 2013).

4.2.6 Applications

Some of the Proof-of-Stake (PoS) based blockchains are as follows:

- *Peercoin* is a well-known application of Proof-of-Stake, it is based on "proof blocks" in which target of miner is in reverse to the number of coin days consumed. Only Peercoin owner can mine Peercoin transactions by committing some of their coins towards the security of Peercoin (Larimer, 2013).
- *BlackCoin* is another popular implementation of Proof-of-Stake (PoS) protocol. It provides the user's ability to have the anonymous address online unlike Bitcoin (Averin *et al.*, 2020), thus considered as the secure system having the market capitalization of 15 to 20 million dollars (Vasin, 2014).

5 Proof-of-Work vs. Proof-of-Stake

5.1 Energy/Electricity Consumption

According to Sedlmier *et al.*, bitcoin's Proof-of-Work (PoW) consumption of high energy is not the outcome of older hardware or ineffective consensus algorithm (Sedlmier *et al.*, 2020). It was meant to use intensive resources by design, which guards the blockchain from various attacks. To tamper blockchain, attacker should have at least 25 to 50 percent of the computation units in comparison to the miners, hence equivalent resources will also be consumed. Crypto-currency is mainly dependent on energy consumption according to Nakamoto's Proof-of-Work (PoW). Thus, bitcoin network operations introduce cost overhead and when network slows down, transaction fees are spiked to counter the preferred level of security.

Generally, the estimates of upper and lower bounds can be obtained as the cryptographic puzzles' difficulty is easily observable (Vranken, 2017). For example, the lower bound of the Proof-of-Work (PoW) blockchain will be given as:

$$total\ energy\ consumption \geq total\ hash\ rate\ \times\ minimum\ energy\ per\ hash$$

To calculate reasonable estimates from above equation no other parameters are involved. Furthermore, the present-day hash rate and most effective hardware used for mining, both can be found from internet. It is also worth noting here that the algorithms used for mining can somehow limit the performance of hardware. For example, Ethereum can be operated on normal GPUs, but Bitcoin's SHA-256 algorithm requires specially integrated circuits which are highly optimized for mining. Next, we can also find the upper bound for the Proof-of-Work (PoW) based blockchain where miners sole purpose is to gain profit:

$$total\ power\ consumption \leq \frac{mining\ reward\ \times\ currency\ price\ \times transaction\ fee}{average\ block\ time\ \times\ minimum\ price\ of\ electricity}$$

Contrary to the lower bound, upper bound cannot be tight due to different prices of electricity worldwide. Therefore, according to De Vries *et al.*, assuming 0.05$ per kWh as lower bound for electricity, then lower bound of power consumption per year will be 60TWh and upper bound 125TWh for Bitcoin (De Vries *et al.*, 2018). This electricity consumption is equivalent to Norway (125GWh) and Austria (75GWh). Figure 10 shows the top 5 digital currencies based on Proof-of-Work along with their annual energy consumption.

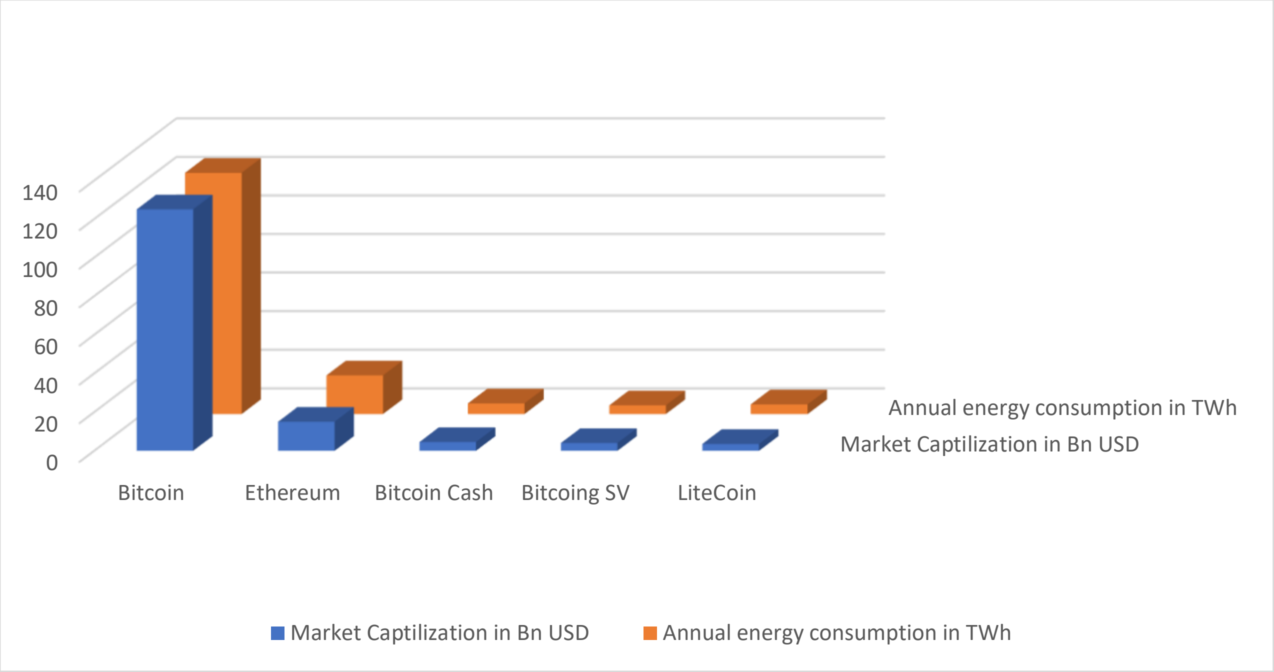


Figure 10: Top 5 Proof-of-Work digital currencies (Log scale). Source: (Sedlmier *et al.*, 2020).

In a nutshell, the cost of consumption of electricity is determined by the average size of block, minimum transaction sizes and maximum size of block. According to De Vries *et al.* (De Vries *et al.*, 2018) bitcoin energy consumption per transaction is ~900kWh by the end of 2018, on the other hand, energy consumption per capita in Germany is 1139 kWh/month (Moser *et al.*, 2018). From this we can assume that a single transaction takes electricity equal to an average (two-person) household in Germany for three weeks (Sedlmier *et al.*, 2020). If we compare this amount energy in case of all payments handled by Bitcoin, it can lead to rise in 2°C of temperature in global warming in coming decades (Mora *et al.*, 2018). Apart from the adverse impact on global environment, theoretically increasing blocksize and throughput should result into constant use of energy consumption but practically the size of block cannot be controlled. Hence, the block will take more time to be distributed across all over the blockchain which can impact both latency and the security of blockchain. However, the increase in overall speed of internet can make room for a considerable size of blocks. Thus, higher rates of transaction in exchange of fair cost of electricity.

As a conclusion, it can be deduced that Proof-of-Work (PoW) consumes a lot more energy than its technical implementation. The threat to environment will also be much significant even if a fair amount of more transactions is done. In addition, we cannot ignore the possibility of blockchain applications ahead of payments. Therefore, let us discuss an alternative consensus algorithm: Proof-of-Stake (PoS) to evaluate the metrics of performance or the energy consumed by considering the opportunities blockchain has provided to us.

So far, Proof-of-Stake (PoS) is probably the known consensus mechanism out there for public permissionless blockchains implemented for cryptocurrencies. The one of main advantage of PoS over PoW is that it skips the overall complicated puzzle solving step, which makes PoS less energy-consuming and efficient for extensively large systems. PoS has many lower orders of magnitude as compared to the PoW, Ethereum (2nd biggest cryptocurrency) is also trying to switch from PoW to PoS (Sedlmeir *et al.*, 2020). Other currencies which are ranked in top 20 with respect to market capitalization like TRON, Tezos and EOS have already adapted PoS.

5.1.1 Evaluation of energy consumption by PoW and PoS

In 2020, Zhang *et al.* (Zhang, R. *et al.*, 2020) presented the results built on an agent-based model analysis which consisted of:

- *Node agents*: It is the participant in blockchain and node generating module generates such node agent x ∈ X, containing three variables i.e., computation power, reliability index (node agent's loyalty) and coinage (product of number of coins and their holding time).
- *Block agents*: It is the block generated in blockchain, denoted as y ∈ Y, containing two variables i.e., timestamp and difficulty degree index.

and three main modules:

- *Node generation*
- *Block generation*
- *Evaluation module*

Figure 11 shows the structure of agent-based model from start to end:

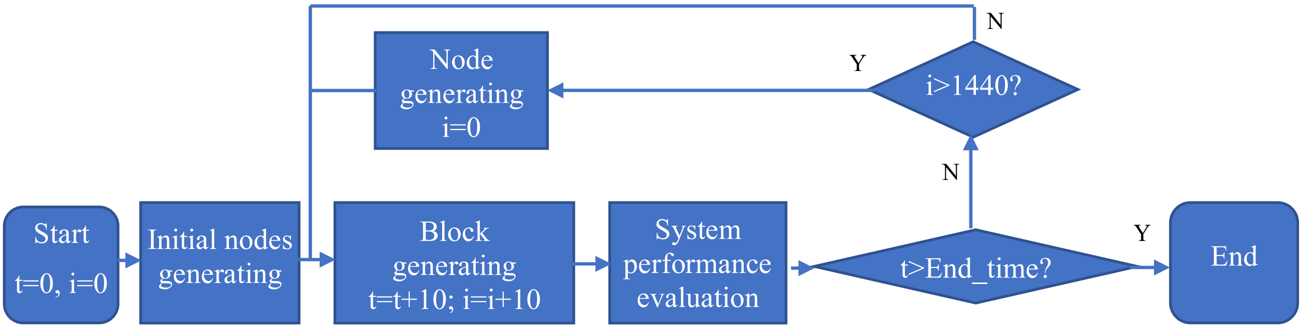


Figure 11: Agent-based model structure. Source: (Zhang, R. *et al.*, 2020).

Simulation experiments had different parameter settings (reliability index, computation power and random block generation) and the following simulation modes:

Table 3: Simulation modes. Source: (Zhang, R. *et al.*, 2020).

	PoW period	PoS period
Mode 1: PoS	0%	100%
Mode 2: 0.2PoW	20%	80%
Mode 3: 0.4PoW	40%	60%
Mode 4: 0.6PoW	60%	40%
Mode 5: 0.8PoW	80%	20%
Mode 6: PoW	100%	0%

Results and analysis of the study was obtained under six consensus mechanism experiments. There were three performance indexes: energy consumption, fairness, and reliability index. But for the purpose of this thesis, the focus will be on the energy consumption only.

The trend of consuming energy as shown in Figure 12 and Figure 13 is comparatively stable. However, it is highest for the Mode 6 and lowest for Mode 2. It is also noted that the energy consumption for Mode 1 is higher than Mode 2, because the adoption cost of the initial 20% period of PoW is less as compared to PoS adoption entirely.

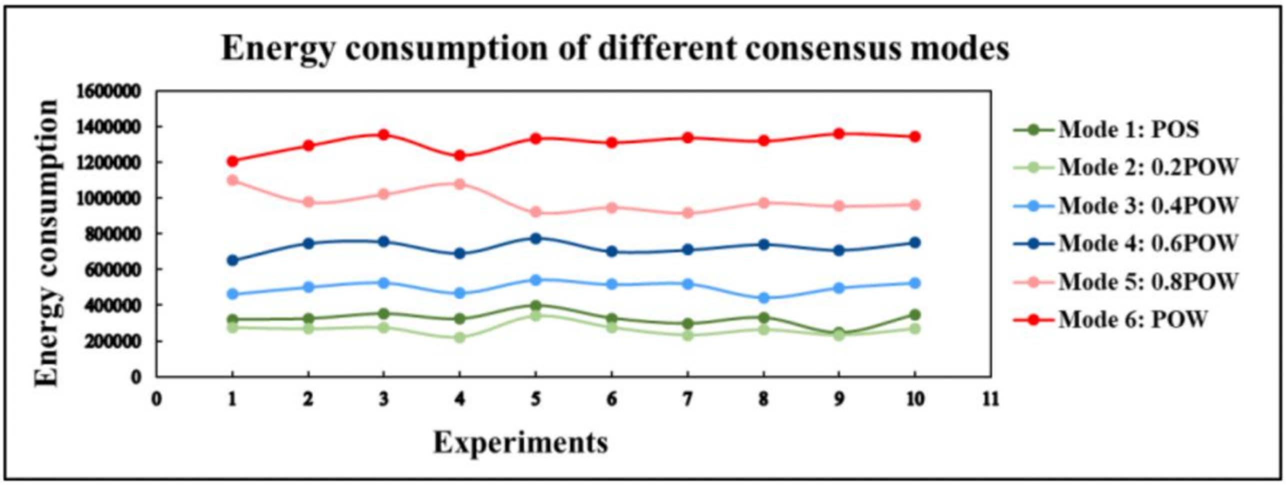


Figure 12: Different simulation modes energy consumption. Source: (Zhang, R. *et al.*, 2020).

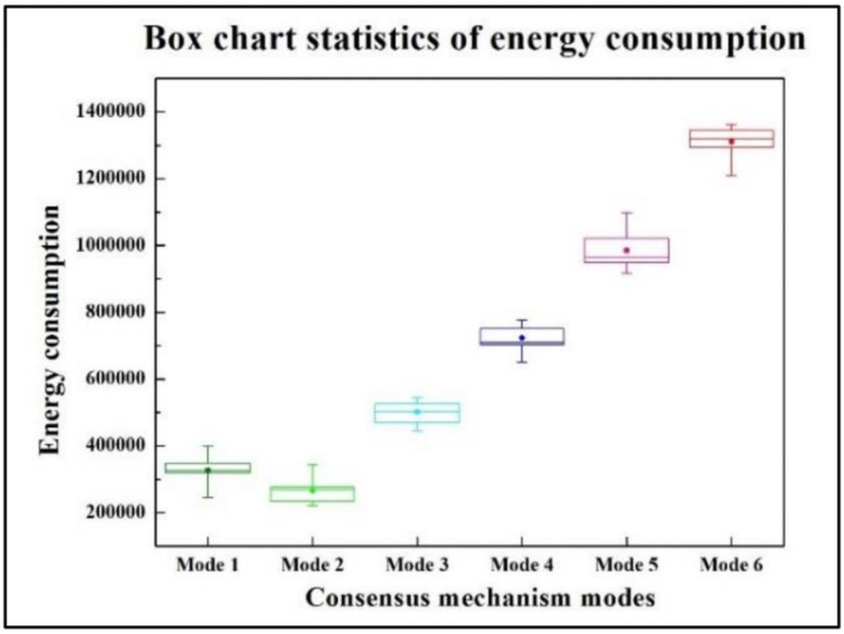
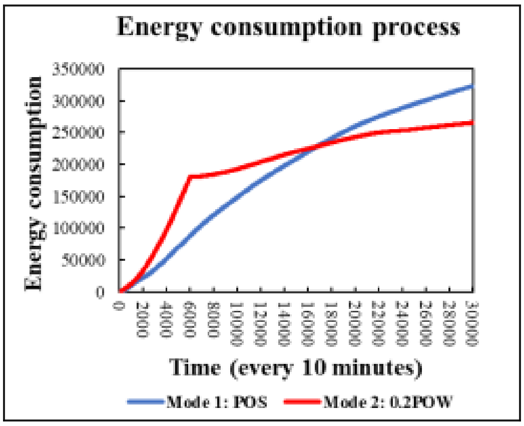


Figure 13: Energy consumption box chart. Source: (Zhang, R. *et al.*, 2020).

To discuss the basis behind Mode 2 consumed less energy than Mode 1. Basically, Mode 1 reduces use of energy a lot quicker than the Mode 2 in the remaining period due to less total current coinage of Mode 1 (Figure 14 and Figure 15). More coinage means the coins are more decentralized due to decrease in coins utility. Furthermore, PoW efficiently allocates the resources and coinage increasing on initial stage.



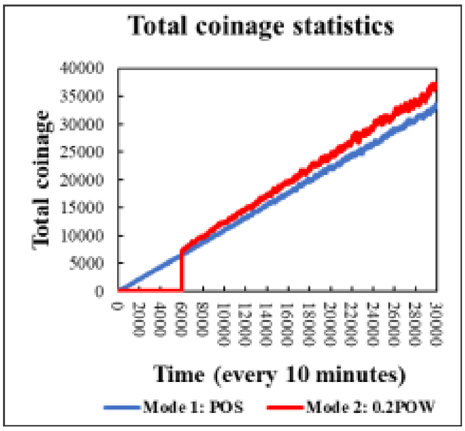


Figure 14: Energy consuming process. Source: (Zhang, R. *et al.*, 2020).

Figure 15: Stats of current total coinage. Source: (Zhang, R. *et al.*, 2020).

In a nutshell, this agent-based model has revealed that we can achieve lowest energy consumption with the mixed model which has 20% PoW and 80% PoS as well as can provide high fairness and reliability index to the system.

5.2 Decentralization

Proof-of-Work (PoW) faces a major risk of centralization, PoW's dedicated data centers for computation and transaction verification may outperform amateur miners due to huge economy of scale. The hash rate is a measure for computation power, roughly a bitcoin networks' hash rate is around 24.4 x 10^{18} hashes per second and 30 x 10^{3} hashes per second of an average commercial computer. Hence, such centralized organizations owning thousands of mining devices, known as 'mining pools', have the highest chance of winning. Processing powers are being shared on network within this mining pools and the mining rewards based on their resources used to solve the puzzle (Valdivia *et al.*, 2019).

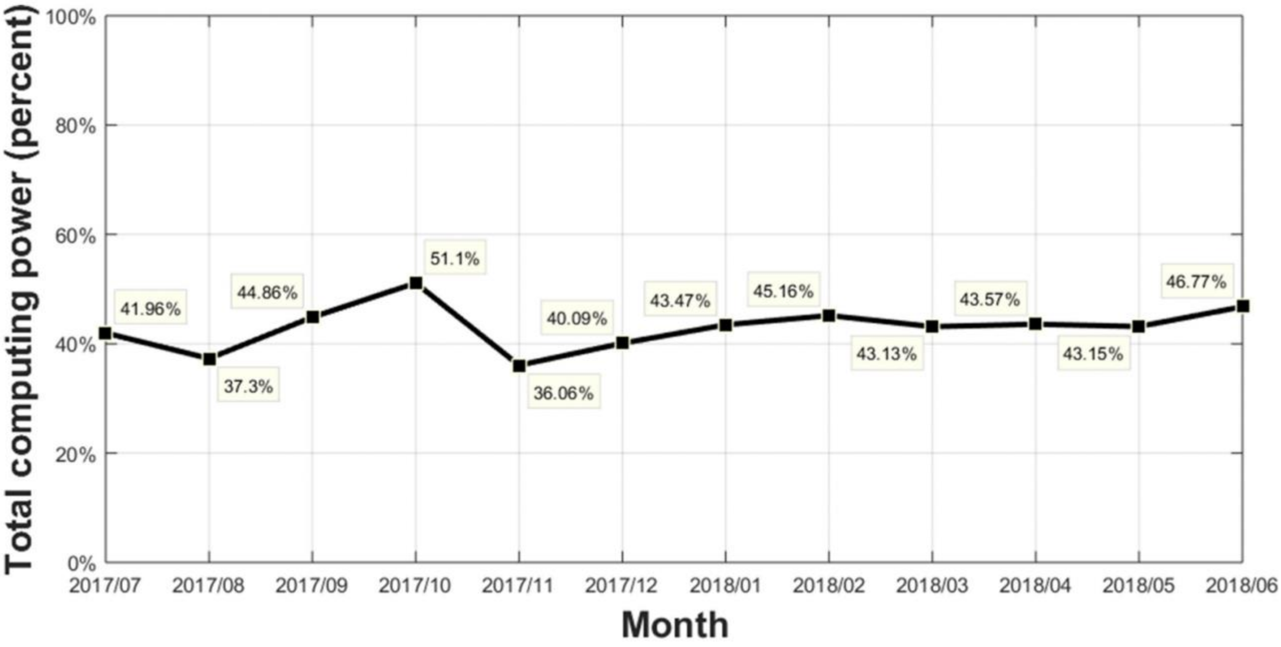


Figure 16: Combined computation power of top 3 mining pools over one year. Source: (Valdivia *et al.*, 2019).

From the Figure 16, is clear that the PoW causes major centralization as these 3 top mining pools own the 40 to 50 percent of the total computation power required to process bitcoin transactions. One of biggest disadvantage of centralization is that security of blockchain can be easily compromised by merely taking control of three main pools and it can cause network failure, effect availability or reverse new transactions (Valdivia *et al.*, 2019). Moreover, these pools can associate fees with transaction processing as they control the major chunk of network.

Secondly, if we look at the countries from where these huge numbers of computation powers are generated then China will be at top of the list, after that Czech Republic and USA as indicated in the Figure 17. Due to this, pollution is the growing concern for China. Also, high hash rate can restrict the cryptocurrencies' regulations that can distress the network.

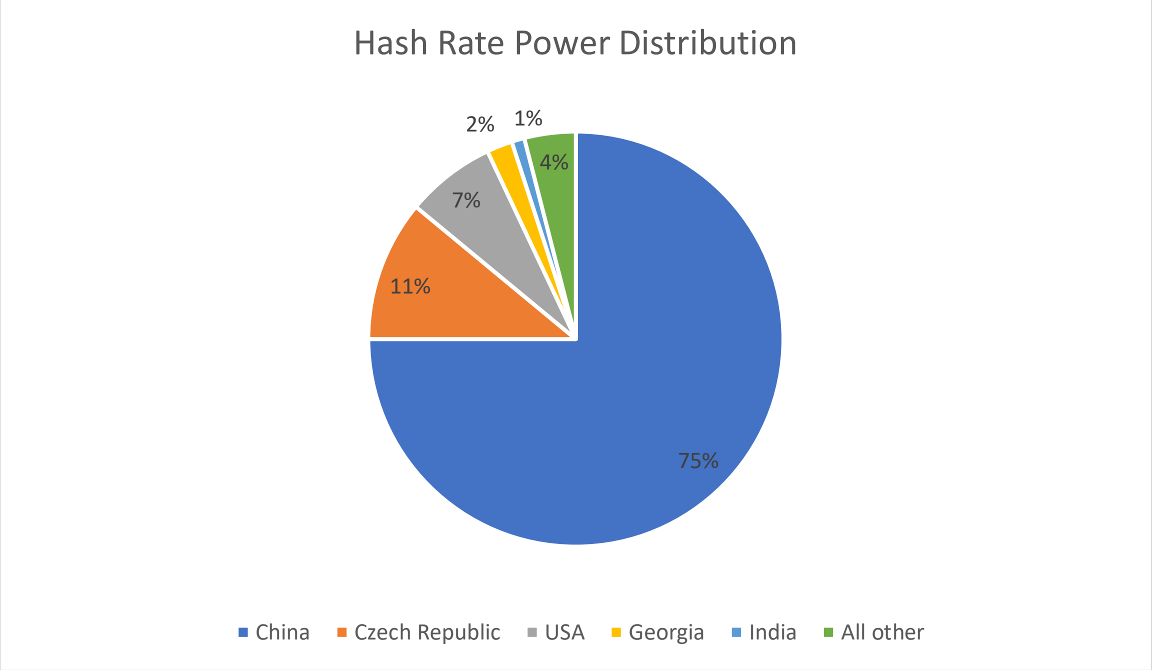


Figure 17: Per country hash rate power distribution. Source: (Valdivia *et al.*, 2019).

On the other hand, the risks of Proof-of-Work (PoW) data centers, energy costs, pollution are reduced with Proof-of-Stake (PoS) procedures, while some other risks remain intact (Bentov *et al.*, 2014). The main risk PoS includes is that large stakeholders may control the system, in other words wealthy people get benefit of it, and it would be centralized around rich who has more means to have bigger stake. In addition, if some individual or organization owns more than 50 percent of cryptocurrency coins then the same centralization issue can arise as PoS (Valdivia *et al.*, 2019).

5.3 Security

As we already discussed, the security model of Proof-of-Work (PoW) depends relies on the high computation power of hashes. This level of high hash power works as a proxy for total investment put into the blockchain. It can lead towards general assumption that biggest investment denotes majority consensus as to the reality, as we have seen in case of "mining pools". This assumption makes the PoW security model is more vulnerable to the attackers to exploit the trust than the PoS security model.

As we already discussed the 51% attack, the security principle of PoW says that no one should acquire more than 50% of the blockchain's processing power otherwise it can lead to centralized control of the blockchain by that authority/entity. Following are the known attacks for PoW-based-blockchains:

- *Double Spending*: As the name suggests, double spending means that when you utilize the same coin twice. Therefore, adversary can spend more than what they possess by taking advantage of network latency (Gervais *et al.*, 2016). In addition, these sync delays can be exploited more by *eclipse attacks*, where the attackers divide the blockchain network logically and provides the false information to the other blockchain nodes. The countermeasure to these attacks is to tightly synchronize the nodes of blockchain.

  The risk of double spending is high in the PoW as compared to PoS. Because PoW transaction takes reasonable time to process and add a new block to blockchain, on contrary PoS has much lower rate of adding the block as it does not have any riddles to solve before processing the transaction (Velliangiri *et al.*, 2020).
- *Selfish Mining*: Proof-of-Work (PoW) mechanism is also prune to selfish mining when miners attempt to withhold the major portion of the mined blocks to create a fork and then publishes them to go ahead of public chain and increase their relative mining reward share. It has been seen in the studies that with 33% a selfish miner can earn 50% of the mining power. But it is not considered as a rational strategy always, for example if the difficulty is not changed frequently than the honest miner can earn more reward than the selfish miner as in case of Bitcoin difficulty changes only once in two weeks (Gervais *et al.*, 2016).
- *Balance Attack*: According to Natoli *et al.*, PoW-based-blockchains are identified with new attack, known as balance attacks (Natoli *et al.*, 2016). They exploit the "block-obliviousness" limitation of Proof-of-Work (PoW), it says that:

  (Block Obliviousness) "A blockchain system is block oblivious if an attacker can:

  1) make the recipient of a transaction *tx* observe that *tx* is committed and
  2) later remove the transaction *tx* from the main branch, with a probability $1 - \varepsilon$, where ε is a small constant."

  Attackers delay the communication within the correct network's subgroup nodes having equivalent balanced mining power. Then, issues transaction in one subgroup and mines in another subgroup to ensure that the subtree of one outweighs the other. This attack is enough for double spending, only requires spotting the subgroup containing merchants and transactions can be created to buy items from these merchants. Due to high chances of outweighed subtree will be seen by merchant, intruder can reissue the other transaction utilizing the same existing coin. When the required items are shipped by merchant, the delayed messages can be resumed.

In a nutshell, by considering the overall picture of Proof-of-Work (PoW) security model vs. the Proof-of-Stake (PoS) security model, we can say that the known issues of PoW outnumbers than in PoS. However, the security issues in PoS such as greedy honest nodes, which keep the coin offline and get online for stake reward are kind of encourages the nodes' abusive behavior (Pavel, 2014).

6 Conclusions

The applications based on blockchain are becoming widely important throughout all fields especially in financial, security and privacy, Internet-of-things (IoT), reputation system, public and social services (Zheng *et al.*, 2018). The demands are getting high in these sectors and spreading towards other as blockchain is getting noticeable by the businesses. Therefore, it is of great interest to increase the research focus on attaining the deeper and better grip to make blockchain more reachable and improve the system under consideration.

Usually, blockchain has to tackle with the issue of scalability in order to offer the services and match the demand in all these areas. According to studies the issue of scalability is tough one to answer (Zheng *et al.*, 2018). But consensus algorithm constitutes one of the main components of blockchain. Thus, this thesis has focused on the two main protocols Proof-of-Work (PoW) and Proof-of-Stake (PoS). Both are considered to have the same underlying concept of using the cryptographic puzzle to give access to the network. But the idea of finding the cryptographic nonce on an unlimited space in PoW while PoS only people withholding cryptocurrency stake requiring to prove their stake ownership makes the whole difference (Zheng *et al.*, 2018). Hence, the focus on cutting the cost at base consensus protocol level can resolve one of the biggest hurdles coming in the way of spreading blockchain based applications on the wider scale.

This report has been targeted to make the underlying understanding of consensus mechanism process a lot simpler for the students focusing on particular area of consensus protocol within the blockchain. As a starting point, basic introduction, structure, overview of blockchain technology was and other founding concepts of blockchain architecture were presented. Based on the core concepts of consensus protocol such as properties, algorithm, process, transaction verification techniques advantages and disadvantages, implementation examples, ideas and related research, special focus of the study was given to the comparison of popular consensus mechanisms PoW and PoS according to the energy they consume, as well as decentralization and security they offer because they both are also a vital part of blockchain based solutions along with cost efficiency to provide scalable applications platform.

Efficiency, safety, and convenience are the key factors for a good consensus mechanism (Zheng *et al.*, 2018). Hence the main factors we sketched in the comparison analysis are energy consumption, decentralization, and security. When these features are combined within the blockchain application, a suitable conclusion can be drawn to assess which consensus mechanism serves the purpose best. This study corresponds and constructs the conclusions upon the workings of Zhang *et al.*, Gervais *et* *al.*, De Vries *et al.*, Mora *et al.*, Sedlmeir *et al.* and others (Zhang, R. *et al.*, 2020, De Vries *et al.*, 2018, Mora *et al.*, 2018, Sedlmeir *et al.*, 2020).

In this thesis, it has been determined that Proof-of-Stake (PoS) clearly outnumbered the advantages in terms of energy consumption and ability to takeover over the Proof-of-Work (PoW) as the search space has been reduced in the Proof-of-Stake (PoS). There is still room for improvement in the PoS to reduce the required energy resources. Therefore, other consensus protocols were proposed for example Tendermint and Ripple which do not even involve the mining, saves all the energy. But despite they are saving all the energy consumption, future studies are required to analyse their possibility of being widely used as a suitable consensus mechanism.

References

Criddle, Christina (February 20, 2021) "Bitcoin consumes 'more electricity than Argentina'." BBC News.

Haber, S., & Stornetta, W. S. (1990, August). How to time-stamp a digital document. In *Conference on the Theory and Application of Cryptography* (pp. 437-455). Springer, Berlin, Heidelberg.

Szabo, N. (1998). Secure property titles with owner authority. *Online at http://szabo. best. vwh. net/securetitle. html*.

Konst, S. (2000). Secure log files based on cryptographically concatenated entries. *Technische Universitat Braunschweig*.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review*, 21260.

Nakamoto, S. (2009). Bitcoin: A peer-to-peer electronic cash system Bitcoin: A Peer-to-Peer Electronic Cash System. *Bitcoin. org. Disponible en https://bitcoin. org/en/bitcoin-paper*.

Ulieru, M. (2016). Blockchain 2.0 and beyond: Adhocracies. In *Banking beyond banks and money* (pp. 297-303). Springer, Cham.

Niranjanamurthy, M., Nithya, B. N., & Jagannatha, S. J. C. C. (2019). Analysis of Blockchain technology: pros, cons and SWOT. *Cluster Computing*, *22*(6), 14743-14757.

Malik, A., Gautam, S., Abidin, S., & Bhushan, B. (2019, July). Blockchain technology-future of IoT: including structure, limitations and various possible attacks. In *2019 2nd International Conference on Intelligent Computing, Instrumentation and Control Technologies (ICICICT)* (Vol. 1, pp. 1100-1104). IEEE.

Lu, Y. (2018). Blockchain: A survey on functions, applications and open issues. *Journal of Industrial Integration and Management*, *3*(04), 1850015.

Andreev, R. A., Andreeva, P. A., Krotov, L. N., & Krotova, E. L. (2018). Review of blockchain technology: Types of blockchain and their application. *Intellekt. Sist. Proizv.*, *16*(1), 11-14.

Maurer, U., & Wolf, S. (1997, June). The intrinsic conditional mutual information and perfect secrecy. In *Proceedings of IEEE International Symposium on Information Theory* (p. 88). IEEE.

Raikwar, M., Gligoroski, D., & Kralevska, K. (2019). SoK of used cryptography in blockchain. *IEEE Access*, *7*, 148550-148575.

Goldreich, O., & Oren, Y. (1994). Definitions and properties of zero-knowledge proof systems. *Journal of Cryptology*, *7*(1), 1-32.

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., ... & Yellick, J. (2018, April). Hyperledger fabric: a distributed operating system for permissioned blockchains. In *Proceedings of the thirteenth EuroSys conference* (pp. 1-15).

Dorri, A., Kanhere, S. S., Jurdak, R., & Gauravaram, P. (2017, March). Blockchain for IoT security and privacy: The case study of a smart home. In *2017 IEEE international conference on pervasive computing and communications workshops (PerCom workshops)* (pp. 618-623). IEEE.

Preneel, B. (1998, June). The state of cryptographic hash functions. In *School organized by the European Educational Forum* (pp. 158-182). Springer, Berlin, Heidelberg.

Wegner, P. (1996). Interoperability. *ACM Computing Surveys (CSUR)*, *28*(1), 285-287.

BIS, C. (2018). Looking Beyond the Hype. *Bank of International Settlement, Basel.*

Zhang, C., Wu, C., & Wang, X. (2020, May). Overview of Blockchain consensus mechanism. In *Proceedings of the 2020 2nd International Conference on Big Data Engineering* (pp. 7-12).

Golosova, J., & Romanovs, A. (2018, November). The advantages and disadvantages of the blockchain technology. In *2018 IEEE 6th workshop on advances in information, electronic and electrical engineering (AIEEE)* (pp. 1-6). IEEE.

Koops, D. (2018). Predicting the confirmation time of bitcoin transactions. *arXiv preprint arXiv:1809.10596*.

Gervais, A., Karame, G. O., Wüst, K., Glykantzis, V., Ritzdorf, H., & Capkun, S. (2016, October). On the security and performance of proof of work blockchains. In *Proceedings of the 2016 ACM SIGSAC conference on computer and communications security* (pp. 3-16).

King, S., & Nadal, S. (2012). Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. *self-published paper, August*, *19*(1).

Larimer, D. (2013). Transactions as proof-of-stake. *Nov-2013*

Moindrot, O., & Bournhonesque, C. (2017). Proof of stake made simple with casper. *ICME, Stanford University*.

Bentov, I., Lee, C., Mizrahi, A., & Rosenfeld, M. (2014). Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract] y. *ACM SIGMETRICS Performance Evaluation Review*, *42*(3), 34-37.

Szydlo, M. (2004, May). Merkle tree traversal in log space and time. In *International Conference on the Theory and Applications of Cryptographic Techniques* (pp. 541-554). Springer, Berlin, Heidelberg.

Dinh, T. T. A., Liu, R., Zhang, M., Chen, G., Ooi, B. C., & Wang, J. (2018). Untangling blockchain: A data processing view of blockchain systems. *IEEE transactions on knowledge and data engineering*, *30*(7), 1366-1385.

Dattani, J., & Sheth, H. (2019). Overview of blockchain technology. *Asian Journal of Convergence in Technology*, *5*(1), 1-3.

Böhme, R., Christin, N., Edelman, B., & Moore, T. (2015). Bitcoin: Economics, technology, and governance. *Journal of economic Perspectives*, *29*(2), 213-38.

Yaga, D., Mell, P., Roby, N., & Scarfone, K. (2019). Blockchain technology overview. *arXiv preprint arXiv:1906.11078*.

Foroglou, G., & Tsilidou, A. L. (2015, May). Further applications of the blockchain. In *12th student conference on managerial science and technology* (pp. 1-8).

Korpela, K., Hallikas, J., & Dahlberg, T. (2017, January). Digital supply chain transformation toward blockchain integration. In *proceedings of the 50th Hawaii international conference on system sciences*.

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

Zhang, P., White, J., Schmidt, D. C., & Lenz, G. (2017). Applying software patterns to address interoperability in blockchain-based healthcare apps. *arXiv preprint arXiv:1706.03700*.

Sedlmeir, J., Buhl, H. U., Fridgen, G., & Keller, R. (2020). The energy consumption of blockchain technology: beyond myth. *Business & Information Systems Engineering*, *62*(6), 599-608.

Vranken, H. (2017). Sustainability of bitcoin and blockchains. *Current opinion in environmental sustainability*, *28*, 1-9.

De Vries, A. (2018). Bitcoin's growing energy problem. *Joule*, *2*(5), 801-805.

Creswell, J. W. (2009). Research designs: Qualitative, quantitative, and mixed methods approaches. *Callifornia: Sage*.

Mora, C., Rollins, R. L., Taladay, K., Kantar, M. B., Chock, M. K., Shimada, M., & Franklin, E. C. (2018). Bitcoin emissions alone could push global warming above 2 C. *Nature Climate Change*, *8*(11), 931-933.

Zhang, R., & Chan, W. K. V. (2020, July). Evaluation of energy consumption in block-chains with proof of work and proof of stake. In *Journal of Physics: Conference Series* (Vol. 1584, No. 1, p. 012023). IOP Publishing.

Yoshida, H., & Biryukov, A. (2005, August). Analysis of a SHA-256 variant. In *International Workshop on Selected Areas in Cryptography* (pp. 245-260). Springer, Berlin, Heidelberg.

Valdivia, L. J., Del-Valle-Soto, C., Rodriguez, J., & Alcaraz, M. (2019). Decentralization: The failed promise of cryptocurrencies. IT Professional, 21(2), 33-40.

Velliangiri, S., & Karthikeyan, P. (2020, January). Blockchain technology: challenges and security issues in consensus algorithm. In *2020 International Conference on Computer Communication and Informatics (ICCCI)* (pp. 1-8). IEEE.

Tikhomirov, S. (2017, October). Ethereum: state of knowledge and research perspectives. In *International Symposium on Foundations and Practice of Security* (pp. 206-221). Springer, Cham.

Porat, A., Pratap, A., Shah, P., & Adkar, V. (2017). Blockchain Consensus: An analysis of Proof-of-Work and its applications.

Natoli, C., & Gramoli, V. (2016). The balance attack against proof-of-work blockchains: The R3 testbed as an example. *arXiv preprint arXiv:1612.09426*.

Vasin, P. (2014). Blackcoin's proof-of-stake protocol v2. *URL: https://blackcoin. co/blackcoin-pos-protocol-v2-whitepaper. pdf*, *71*.

Gupta, D., Saia, J., & Young, M. (2018, January). Proof of work without all the work. In *Proceedings of the 19th international conference on distributed computing and networking* (pp. 1-10).

Aljassas, H. M. A., & Sasi, S. (2019, May). Performance evaluation of proof-of-work and collatz conjecture consensus algorithms. In *2019 2nd International Conference on Computer Applications & Information Security (ICCAIS)* (pp. 1-6). IEEE.

Vashchuk, O., & Shuwar, R. (2018). Pros and cons of consensus algorithm proof of stake. Difference in the network safety in proof of work and proof of stake. *Electronics and Information Technologies*, *9*(9), 106-112.

Averin, A., Samartsev, A., & Sachenko, N. (2020, September). Review of Methods for Ensuring Anonymity and De-Anonymization in Blockchain. In *2020 International Conference Quality Management, Transport and Information Security, Information Technologies (IT&QM&IS)* (pp. 82-87). IEEE.

Li, W., Andreina, S., Bohli, J. M., & Karame, G. (2017). Securing proof-of-stake blockchain protocols. In *Data privacy management, cryptocurrencies and blockchain technology* (pp. 297-315). Springer, Cham.

Gilbert, H., & Handschuh, H. (2003, August). Security analysis of SHA-256 and sisters. In *International workshop on selected areas in cryptography* (pp. 175-193). Springer, Berlin, Heidelberg.

Sriman, B., Ganesh Kumar, S., & Shamili, P. (2021). Blockchain technology: Consensus protocol proof of work and proof of stake. In *Intelligent Computing and Applications* (pp. 395-406). Springer, Singapore.

Zheng, Z., Xie, S., Dai, H. N., Chen, X., & Wang, H. (2018). Blockchain challenges and opportunities: A survey. *International journal of web and grid services*, *14*(4), 352-375.

Monrat, A. A., Schelén, O., & Andersson, K. (2019). A survey of blockchain from the perspectives of applications, challenges, and opportunities. *IEEE Access*, *7*, 117134-117151.

Dresch, A., Lacerda, D. P., & Antunes, J. A. V. (2015). Design science research. In *Design science research* (pp. 67-102). Springer, Cham.

Chi, L., & Zhu, X. (2017). Hashing techniques: A survey and taxonomy. *ACM Computing Surveys (CSUR)*, *50*(1), 1-36.

Nguyen, C. T., Hoang, D. T., Nguyen, D. N., Niyato, D., Nguyen, H. T., & Dutkiewicz, E. (2019). Proof-of-stake consensus mechanisms for future blockchain networks: fundamentals, applications and opportunities. *IEEE Access*, *7*, 85727-85745.

Moser, S., & Kleinhückelkotten, S. (2018). Good intents, but low impacts: diverging importance of motivational and socioeconomic determinants explaining pro-environmental behavior, energy use, and carbon footprint. *Environment and behavior*, *50*(6), 626-656.