TALLINN UNIVERSITY OF TECHNOLOGY
School of Information Technology
Cybersecurity

Deniz Basar 177238IVCM

Uniqueness Criteria for Blockchain Type Distributed Ledgers

Master's thesis

Supervisor: Prof. Dr. Ahto Buldas

Tallinn 2020

TALLINNA TEHNIKAÜLIKOOL
Infotehnoloogia Teaduskond
Küberturvalisus

Deniz Basar 177238IVCM

Plokiahela Tüüpi Hajusraamatute Unikaalsuskriteeriumid

Magistritöö

Juhendaja: Prof. Dr. Ahto Buldas

Tallinn 2020

Author's declaration of originality

I hereby certify that I am the sole author of this thesis. All the used materials, references to the literature and the work of others have been referred to. This thesis has not been presented for examination anywhere else.

Author: Deniz Basar

January 2, 2020

Autorideklaratsioon

Olen koostanud antud töö iseseisvalt. Kõik töö koostamisel kasutatud teiste autorite tööd, olulised seisukohad, kirjandusallikatest ja mujalt pärinevad andmed on viidatud. Käesolevat tööd ei ole varem esitatud kaitsmisele kusagil mujal.

Autor: Deniz Basar

Jaanuar 2, 2019

Abstract

One of the most important features required from blockchain type distributed ledger technologies is their verifiable uniqueness, i.e. the verifier (observer) of the ledger has to be convinced that the version of the ledger it sees is and stays the same for all potential verifiers. For example, the Bitcoin ledger is believed to be one, single, valid, and unique, because the PoW blockchain consensus protocol mechanism enables verifiers to calculate the total amount of electirical energy required to create the ledger on the blockchain system. Comparing this necessary electrical energy with the total available electrical energy resources of all around the world, the observer can be convinced that creating of parallel alternative versions of the ledger would cost so much. This research studies the uniqueness condition criterias of blockchain type distributed ledger technologies that are based on various different (apart from PoW,) blockchain consensus protocols. For every blockchain type distributed ledger technology, author explains the simple work principle at first and then regarding to the fundamental basic work principle of each blockchain type distributed ledger technology, author figures out the uniqueness conditions againt both alternative branches and block extensions that are existing on the ledger as well as describes the real world physical required measurements that are necessary to verify the uniqueness of the ledger. Furthermore, some relevant possible attacks are discussed and handled for each blockchain consensus protocols. In essence, the work is definitely not a literature review, but an analytical research that are mostly based on conference papers, journal articles, technical reports, whitepapers and relevant websites of the different blockchain systems. At the same time, many necessary assumptions are not just extracted from the cited whitepapers and websites of the different blockchain consensus protocols, but have been deduced by the author based on all other available book sections and electronic materials. The final evaluated results are summarized in concluding table.

This thesis is written in English and is 84 pages long, including 6 chapters, 6 figures and 1 table.

Annotatsioon

Üks hajusraamatutelt nõutavaid tähtsamaid nõutud omadusi on nende verifitseeritav unikaalsus, st arvestusraamatu verifitseerija (vaatleja) peab lõpuks olema veendunud, et see versioon arvestusraamatust, mida ta näeb, on ja jääb samaks kõigile potentsiaalseile vaatlejaile. Näiteks Bitcoini arvestusraamatus kasutatav töötõenduse mehhanism võimaldab arvestusraamatu verifitseerijal välja arvutada arvestusraamatu loomiseks kulunud energiahulga. Võrreldes seda energiahulka maailmas toodetava energiahulgaga võib arvestusraamatu verifitseerijat veenda selles, et paralleelse alternatiivse arvestusraamatu loomine oleks liiga kulukas.

Selles magistritöös uuritakse paljude, (töötõendusest) erinevatel konsensusmehhanismidel põhinevate hajusraamatute unikaalsuskriteeriume. Iga hajusraamatu tüübi jaoks selgitatakse välja vajalikud korrektselt verifitseeruva arvestusraamatu unikaalsust tagavad eeldused maailma kohta ja samuti kirjeldatakse nende eelduste kehtivuse verifitseerimiseks vajalikke füüsikalisi mõõtmisi, juhul kui tehtud eeldused üldse on verifitseeritavad.

Töös kasutatud infoallikad on lisaks teadusartiklitele ka paljud hajusraamatulahendusi kirjeldavad veebilehed. Paljud vajalikud eeldused ei ole lihtsalt ekstraheeritud viidatud allikatest vaid on töö autori poolt tuletatud, kasutades kõiki kättesaadavaid materjale. Töö tulemused on summeeritud kokkuvõtvas tabelis.

Lõputöö on kirjutatud inglise keeles ning sisaldab teksti 84 leheküljel, 6 peatükki, 6 joonist, 1 table.

Acronyms

BGP Border Gateway Protocol. 38

dBFT Delegated Byzantine Fault Tolerance. 13, 79–82, 88

DoS Denial of Service. 42

DPoS Delegated Proof of Stake. 9, 10, 44–47, 88

DSA Digital Signature Algorithm. 21

ECDSA Elliptical Curve Digital Signature Algorithm. 21

pBFT Practical Byzantine Fault Tolerance. 10, 50–53, 80

PoA Proof of Authority. 12, 13, 75–78

PoB Proof of Burn. 12, 68, 70–72

PoC Proof of Capacity. 10, 18, 47–50, 88

PoH Proof of History. 13, 82–84, 88

PoI Proof of Importance. 11, 58–61, 63, 88

PoR Proof of Reputation. 12, 72–75, 88

PoS Proof of Stake. 9, 38–42, 44, 45, 58, 62, 66, 85, 88

PoST Proof of Stake Time. 11, 12, 65–68

PoSV Proof of Stake Velocity. 11, 62–66

PoW Proof of Work. 3, 9, 18, 19, 25, 33–37, 39, 40, 42, 48, 50, 59, 69, 88

PoWeight Proof of Weight. 13, 14, 84–88

RAM Random Access Memory. 43

RPCA Ripple Protocol Consensus Algorithm. 10, 11, 53–58

RSA Rivest Shamir Adleman. 21

UNL Unique Node List. 54–58

List of terms and explanations

blockchain A data structure that consists of successive data blocks. After a fixed time period each new block is created or a block can also be created as a result of some other event, such as successful mining [3]. 3, 8, 9, 15–19, 21, 27–30, 33, 34, 36–44, 46–53, 55–58, 60–82, 84, 86

blockchain as a service Implementing traditional TCP/IP applications to enterprises using blockchain technology. 76

blockchain system Set of blockchain users and operators connected by network in order to make up blockchain. 3, 8, 14–21, 23, 27–31, 33, 35–38, 40–42, 44–89

byzantine/arbitrary failure Blockchain users and operators in a blockchain system may produce arbitrary responses, irregular behaviors, and perform malicious activities intentionally at any time. 23, 55

consensus protocol A consensus protocol between the operators is required in order to ensure the consistency among all the copies of the ledger [3]. 3, 14, 15, 18, 19, 21, 27, 30–34, 36–42, 44, 46, 47, 49–52, 55–58, 60–62, 64, 65, 67, 68, 71, 72, 74, 75, 77–79, 81, 82, 84, 86, 88

cryptocurrency A digital asset developed by using strong cryptography in order for exchange. 16, 39–43, 45–47, 54, 58–71, 85–88

cryptographic hash function Appeared in the 1970s in relation to the works of Merkle [46], Rabin [54], Yuval [68], and others. 30, 33, 34, 39, 44, 48, 51, 53, 58, 62, 66, 69, 76, 79, 82–84

cryptographic primitives Cryptographic algorithms, which are used to build up cryptographic protocols in order to have secure computer systems. 15–17, 29, 30, 33

difficulty Showing difficulty level about finding a cryptographic hash that will be lower than the target defined by the blokchain system. 34, 35

digital signatures Digital signatures of people authorised in some way (with public keys) [3]. 30, 33

distributed ledger technology A ledger technology, which contains multiple ledger operators. Entries sent by users are independently received, directly or indirectly by all operators managing the Ledger [3]. 3, 15, 17, 51

encryption Taking readable data as input and altering it to unreadable as output. 30, 33, 34, 39, 44, 48, 51, 53, 58, 69, 79, 82, 84

ledger An electronic document constantly used to record the events of informational, commercial, or legal significance [3]. 3, 8, 15–20, 23, 27, 28, 30–33, 35–37, 40–43, 45–57, 59–61, 63–68, 70, 71, 73–78, 80–88, 90

merkle tree Binary hash tree appeared in the 1979 by R. C. Merkle [46, 47]. 34

nonce A number only used once and added in the blockchain header. 34, 35, 48

peer-to-peer network Interconnected nodes (peers) without the centralized authority. In other words, there are computers that use and share their computing power, data storage, or network bandwidth etc. between each other. 16, 38

private blockchain Provision of services is distributed between a number of fixed actors acting on a contractual or other legal basis [3]. 73, 76, 78

private key A very large numerical value known only by the owner to decrypt data. 34, 39, 69

public blockchain Service providers are not fixed and in principle, anyone can start operating the service [3]. 34, 82

timestamp Appeared in the 1990s in relation to the works of Haber, Bayer, and Stornetta [7]. 34, 43, 83, 88

Contents

List of Figures

List of Tables

1 Introduction

Distributed ledger technology is a consensus of replicated, shared, and synchronized digital data, which geographically spreads across multiple sites, countries, or institutions. One of its main advantages of distributed ledger technology is that there is no central administrator and centralized data storage. All nodes in the system must hold identical copies of the ledger. All nodes have to update themselves with the new, correct copy of the ledger once a consensus has been determined. Thereby, after the update of the correct copy of the ledger is done properly, then there can be only one, single, valid, and unique ledger in every node in the system. Security in a distributed ledger technology is accomplished through cryptographic primitives and blockchain system is one form of distributed ledger technology.

The main goal of this research is to understand and figure out with what conditions and under which assumptions a blockchain type distributed ledger technology provides a one, single, valid, and unique ledger in the blockchain system.

The meaning by the uniqueness of the ledger is that there should not be either an alternative version of the original ledger or extended blocks on the original ledger on the blockchain system in the entire world. Only one, single, valid, and unique ledger should be seen from outside of the blockchain system by public. Cybersecurity related specific technical requirements are usually based on cryptographic primitives. When one or some of the cryptographic primitives are broken, they might end up with local compromise of the blocks, stolen private keys, accounts, financial loss, and so on.

In this thesis, only the global effect of broken cryptographic primitives, one of which is violation of the uniqueness is handled and analyzed. Local effects of compromised blockchain systems were not taken into account in terms of uniquness. Why the uniqueness of the ledger is important is that because this is the most basic, fundamental non-functional system design requirement of all blockchain consensus protocols and it is related to the global/entire security of the blockchain type distributed ledger technologies.

1.1 Blockchain History

During the United States origin big global financial crisis in 2008, some banks collapsed, some insurance companies lost a lot of money in the stock markets in all around the world, and the trust of nation-based currencies such as US dollar decreased significantly as a result. The consequence of that big economic crisis in all around the world forced people to think that there might be necessity to have such a currency that is not under control of

any central authority, government, and/or their public and private sector partners as well. Therefore, an unknown person or a group of people called "Satoshi Nakamoto" presented a cryptocurrency called Bitcoin.

The main idea behind of Bitcoin is that there will be a decentralized digital asset (cryptocurrency) without a central bank, which means that without the need for intermediaries, that allows money transactions from one user to another on the peer-to-peer network since it was shown that one of the main and important reasons of the big economic crisis was related to the intermediaries of the loan-chain, which basically indicated the relation between people, banks, insurance companies, and stock markets. Therefore, they decided to develop the first blockchain database, the main technology underlying Bitcoin as a part of the implementation. [14]

Bitcoin was released by Satoshi Nakamoto as an open-source software in 2009. Transactions are going to be verified by a special network node called miner using cryptographic primitives. Furthermore, transactions are going to be recorded in a ledger, so that the records cannot be changed backswept without the consensus of the blockchain system. After a while, many people started to think that this decentralized peer-to-peer network with no central authority provides cheaper, faster, and safer money transactions around the world and the decentralized peer-to-peer network blockchain technology can also be implemented not just to cryptocurrencies but to any kind of centralized applications running on the existing network as well.

1.2 Research Motivation

The overall security concepts of blockchain type distributed ledger technology are not systematically covered in the literature. The main focus in the literature is mostly on specific technical requirements and this seems to lead the community towards insufficient security arguments. For example, there is a widespread belief that Bitcoin is "secure" as long as the majority of its users and miners are honest. Even though there are many proposed distributed ledger technology solutions, where many different "security measures" have been used, there is no research that systematically analyzes and discusses the most important and fundamental non-functional system design requirements. Uniqueness of the ledger is one of the most important and fundamental non-functional system design requirements in a blockchain system. The inherent complexity of blockchain consensus protocols and their immediate, fast, and dramatic evolution make the analysis and evaluations harder. However, this study addresses this challenge by conducting the fundamental work knowledge of each different blockchain consensus protocols. After first discussing key working principles in each different blockchain consensus protocols, the study describes: (i) variables based on working principle of each different blockchain consensus protocols;

(ii) specify the unique ledger condition criterias using the pre-defined variables for each different blockchain consensus protocols; (iii) emphasize what sort of physical necessary measurements and observations should be done from the real world to verify the pre-defined uniqueness conditions; and (iv) cover some of the relevant potantial attack types against each different blockchain consensus protocol.

1.3 Scope of Research

The most fundamental security question of blockchains, namely the verifiable uniqueness is the only scope and main focus of this research. In other words, instead of local compromise related security issues in a blockchain system, the global security conditions of the blockchain systems were analyzed and discussed. For example, it was assumed that the cryptographic primitives that are used in the blockchain systems are sufficiently secure not to cause global effects, such as uniqueness violation or destruction of the whole blockchain system. This research is guided by a systematization framework that was developed to highlight the uniquness of various blockchain consensus protocols, along with a discussion on their necessary physical measurements and observations from the real world. Therefore, the research gaps were identified in the current state of art and insights for the community to consider in future research endeavours.

1.4 Research Questions

The following research questions are to be answered:

1. What is the uniqueness of ledger?
2. What are the possible uniqueness violation situations on the ledger?
3. Under which assumptions and with what conditions a blockchain consensus protocol can provide a one, single, valid, and unique ledger in the blockchain system?
4. Can these uniqueness conditions be verified?
5. In addition to verifying the correctness (syntax and semantics) of the ledger, is it necessary to make some physical measurements and observations from the real world?
6. What are the potential attacks against each of different blockchain systems?

1.5 Outcomes of the Research

Apart from PoW type blockchain consensus protocol, fourteen different blockchain consensus protocols are studied and determined with the assumptions and conditions under which the ledgers produced by these blockchain consensus protocols would be unique. The necessary real world measurability of the assumptions and conditions are handled and discussed. It turned out that the ledgers based on PoW and PoC are, at least in principle, verifiable. However, their necessary uniqueness conditions tend not hold for the real world implementations of these types of blockchains.

The uniqueness conditions of almost all other types of blockchain consensus protocols contain adversarial parameters that are not measurable in the real world, at least it could not be imagined that any measurement techniques to determine these parameters. In practice, this means there may be other types of reasons why one can assume that these unmeasurable assumptions hold. For example, the reasons may be social-science oriented or coming from economic arguments such as economical infeasibility of launching an attack. The security of the implementations of most blockchain consensus protocols certainly depends on socio-technical arguments. Hence, the blockchains' "100% security guarantee" only applies under some physically unmeasurable socio-technical assumptions.

1.6 Research Gaps

There is no research that systematically describes what the uniqueness of the ledger concretely means in a blockchain system. In addition, there are few papers that have analyzed blockchain consensus protocols in terms of tolerated power of adversaries. However, these studies do not provide any detailed systematic anaylsis, but just consequences that are irrelavant for some cases as in Proof of Work (PoW), for example. Furthermore, there is no such research that discusses fifteen different blockchain consensus protocols at the same time. Therefore, a comprehensive logical approach was derived to fulfill the expectations and gaps of the nearest future academic studies.

1.7 Novelty of the Research

This research is the first study that analyzes and explains the uniqueness of the ledger as the most important and fundamental non-functional system design requirement in a systematic way and combines the unique ledger threshold condition criterias along with necessary physical measurements and observations from the real world, while deciding the uniqueness of the ledger. Furthermore, it is the most comprehensive research that

handles fifteen different blockchain consensus protocols at the same time with possible attack types in one research.

1.8 Methodology

This research is an analytical research based on mainly academic studies. For the accomplishment of this research some conference papers, journal articles, technical reports, and whitepapers of the relevant blockchain systems were consulted. In addition, book sections, electronic materials, and many techical websites/forums were also taken into consideration as supportive.

1.9 Limitations of the Research

The lack of the implementation of all the built up theoretical logic to practice may make the possible outcomes and consequences of the research unreliable. In addition, the lack of academic studies that have similar approaches in terms of uniqueness of the ledger makes the anaylsis harder and more challenge.

1.10 Structure of the Thesis

The thesis is organized as follows: Having given an introduction into the topic in chapter 1. In chapter 2, proceeding with the explanations about blockchain background, system design requirements, and consensus are presented. Uniquness of the ledger in blockchain system is given in chapter 3. In chapter 4 with subchapters, particular blockchain consensus protocols in terms of their fundamental work principle are handled and explained. Their unique ledger conditions are analyzed and discussed along with their necessary measurements that need to be done from the real world. Possible attack types against each blockchain consensus protocol are pointed and mentioned briefly. Conclusions are summarized in chapter 5 with a conclusion table. The description of the conclusion table is explained in chapter 6.

2 Blockchain Background

2.1 General Description of a Blockchain System

A blockchain system should consist of the following components/parties at least: [3, 50, 69]

- **Users**: People or entities that are usually identified by their public key mostly associated with digital signatures, such as RSA, DSA, ECDSA (generally also known as account number) etc. in the ledger and able to add entries to the ledger.
- **Operators**: People, who can only accept items from the users and add them to the ledger with respect to the meeting format. In other words, they are responsible for the operation, maintenance, and the validity of the ledger.

Ledgers in blockchain technology are created block by block according to the following fundamental steps: [70, 67, 53]

- Users send the operators the entries that they have added to the ledger.
- The operators check the incoming entries, if they are in valid format.
- The operators verify the valid entries.
- The operators choose stored valid entries and combine them in a block.
- The operators finally add the formed block to the ledger.

Nodes are special computers in the blokchain system. All copies of the ledger should be passed through the entire nodes by the relevant consensus protocol properly.

2.2 Systems Design Requirements

There are two main requirements in Systems Design Engineering as follows: Functional and Non-Functional.

In terms of the needs of business and end users, these requirements describe the features that the system has to meet [26, 41].

I. Functional Requirements

Functional Requirements are also known as software requirements specification. They determine what a system should do or what should not do. In a particular system, they also describe what specific functions are needed to be implemented. In order to interact with the systems software, they describe what kind of proper actions that the users have to take.

II. Non-Functional Requirements

Non-Functional Requirements are also known as product quality attributes, but not specific functions or behaviors. They indicate how the system will work and explain what for.

Here are some of the system quality features listed as follows: [27, 93]

- **Availability:** Requirements for the application running continuously.
- **Reliability:** Behaviors of the application in case of failure.
- **Scalability:** Ways about extending the system by avoiding performance issues.
- **Performance:** How many users can perform simultaneous or transactions the system can service at the same time.
- **Security:** Application security and safety requirements. Such as access control, processing private data, and so on.
- **Usability:** How easy to use for the application. In other words, it describes how user-friendly the application usage is.

Uniqueness of the ledger is one of the non-functional requirements in the blockchain systems. It is directly related to the entire, whole security of the ledger. There is no systematic studies about the uniqueness criteria in blockchain systems are known and it is a big research gap in the literature. That is why the author focuses on it.

2.3 Consensus Protocols

After the operators finally add the verified block to the ledger, it is needed to be ensured that all copies of the ledger are spread through the entire nodes properly. That is why

a **consensus protocol** between the operators are required to ensure consistency of the ledger in entire blockchain system [6, 12, 28].

There are two different forms for reaching consensus: Byzantine Consensus and Nakamoto Consensus [48, 51].

2.3.1 Byzantine Consensus

Let $B_1, B_2, ...B_t$ be the blocks of the ledger at moment t.

If $B_1, B_2, ...B_t$ blocks are agreed among the operators (Figure 1), then the next block (B_{t+1}) should be agreed between the operator after the moment t [3].

In overall, there must be (3f + 1) nodes at least, if there are f adversaries in the block system. In other words,

$$f \leq \frac{n-1}{3}$$

where, f is the total number of nodes with byzantine/arbitrary failure and n is the total number of nodes in the network [24, 39, 21, 40].

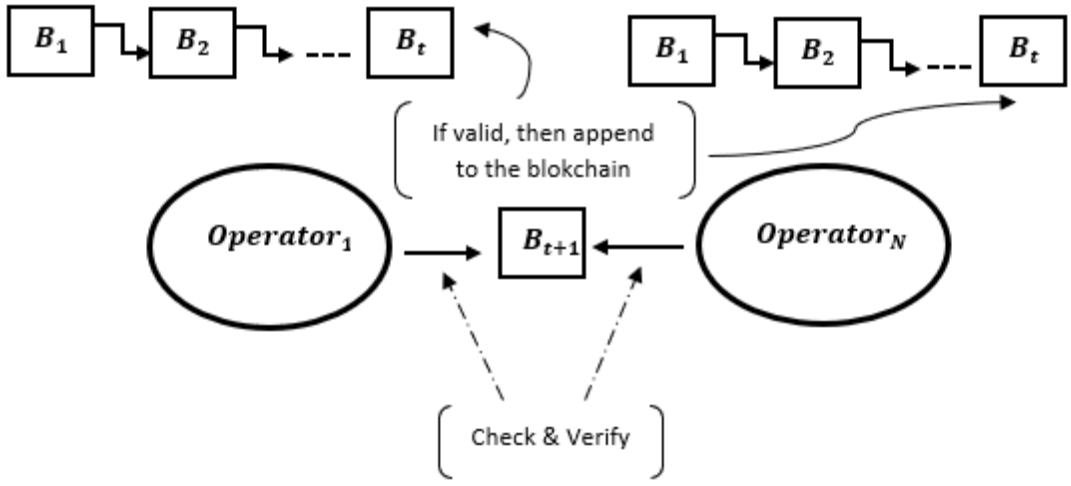

Figure 1: Illustration of Byzantine consensus

Therefore, in order to increase the resistance against faulty adversaries, by the way of its design principle, it is needed to have a very sufficiently large number n operators that

are functioning properly in order to reach a consensus on the same version of block B_{t+1}. However, the main obstacle of Byzantine consensus is that before the new block creation, Byzantine consensus protocol has to be accomplished among the operators necessarily. That is why, it may usually get stuck, so that it can disrupt and even cause the entire ledger management collapse. [22, 23, 9]

2.3.2 Nakamoto Consensus

Let $B_1, B_2, ...B_t$ be the blocks of the ledger at moment t in an operator.

Let $B'_1, B'_2, ...B'_{t'}$ be the blocks of the ledger at moment t in another operator.

If there are two chains such as $B_1, B_2, ...B_t$ and $B'_1, B'_2, ...B'_{t'}$ (Figure 2), then the longer chain should be agreed and prefered between the operators at the moment t in PoW type blockchain consensus protocol like Bitcoin [3].

As there is comparison of the chains and is not synchronised $B_1, B_2, ...B_t$ blocks among the operators, if there encounters a poor network connection in the blockchain system, Nakamoto consensus based blockchain consensus protocols may be much more reliable than Byzantine consensus based blockchain consensus protocols [11, 60].

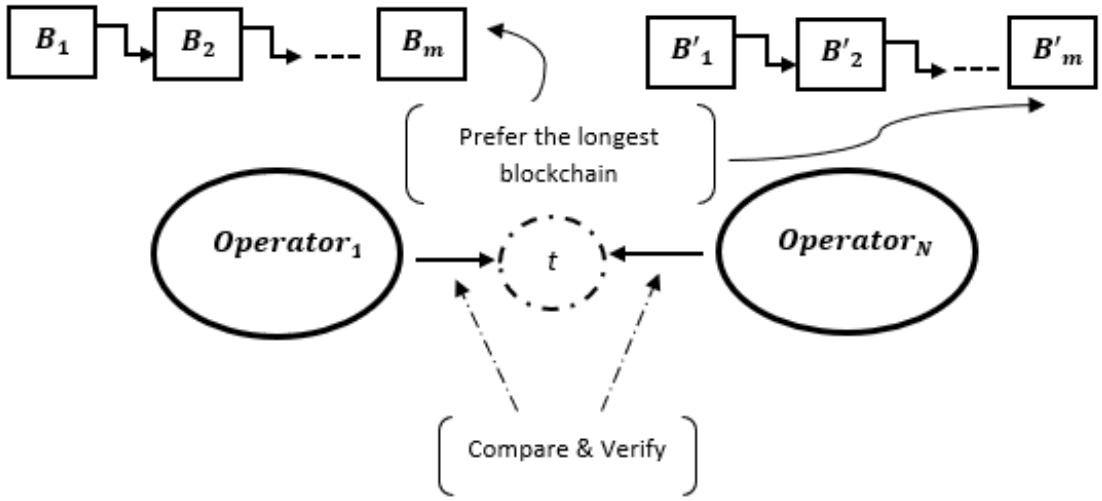

Figure 2: Illustration of Nakomoto consensus

While creating blockchain, the main and fundamental purpose of the Nakamoto consensus

is that it tries to reach and arrive such a situation, where all the operators that are functioning properly have the same initial segments of blocks such as $B_1, B_2, ...B'_{t'}$ at time $t \leq t'$. However, they may have such a situation that block B_t contains such transaction r, but the block B'_t winning later may not be able to contain the transaction r. In other words, there may exist such a case, where some recently added transactions might be dropped from the ledger. [62, 58]

3 Ledger Uniqueness in Blockchain Systems

3.1 Uniqueness Description

The meaning of uniqueness criteria for the ledger in the blockchain system is that it simply describes and explains the situation where and how a blockchain consensus protocol provides a one, single, valid, and unique ledger. In other words, it includes and explains the threshold conditions for the ledger in the blockchain system along with relative assumptions, necessary measurements and observations from the real world.

Therefore, there may exist two different situations in terms of uniqueness violation as follows: Alternative branch and blockchain extension.

3.1.1 Alternative Branch

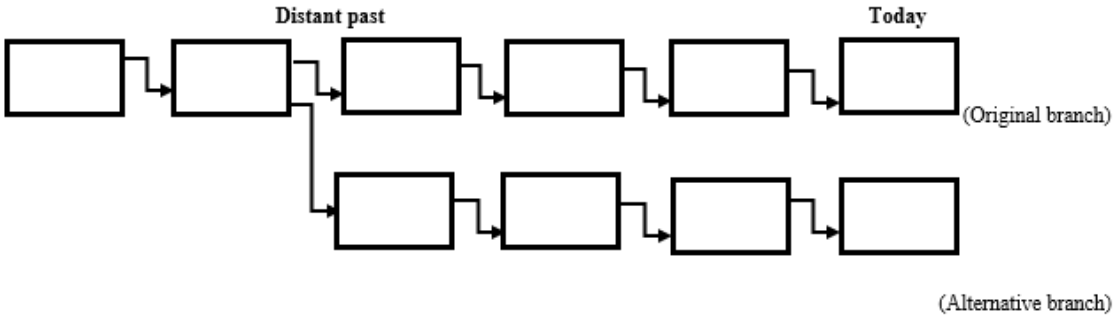

Figure 3: Creating alternative branch for uniqueness violation

A blockchain system can contain one or some of ledgers that existed distant in the past (Figure 3) and they have been still existing up to now. In other words, there may exist an alternative branch or branches of the original branch in the blockchain system. Such

a situation must be avoided in all blockchain systems in order to establish the unique ledger.

3.1.2 Blockchain Extension

A blockchain system can contain one of some of extended blocks on ledger. In other words, there may exist an extension of blocks (Figure 4) on the original branch in the blockchain system. Such a situation must be avoided in all blockchain systems in order to establish the unique ledger.

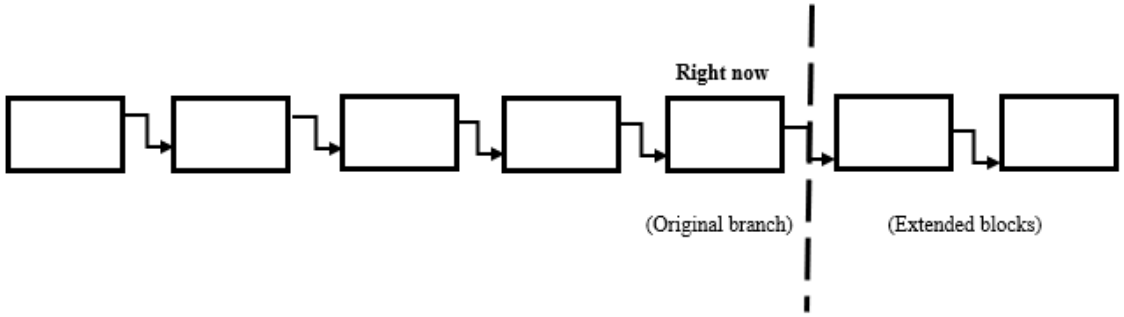

Figure 4: Creating extended blocks for uniqueness violation

3.2 Threats to Uniqueness

Every blockchain system uses some cryptographic primitives depending on their design specifications. It is only considered that the global effect or entire security of the blockchain system, which means that there must be one, single, valid, unique blockchain should be seen by the blockchain nodes is taken into account in this research. The breakage of cryptographic primitives are important and must be evaluated, when they have a global effect that threatens the uniqueness of ledger. However, it is strongly assumed that cryptographic primitives such as cryptographic hash functions, digital signatures, and encryption etc. are powerful and secure enough not to be broken in order to cause global effects for the uniqueness of the ledger in terms of alternative branching and block extensions on a blockchain system.

Figure 5: Threat landscape and possible effects of broken consensus protocol

In addition, the breakage of cryptographic primitives can cause local effects (Figure 5) such as stolen compromised accounts, financial loss, and so on. However, any effects of broken cryptographic primitives are not handled to be evaluated in the thesis. Thereby, the proposed idea for the uniqueness of ledger in blockchain systems is mainly and fundamentally related (bold straight arrows in Figure 5) to the broken properties of blockchain consensus protocol.

3.3 Uniqueness Verification

The uniqueness of the ledger describes a ledger that is one, single, valid, and unique in the blockchain system. However, it is necessary to be ensured that the uniqueness of the

ledger is verifiable. Verifier/observer is either user or operator in the blockchain system. The consensus protocol is taken into account with respect to necessary measurements and observations that are needed to be done physically from the real world environment. Assumptions are relative and applied on both consensus protocol and necessary measurements and observations. To reduce the wrong consequences of weak assumptions, the fundamental logic of uniqueness of the ledger is derived from the basic and general work principle of the consensus protocols.

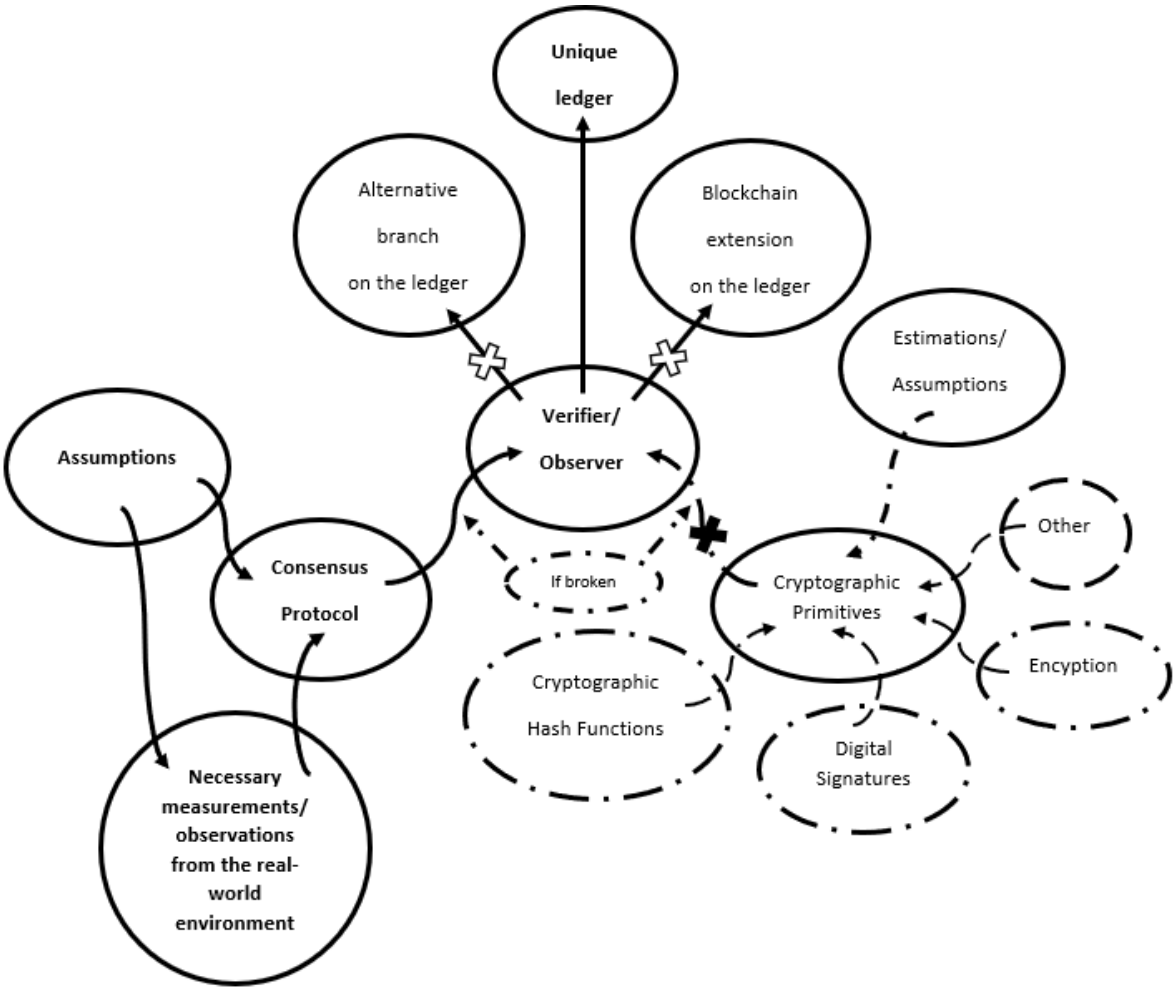

Figure 6: Effects and possible results of uniqueness verification.

As being told and emphasized before, cryptographic primitives such as cryptographic hash functions, digital signatures, and encryption etc. are estimated that they are powerful and secure enough not to be broken in order to cause global effects for the uniqueness of the ledger. In other words, the verifier/observer does not consider (black cross in Figure

6) the effects of broken cryptographic primitives. In addition, it excludes (white cross in Figure 6) the results of alternative branching and blockchain extension on the ledger by only focusing the result of unique ledger in the blockchain system. Every blockchain has its own uniqueness threshold properties that indicate the conditions (bold straight arrows in Figure 6) that have to be satisfied for (together with the assumptions and necessary measurements and observations from the real world environment) the blockchain being provably unique.

4 Studies of Blockchain Consensus protocols

Description and simple work principle of the most commonly used blockchain consensus protocols by choosing a sample cryptocurrency are described briefly. The uniqueness threshold criterias in terms of both situations "having alternative branches" and "extended blocks" in the blockchain system are handled, analyzed, and explained. In other words, under which conditions, the relevant blockchain consensus protocol can have a one, single, valid, and unique ledger in the blockchain system. Furthermore, what necassary physical measurements and observations should be done from real world enviroment are emphasized in order to verify the uniqueness of ledger in the blockchain system. Moreover, possible attacking types for each blockchain system are covered as well.

4.1 Proof of Work (PoW)

A sample blockchain system that is chosen while explaining the fundamental work principle of PoW type blockchain consensus protocol is Bitcoin. However, other PoW based cryptocurrencies also have a lot of similaries in terms of their fundamental work principles.

4.1.1 General Information

An open-source code peer-to-peer "Electronic Cash System" released on October 2008. It was known that it has been implemented by an unknown person or a group of people called Satoshi Nakamoto. However, it was reported on 21 May 2019 22:53 GMT+3 that Craig Wright is the inventor of Bitcoin [78]. Bitcoin is a public blockchain and cryptographic hash function, which is used in Bitcoin is SHA256. In Bitcoin, private key is a 256-bit and encryption is governed by the secp256k1 ECDSA standard used by Bitcoin. Number of blocks needed and considered to be secure in Bitcoin blockchain is 6 blocks, which means that the average time for finality is 1 hour. Finality points out the final version of the

blockchain that must be ensured by the miners. In other words, the required number of blocks that are needed for block confirmations are 6 blocks in Bitcoin. Block mining reward halves every 210,000 blocks and the coin reward will decrease from 12.5 to 6.25 coins at 24 May 2020 12:35:56. That means a new block is created and gets added to the Bitcoin blockchain in every 10 minutes in average [49]. In other words, the interval between subsequent block creation is approximately 10 minutes.

4.1.2 Fundamental Work Principle

There are special nodes called miners in PoW type blockchain consensus protocol. New transactions digitally signed are broadcasted to all miners. Each miner collects new transactions and combine them into a block. A block consists of two parts. Block header and data.

A. Block header contains the followings: [49]

- block version number (80 bytes),
- hash of the previous block header (256 bits),
- merkle tree root (256 bits) [47],
- timestamp (32 bits) [31],
- current difficulty target (256 bits),
- nonce (32 bits)

B. Data contains all the confirmed transactions.

Each node tries to produce PoW by incrementing the nonce value in the block header until a value is found that gives the block's hash the required zero bits (68-bit). In other words, miners keep generating the nonce value until they find the valid nonce value.

A block is valid if and only if the transactions inside of the block are valid and confirmed. The nonce is only actual for the current valid block. It cannot be reused again for another block. If the miners see that the block is valid, but the nonce is not actual, then it gets rejected. If the miners see that the block is not valid, but the nonce is actual, then it also gets rejected. Only the combination of a valid block and the nonce are accepted by the miners. When a miner finds the actual nonce, the block is broadcasted to all the other miners. While miners work on creating the next block in the blockchain using the

hash of the accepted block as the previous hash, they express the acceptance of the block. There may be a special case that if two or more miners broadcast different versions of the next valid block simultaneously and some miners may receive one or the other first. If such kind of case exists, then miners work on the first one they receive but they save the other branch in any case it becomes longer. Only the miner, who first generates the actual nonce for the valid block is rewarded. If blocks are generated so fast, the current difficulty of target is increased by the blockchain system. [49]

4.1.3 Uniqueness Threshold in PoW

Two variables N and T are described in order to decide uniqueness against alternative branches of the ledger in the PoW blockchain system.

Let **N** be the total amount of electrical energy available in the world.

Let **T** be the total electrical energy consumed by miners for creating the PoW.

Therefore, the theoretical uniqueness threshold condition can be formulated as follows:

$$T > \frac{N}{2} \tag{1}$$

This is the uniqueness threshold condition criteria for the prevension of having alternative branches on the ledger in the PoW blockchain systems. In other words, total electrical energy consumed by miners for creating the PoW should be greater than the half of the total amount of electrical energy available in the world in order not to have alternative branches on blockchain.

The intuition behind this reasoning is that PoW blockchain systems are public blockchains. That basically means that there is no central authority permission needed for being a miner. In other words, as long as people, who can have enough resources in terms of electrical energy consumption to create the PoW can be miners. Therefore, being thought while deciding the limitations/borders of the assumptions, it is needed to be decided and covered the extreme case, where the electrical energy that may be used on PoW blockchain system could exceeed the level now and reach to the total electrical energy available in the world. That is why, the miners should be able to control more than half of the total electrical energy available in the world in order to theoretically imply the uniqueness of the ledger in the PoW blockchain system.

In terms of uniqueness for the prevension of having block extension on the ledger, PoW

blockchain systems promise to create 1 block per 10 minutes in average. In addition, it promises number of blocks needed for block confirmation, which are 6 blocks. Therefore, by looking at the promised block creation time and number of blocks needed for block finalization, it can be estimated and accepted that PoW blockchain system can fully perform uniqueness against block extension on the ledger.

The intuition behind this reasoning is that interval between subsequent block creation might be used to provide reliability for each of the miners in the PoW blockchain system that every miner will be able to believe when a new block will be added to the blockchain. When there becomes such a blockchain extension situation, if the miners know in advance about when exactly a new block should be created and appended to the blockchain, there will not be any confusion, so that block extension created by the violated miners would be ignored and dropped. In terms of minimal number of blocks, required for block confirmation might be used to provide certainty at some point that even though blockchain extension occurs, the miners would be able to make sure about which blockchain is securer than the other (the longer, the securer in PoW). In other words, it might be called as indirect prevension mechanism against blockchain extension.

4.1.4 Necessary Measurements for Uniqueness in PoW

Beside theoretical uniqueness threshold condition described by N and T variables, the research also describes what necessary real world measurements and observations need to be done along with specifying their measurabilities in order to finalize the expression of verifiable uniqueness in PoW based blockchain consensus protocols.

Measurability of Determining N: It is needed to determine the total amount of electrical energy existing in the world. Total amount of electrical energy is large, but it can be measurable.

Measurability of Determining T: T can be computed based on the ledger by analyzing the strength of PoW. That is why T is measurable.

4.1.5 Uniqueness of Ledger in PoW

Regarding to the theoretical uniqueness threshold criteria and the necessary physical real world measurements and observations of N and T variables, as a result, it can be concluded that PoW type blockchain consensus protocol provides the uniqueness of ledger against having alternative branches on the ledger as long as miners consume more than 50% of the total electrical energy available in the world, so that at that time it can be claimed

that PoW type blockchain system provides verifiable uniqueness. In other words, only under the condition described in the formula (1) with the necessary physical real world measurements and observations, it can be told that there is only one, single, valid, and unique ledger in entire PoW type blockchain system. In addition, PoW type blockchain system promises full prevention for block extention on the ledger by the estimated block creation time in average and the number of blocks needed for confirmation.

4.1.6 Potential Attacks against Uniqueness in PoW

51% Attack

That type of attack explains the ability of the adversaries, who want to take the control of the majority of network using hash rate in order to revise transaction back in the history in addition to preventing to confirm new transactions. [81]

A successful 51% attack; [79] Around 1.4 billion $ would cost. 5 million specialized ASIC mining computers would be needed. Almost 29 terawatt hours of electricity would be consumed per year (Almost entire country-Morocco).

Four main attacks, as potential results of the 51% attack are as follows: [83]

1. **Selfish Mining:** Without letting the blockchain system recognize, collecting all the mining rewards and transaction fees by mining on top of blocks.
2. **Cancelling Transactions:** Rejecting any transactions into any of the blocks.
3. **Double Spending:** Spending the same coin on more once.
4. **Random Forks:** Getting the exact amount of cryptocurrency in the newly forked block.

Hijacking Attack

Manipulating Bitcoin traffic by either intercepting traffic, Autonomous Systems (ASes) naturally or by manipulating BGP advertisements via the Internet routing infrastructure itself. [4]

Sybil Attack

A single adversary, who blocks the transactions from other nodes takes the control of the multiple nodes by disconnecting the them from the public peer-to-peer network. However,

it is unknown by the public that there is only one and same adversary. After that, in a separate network, normal nodes are connected by the adversary to the blocks that the adversary already created. Therefore, double spending can appear as a result of this transaction. [77]

Eclipse Attack

An adversary aims to target a specific individual by cutting off all of the inbound and outbound communications between the target individual victim and the other peers in the public peer-to-peer network rather than multiple nodes. [33]

4.2 Proof of Stake (PoS)

A sample blockchain system that is chosen while explaining the fundamental work principle of PoS type blockchain consensus protocol is Peercoin. However, other PoS based cryptocurrencies also have a lot of similaries in terms of their fundamental work principles.

4.2.1 General Information

Alternative blockchain consensus protocol to Bitcoin's PoW released in 2012 and cryptographic hash function, which is used in Peercoin is SHA256. In Peercoin, a private key is a 256-bit and encryption is governed by the secp256k1 ECDSA. Number of confirmations needed and considered to be secure in Peercoin blockchain is 6 blocks, which means that the average time for finality is 42-51 minutes. A new block is created and gets added to the Peercoin blockchain in every 7-8.5 minutes in average. [96]

4.2.2 Fundamental Work Principle

There are not miners in PoS type blockchain consensus protocol. The mining process refers to forging/minting in PoS type blockchain consensus protocol, so that instead of miners there are forgers/minters. In PoW, the stake for block validation/confirmation is electrical energy, which is external to the cryptocurrency. In PoS, the stake for block validation/confirmation is cryptocurrency coin itself. In other words, money. There are stakeholders. A forger/minter is chosen among stakeholders based on two different methods. Peercoin uses both. Purchasing more than half of the coins costs more than having 51% of PoW hash power. [76, 43, 52, 35]

There are two different way of choosing forgers/minters to validate/confirm next block:

1. **Randomized Block Selection:** Combination of the lowest hash value of the stakeholders and the size of their cryptocurrency coins. Both are public information, so that it is predictable, who is selected to forge the next block.
2. **Coin Age Based Selection:** Multiplication of the number of days the cryptocurrency coins are held on the stake with the number of cryptocurrency coins staked. When a block is forged/minted, then the coin age is reset, it becomes zero. In order to validate/confirm another block, it is needed to wait at least 30 days.

As rewards forgers/minters receive transaction fees. A forger/minter puts his/her own coins as stake in order to validate/confirm transactions and create blocks. If a block is not validated/confirmed properly, then forger/minters can lose the cryptocurrency coins that they have staked.

As in Peercoin, some PoS type blockchain consensus protocols make both PoW and PoS behaviors to secure the blockchain system. [56, 19, 84, 42]

1. **PoS behavior:** The block verification/confirmation selection is based on how much cryptocurrency coins being held or the multiplication of the number of days the cryptocurrency coins are held on the stake with the number of cryptocurrency coins staked.
2. **PoW behavior:** The one, who is selected as block validator/confirmer mines the next block.

4.2.3 Uniqueness Threshold in PoS

Two variables N and T are described in order to decide uniqueness of ledger in the PoS blockchain system.

Let **N** be the total amount of cryptocurrency coins in PoS blockchain system.

Let **T** be the total amount of cryptocurrency coins controlled by adversaries in PoS blockchain system.

Therefore, the theoretical uniqueness threshold condition can be formulated as follows:

$$T < \frac{N}{2} \tag{2}$$

This is the uniqueness threshold condition criteria for the prevension of having alternative branches on the ledger in the PoS blockchain systems. In other words, total amount of cryptocurrency coins controlled by adversaries in PoS blockchain system should be less than the half of the total amount of cryptocurrency coins in PoS blockchain system in order not to have alternative branches on blockchain.

The intuition behind this reasoning is not as in PoW blockchain system. Even though PoS blockchain system seems to be public blockchain, it operates in a relatively private enviroment. That means that in order to become forgers/minters, it is needed to convert the real/physical money to cryptocurrency coins by being a member of the PoS blockchain system. In other words, it is an indirect behavior of permissioned blockchain in some meaning. Thereby, here the adversaries come out on the stage in a partly closed blockchain system enviroment. In addition, the limitations/borders of the assumption in PoS blockchain system are relatively smaller than PoW blockchain system.

In terms of uniqueness for the prevension of having block extension on the ledger, PoS blockchain systems promise to create 1 block per 7-8.5 minutes in average. In addition, it promises number of blocks needed for block confirmation, which are 6 blocks. Therefore, by looking at the promised block creation time and number of blocks needed for block finalization, it can estimated and accepted that PoS blockchain system can fully perform uniqueness against block extension on the ledger.

4.2.4 Necessary Measurements for Uniqueness in PoS

Beside theoretical uniqueness threshold condition described by N and T variables, the research also describes what necessary real world measurements and observations need to be done along with specifying their measurabilities in order to finalize the expression of verifiable uniqueness in PoS based blockchain consensus protocols.

Measurability of Determining N: It is needed to determine the total amount of cryptocurrency coins in PoS blockchain system. Total amount of cryptocurrency coins is large, but it can be determined based on the contents of the ledger, so that it is measurable.

Measurability of Determining T: T cannot be computed because it mostly cannot be known who the adversaries are and how much cryptocurrency coins they have in PoS blockchain system. That is why T is not measurable.

4.2.5 Uniqueness of Ledger in PoS

Regarding to the theoretical uniqueness threshold criteria and the necessary physical real world measurements and observations of N and T variables, as a result, it can be concluded that PoS type blockchain consensus protocol provides the uniqueness of ledger against having alternative branches on the ledger as long as adversaries don't have more than 50% of the total amount of cryptocurrency coins in PoS blockchain system, so that at that time it can be claimed that PoS type blockchain system provides verifiable uniqueness. In other words, only under the condition described in the formula (2) with the necessary physical real world measurements and observations, it can be told that there is only one, single, valid, and unique ledger in entire PoS type blockchain system. In addition, PoS type blockchain system promises full prevention for block extention on the ledger by the estimated block creation time in average and the number of blocks needed for confirmation.

4.2.6 Potential Attacks against Uniqueness in PoS

51% Attack

51% of total amount of cryptocurrency coins is needed to be controlled in PoS blockchain system in order to conduct a double spending attack as a result of 51% attack. Total market cap of Peercoin is $12,017,024, so that for example, 51% attack to conduct a double spending attack would cost around $6,128,682 [85].

Nothing at Stake

When there is fork in the PoS type blockchain system, it may occur either maliciously or accidentally as a potential result of double spending attack. For example, if there is fork in PoW type blockchain system, miners can only mine on one of the fork branches. However, for PoS blockchain system as in Peercoin, forgers/minters can mine on mulptiple sides of the fork branches because they do not pay for mining. Consequently, forgers/minters can get their reward no matter which fork wins in the PoS type blockchain system. [89]

Fake Stake Attack

Vulnerabilities at resource exhaustion on a victim node can cause DoS attack, such as Fake Stake. [74]. An attacker can connect to a victim node and fill up the disk or RAM of the victim node with bogus data until the victim node gets crashed or slows. [97].

Long-Range Attack

Making a longer chain that rewrites the content of the ledger in terms of attacker's need. The main principle is as same as 51% attack. Attack returns to the genesis block and makes forking on the blockchain. For example, For 51% attack, where the attacker starts forking from 6 blocks back at least. For Long-range attack, where the attack starts forking from 60000 blocks back at least. [86].

Three different types of Long-Range Attacks are existed so far [80]:

1. **Simple:** On the blockchain an attacker returns and forks the genesis block. Validator information is located inside the genesis block. Therefore, the attacker will not be able to produce blocks on the fork faster than s/he would do in the main blockchain. In addition, the attacker has to forge timestamps in the implementations, where timestamps are not important to take into account.

2. **Posterior Corruption:** Forging the timestamps is no longer possible here. In order to mint more blocks at the same time frame as the main blockchain, the attacker must use the other validator's blocks. Therefore, the attacker either needs to steal the private key of another validator, who has removed his/her cryptocurrency coins, cashes out, and goes on a long vacation, or the attacher bribes the other validator to join the relevant attack.

3. **Stake Bleeding:** On the blockchain an attacker returns and forks the genesis block. Minting is done locally and id not published. The attacker increases his/her cryptocurrency coins step by step in the forked branch, while s/he keeps losing cryptocurrency coins in the main blockchain. For an attacker, 30% of all cryptocurrency coins with approximately 6-year worth of blockchain history would be needed to perform this type of attack successfully. [72]

Sybil Attack and **Short-Range Attack** would also be more likely in PoS.

4.3 Delegated Proof of Stake (DPoS)

A sample blockchain system that is chosen while explaining the fundamental work principle of DPoS type blockchain consensus protocol is BitShares. However, other DPoS based cryptocurrencies also have a lot of similaries in terms of their fundamental work principles.

4.3.1 General Information

Released in 2014 with the cooperation of Steem and EOS cofounder and Ethereum and Cardano cofounder Charles Hoskinson. In addition, cryptographic hash function, which is used in BitShares is SHA512 and encryption is governed by the secp256k1. A new block is created and gets added to the Peercoin blockchain in every 3-10 seconds in average. [88]

4.3.2 Fundamental Work Principle

There are 2 election processes for DPoS type blockchain system [64].

1. **Witness election:** There are witnesses. Stakeholders vote to select witnesses. Every stakeholder can vote for only one witnesses. Witnesses validates transactions, creates blocks. The number of witnesses is decided by stakeholders. For example, if most stakeholders vote for 50 witnesses, then 50 witnesses are used. If most stakeholders vote for 20, then 20 witnesses are used. The number of witnesses cannot be less than 11. The witnesses' selection process goes on until 50% of stakeholders, who participates in the election believe that there is enough decentralization.
2. **Delegate election:** There are delegates. Stakeholders vote to select delegates. Every stakeholder can vote for only one delegates. They are responsible for maintenance and performance of the entire blockchain system. They cannot create blocks or validate blocks. A delegate can offer changing the size of a block, for example. Another example is that they can propose changing block validation fee for the witnesses. Delegates are not paid. In addition, whatever delegates offer as proposal, the last decision makers are stakeholders. In other words, it is up to the stakeholders whether the relevant changes should be implemented or not.

The election process is like an ongoing democracy process in the parliament systems. That means the voting processes for witnesses and delegates are dynamic. That is used to prevent the witnesses and delegates being monopolized in the DPoS blockchain system. If a stakeholder doesn't have any cryptocurrency coins, then s/he cannot vote. The more stake he or she has, the more powerful his or her vote is. One problem with this situation is that it may work in theory. However, when it comes to practice, it may be seen that developers take a lot of cryptocurrency coins initially. In PoS, the richer can get richer. In DPoS, developers or early investors can become richer. It seems like there is centralized democracy. Developers or early investors may elect themselves as validators. [1]

4.3.3 Uniqueness Threshold in DPoS

Two variables N and T are described in order to decide uniqueness of ledger in the DPoS blockchain system.

Let **N** be the total amount of cryptocurrency coins in DPoS blockchain system.

Let **T** be the total amount of cryptocurrency coins controlled by adversaries in DPoS blockchain system.

Therefore, the theoretical uniqueness threshold criteria can be formulated as follows:

$$T < \frac{N}{2} \tag{3}$$

This is the uniqueness threshold condition criteria for the prevension of having alternative branches on the ledger in the DPoS blockchain systems. In other words, total amount of cryptocurrency coins controlled by adversaries in DPoS blockchain system should be less than the half of the total amount of cryptocurrency coins in DPoS blockchain system in order not to have alternative branches on blockchain.

In terms of uniqueness for the prevension of having block extension on the ledger, DPoS blockchain systems promise to create 1 block per 3-10 seconds in average. However, it obviously does not promise any number of blocks needed for block confirmation. Therefore, by only looking at the promised block creation time, it can be estimated and accepted that DPoS blockchain system can partially perform uniqueness against block extension on the ledger.

4.3.4 Necessary Measurements for Uniqueness in DPoS

Beside theoretical uniqueness threshold condition described by N and T variables, the research also describes what necessary real world measurements and observations need to be done along with specifying their measurabilities in order to finalize the expression of verifiable uniqueness in DPoS based blockchain consensus protocols.

Measurability of Determining N: It is needed to determine the total amount of cryptocurrency coins in DPoS blockchain system. Total amount of cryptocurrency coins is large, but it can be determined based on the contents of the ledger, so that it is measurable.

Measurability of Determining T: T cannot be computed because mostly it cannot be known who the adversaries are and how much cryptocurrency coins they have in DPoS blockchain system. That is why T is not measurable.

4.3.5 Uniqueness of Ledger in DPoS

Regarding to the theoretical uniqueness threshold criteria and the necessary physical real world measurements and observations of N and T variables, as a result, it can be concluded that DPoS type blockchain consensus protocol provides the uniqueness of ledger against having alternative branches on the ledger as long as adversaries don't have more than 50% of the total amount of cryptocurrency coins in DPoS blockchain system, so that at that time it can be claimed that DPoS type blockchain system provides verifiable uniqueness. In other words, only under the condition described in the formula (3) with the necessary physical real world measurements and observations, it can be told that there is only one, single, valid, and unique ledger in entire DPoS type blockchain system. In addition, DPoS type blockchain system promises partially prevention for block extention on the ledger by using the estimated block creation time in average.

4.3.6 Potential Attacks against Uniqueness in DPoS

51% Attack

51% of total amount of cryptocurrency coins is needed to be controlled in DPoS blockchain system in order to conduct a double spending attack as a result of 51% attack. Total market cap of BitShares is $330,651,678,310, so that for example, 51% attack to conduct a double spending attack would cost around $168,632,355,938. [91]

DPoS resolves the problem of "Nothing at Stake" and prevents "Short-Range Attack" like bribe on the system, but still vulnerable against "Sybil Attack" and "Long Range Attack". [99]

4.4 Proof of Capacity (PoC)

A sample blockchain system that is chosen while explaining the fundamental work principle of PoC type blockchain consensus protocol is Burstcoin. However, other PoC based cryptocurrencies also have a lot of similaries in terms of their fundamental work principles.

4.4.1 General Information

Burstcoin was created on August 10th 2014 and introduced on the bitcointalk.org forum. In addition, cryptographic hash function, which is used in Burstcoin is Shabal256. In Burstcoin, encryption is governed by the secp256k1. Number of blocks needed and considered to be secure in Burstcoin blockchain is 24 blocks. A new block is created and gets added to the Burstcoin blockchain in every 4 minutes in average. [75]

4.4.2 Fundamental Work Principle

There are miners like PoW. However, miners compute nonce values once in advance. Miners keep precalculated nonce values into dedicating storage space to be used for the Burstcoin network. This concept is called as plotting. In other words, mining in PoC type blockchain system only requires reading the relevant precalculated nonce values through their hard disk drives. [75]

The more places a miner has for keeping these nonce values, more likely s/he can have the actual nonce value for that round. Therefore, it is called as PoC.

4.4.3 Uniqueness Threshold in PoC

Two variables N and T are described in order to decide uniqueness of ledger in the PoC blockchain system.

Let **N** be the total amount of data storage available in the world.

Let **T** be the total data storage consumed by miners for creating the PoC.

Therefore, the theoretical uniqueness threshold criteria can be formulated as follows:

$$T > \frac{N}{2} \tag{4}$$

This is the uniqueness threshold condition criteria for the prevension of having alternative branches on the ledger in the PoC blockchain systems. In other words, total data storage consumed by miners for creating the PoC should be greater than the half of the total amount of data storage available in the world in order not to have alternative branches on blockchain.

The logic behind this reasoning is same as in PoW blockchain systems. The attribute here that is used while deciding the unique ledger in PoC blockchain system is data storage, which might be assumed that it could exceed and reach to the total amount of data storage available in the world in extreme cases. That is why, the miners should be able to control more than the half of the total amount of data storage available in the world in order to theoretically imply the uniqueness of the ledger in the PoC blockchain system.

In terms of uniqueness for the prevension of having block extension on the ledger, PoC blockchain systems promise to create 1 block per 4 minutes in average. In addition, it promises number of blocks needed for block confirmation, which are 24 blocks. Therefore, by looking at the promised block creation time and number of blocks needed for block finalization, it can estimated and accepted that PoC blockchain system can fully perform uniqueness against block extension on the ledger.

4.4.4 Necessary Measurements for Uniqueness in PoC

Beside theoretical uniqueness threshold condition described by N and T variables, the research also describes what necessary real world measurements and observations need to be done along with specifying their measurabilities in order to finalize the expression of verifiable uniqueness in PoC based blockchain consensus protocols.

Measurability of Determining N: It is needed to determine the total amount of data storage existing in the world. Total amount of data storage is large, but it can be measurable.

Measurability of Determining T: T can be computed based on the ledger by analyzing the strength of PoC. That is why T is measurable.

4.4.5 Uniqueness of Ledger in PoC

Regarding to the theoretical uniqueness threshold criteria and the necessary physical real world measurements and observations of N and T variables, as a result, it can be concluded that PoC type blockchain consensus protocol provides the uniqueness of ledger against having alternative branches on the ledger as long as miners consume more than 50% of the total data storage available in the world, so that at that time it can be claimed that PoC type blockchain system provides verifiable uniqueness. In other words, only under the condition described in the formula (4) with the necessary physical real world measurements and observations, it can be told that there is only one, single, valid, and unique ledger in entire PoC type blockchain system. In addition, PoC type blockchain

system promises full prevention for block extention on the ledger by the estimated block creation time in average and the number of blocks needed for confirmation.

4.4.6 Potential Attacks against Uniqueness in PoC

51% Attack

51% of total amount of data storage is needed to be controlled in PoC blockchain system in order to conduct a double spending attack as a result of 51% attack. Approximately 240 PB of data storage is acquired to deploy a double spend attack on the Burst blockchain. The expense of conducting a double spend attack within 2 hours using 1.688 accelerated computing p2.8xlarge instances would cost more than $5 million. [98]

Nothing at Stake

When there is fork in the PoC type blockchain system, it may occur either maliciously or accidentally as a potential result of double spending attack. For example, In PoW, miners can only mine on one of the forked branches. However, for PoC as in Burstcoin, miners can mine on every forked branches because the nonce values are precalculated in advance, so that miners do not pay to mine on every forked branches. [73]

4.5 Practical Byzantine Fault Tolerance (pBFT)

A sample blockchain system that is chosen while explaining the fundamental work principle of pBFT type blockchain consensus protocol is Hyperledger Fabric. However, other pBFT based cryptocurrencies also have a lot of similaries in terms of their fundamental work principles.

4.5.1 General Information

Announced by the Linux Foundation and supported by IBM, Intel and SAP in 2015 to increase the collaborative development of blockchain type distributed ledger technology. In addition, cryptographic hash function, which is used in Hyperledger Fabric is SHA256 and encryption is governed by the AES256. Hyperledger Fabric provides instant finality in terms of block verification. Hyperledger Fabric supports 10000 transactions per second in average. [95]

4.5.2 Fundamental Work Principle

pBFT is a Byzantine consensus based blockchain consensus protocol [13, 29].

4.5.3 Uniqueness Threshold in pBFT

Two variables N and T are described in order to decide uniqueness of ledger in the pBFT blockchain system.

Let **N** be the total number of nodes in the pBFT blockchain system.

Let **T** be the total number of nodes controlled by adversaries in the blockchain system.

Therefore, the theoretical uniqueness threshold criteria can be formulated as follows:

$$T < \frac{N}{3} \tag{5}$$

This is the uniqueness threshold condition criteria for the prevension of having alternative branches on the ledger in the pBFT blockchain systems. In other words, total number of nodes controlled by adversaries should be less than one third of the total number of nodes in the pBFT blockchain system in order not to have alternative branches on blockchain.

In terms of uniqueness for the prevension of having block extension on the ledger, pBFT blockchain systems promise to create 10000 transactions per 4 minutes in average. In addition, it promises instant finality for block confirmation. Therefore, by looking at the promised transactions creation time and instant block finalization, it can be estimated and accepted that pBFT blockchain system can fully perform uniqueness against block extension on the ledger.

4.5.4 Necessary Measurements for Uniqueness in pBFT

Beside theoretical uniqueness threshold condition described by N and T variables, the research describes what necessary real world measurements and observations need to be done along with specifying their measurabilities in order to finalize the expression of verifiable uniqueness in pBFT based blockchain consensus protocols.

Measurability of Determining N: It is needed to determine the total number of nodes in the pBFT blockchain system. Total number of nodes is large, but it can be determined

based on pBFT blockchain system, so that it is measurable.

Measurability of Determining T: T cannot be computed because mostly it cannot be known who the adversaries are and how many nodes they control in pBFT blockchain system. That is why T is not measurable.

4.5.5 Uniqueness of Ledger in pBFT

Regarding to the theoretical uniqueness threshold criteria and the necessary physical real world measurements and observations of N and T variables, as a result, it can be concluded that pBFT type blockchain consensus protocol provides the uniqueness of ledger against having alternative branches on the ledger as long as adversaries don't have more than 33% of the total number of nodes in the pBFT blockchain system, so that at that time it can be claimed that pBFT type blockchain system provides verifiable uniqueness. In other words, only under the condition described in the formula (5) with the necessary physical real world measurements and observations, it can be told that there is only one, single, valid, and unique ledger in entire pBFT type blockchain system. In addition, pBFT type blockchain system promises full prevention for block extention on the ledger by the estimated transaction creation time in average and the instant block confirmation.

4.5.6 Potential Attacks against Uniqueness in pBFT

34% Attacks

51% attack can be referred here. In other words, it is related to take the control of the majority of the operators in the relevant blockchain consensus protocol. There is not 51% attack here in pBFT. However, it is needed to control of around more than 34% of total nodes in pBFT blockchain system in order to conduct a double spending attack as a result of 34% attack. [38, 45]

4.6 Ripple Protocol Consensus Algorithm (RPCA)

Ripple itself is the blockchain system that uses RPCA.

4.6.1 General Information

Ripple is created and released in the USA by a company called Ripple Labs Inc. in 2012. In addition, cryptographic hash function, which is used in Hyperledger Fabric is SHA256 and encryption is governed by the ED25519. Hyperledger Fabric provides instant finality in terms of block verification. A new block is created and gets added to the Ripple blockchain in every 4 seconds in average. [59]

4.6.2 Fundamental Work Principle

There are actually two types of nodes in RPCA type blockchain system.

1. A **server**, which joins the consensus process. That runs Ripple Server software and it joins in the consensus process.
2. A **client**, which is only cable of transferring the money.

A ledger has three different status in RPCA type blockchain system.

1. A **ledger**, which keeps the record of the cryptocurrency balance in the account of each user.
2. The **last-closed ledger**, which is the recent and the last version of the ledger. That is confirmed by the consensus process.
3. The **open ledger**, which represents the actual presenting status of a node.

Each server maintains a UNL, which includes other servers that query when determining consensus. UNL is not the list of every node on the network. UNL is kind of a subnetwork, which represents the trusted nodes that cannot make fraud or deceive the network. RPCA proceeds in rounds. [59]

1. Each server gets all valid transactions and makes each of them public in a list called "candidate set".
2. After that, each server brings together the candidate sets of all servers in UNL and votes for the honesty of all transactions.
3. Transactions, which have more "yes" votes than the minimum required level are automatically passed on to the next round.

4. However, the ones, who have less than the minimum required level is either discarded or included in the candidate set at the beginning of the next ledger.

5. Finally, it is needed to have an agreement on every transaction by minimum 80% of a server's UNL.

Only the transactions, which meet the requirement about 80% of a server's UNL are applied to the ledger. RPCA is Byzantine agreement based blockchain consensus protocol [10].

In Ripple, there must be (5f + 1) operators at least, if there are f adversaries in the system. In other words,

$$f \leq \frac{n-1}{5}$$

where, f is the total number of nodes with byzantine/arbitrary failure and n is the total number of nodes in the network.

Therefore, the RPCA blockchain system can tolerate up to approximately 20% of byzantine/arbitrary failures in the blockchain system. Ripple uses Distributed Agreement Protocol, which essentially means that a group of servers just agree on which of the transactions come first. It turns out that ordering is very sufficient. Double spending problem occurs because which of the two transactions come first cannot be agreed. If it could have been agreed, then there would have been no question that the second transaction was invalid. Ripple uses Distributed Agreement Protocol just to order the transactions. [30]

4.6.3 Uniqueness Threshold in RPCA

Two variables N and T are described in order to decide uniqueness of ledger in the RPCA blockchain system.

Let **N** be the total number of nodes in the UNL on RPCA blockchain system.

Let **T** be the total number of nodes in the UNL controlled by adversaries in the blockchain system.

Therefore, the theoretical uniqueness threshold criteria can be formulated as follows:

$$T < \frac{N}{5} \tag{6}$$

This is the uniqueness threshold condition criteria for the prevension of having alternative branches on the ledger in the RPCA blockchain systems. In other words, total number of nodes in the UNL controlled by adversaries should be less than one fifth of the total number of nodes in the UNL on RPCA blockchain system in order not to have alternative branches on blockchain.

In terms of uniqueness for the prevension of having block extension on the ledger, RPCA blockchain systems promise to create 1 block per 4 seconds in average. In addition, it promises instant finality for block confirmation. Therefore, by looking at the promised transactions creation time and instant block finalization, it can be estimated and accepted that RPCA blockchain system can fully perform uniqueness against block extension on the ledger.

4.6.4 Necessary Measurements for Uniqueness in RPCA

Beside theoretical uniqueness threshold condition described by N and T variables, the research describes what necessary real world measurements and observations need to be done along with specifying their measurabilities in order to finalize the expression of verifiable uniqueness in RPCA based blockchain consensus protocols.

Measurability of Determining N: It is needed to determine the total number of nodes in the UNL at RPCA blockchain system. Total number of nodes is large, but it can be determined based on RPCA blockchain system, so that it is measurable.

Measurability of Determining T: T cannot be computed because mostly it cannot be known who the adversaries are and how many nodes they control in UNL on RPCA blockchain system. That is why T is not measurable.

4.6.5 Uniqueness of Distributed Ledger in RPCA

Regarding to the theoretical uniqueness threshold criteria and the necessary physical real world measurements and observations of N and T variables, as a result, it can be concluded that RPCA type blockchain consensus protocol provides the uniqueness of ledger against having alternative branches on the ledger as long as adversaries don't have more than 20% of the total number of nodes in the UNL on RPCA blockchain system, so that at that time it can be claimed that RPCA type blockchain system provides verifiable uniqueness. In other words, only under the condition described in the formula (6) with the necessary physical real world measurements and observations, it can be told that there is only one, single, valid, and unique ledger in entire RPCA type blockchain system. In addition,

RPCA type blockchain system promises full prevention for block extention on the ledger by the estimated block creation time in average and the instant block confirmation.

4.6.6 Potential Attacks against Uniqueness in RPCA

Modified Byzantine Attacks

Validators are servers.Therefore, they can influence to the other servers that are configured to be trusted. Modified Byzantine attacks are the possible attacks on RPCA. That means not the classical Byzantine attack, which is related to one third of all nodes.

Other relevant type of attacks could be as followings: [10, 30]

Validators Misbehaving Attack

In order to have influence on the other servers, it is needed to have the control of 80% of trusted validators at least. As a result, it may end up with invalid transactions and double spending attack too.

21% Attack

51% attack can be referred here. There is not 51% attack here in RPCA. However, it is needed to control of 21% of total number of nodes in the UNL in RPCA blockchain system in order to conduct a double spending attack as a result of 21% attack.

Sybil Attack

By using many fake identities, attackers try to take the control of the RPCA blockchain system. It is not important for the other servers, which are configured to trust a validator list or explicit configuration even though an attacker runs a very large number of servers as validators. Therefore, it may seem to be theoretically possible, but practically very difficult to be conducted.

4.7 Proof of Importance (PoI)

A sample blockchain system that is chosen while explaining the fundamental work principle of PoI type blockchain consensus protocol is NEM. However, other PoI based cryptocurrencies also have a lot of similaries in terms of their fundamental work principles.

4.7.1 General Information

NEM was launched on March 25th 2015 written in Java with C++. In addition, cryptographic hash function, which is used in NEM is 512-bit SHA3 and encryption is governed by the ED26619. Number of blocks needed and considered to be secure in NEM blockchain is 360 blocks. [65]

4.7.2 Fundamental Work Principle

Alternative version of PoS. Main idea behind of PoI is that similarly like credit score for a person in a bank, it can be built up a reputation score for a person in blockchain too. In PoS, it is based on how much cryptocurrency coins that have been put in by the stakeholders. In PoI, in addition to how much cryptocurrency coins that have been put in by the stakeholders, it is based on stakeholders' activities in the blockchain system as well. [5]

For example, stakeholders' activities might be as follows: [8]

- Who did a stakeholder send the money to.
- How many transactions is a stakeholder initiating.

There is a process called harvesting. It is closed to mining in PoW, but it doesn't require special hardware as PoW does and it can be done even though the computer is off. In order to have a higher probability of being chosen to harvest a block, it is needed to have accounts with a higher importance score, which means that the account holds at least 10,000 vested NEM cryptocurrency coins, which are known as XEM. In addition, the higher the number of vested cryptocurrency coins, the higher PoI score. [57]

4.7.3 Uniqueness Threshold in PoI

Two variables N and T are described in order to decide uniqueness of ledger in the PoI blockchain system.

Let **N** be the total amount of cryptocurrency coins with good reputation scores in PoI blockchain system.

Let **T** be the total amount of cryptocurrency coins with good reputation scores controlled by adversaries in PoI blockchain system.

Therefore, the theoretical uniqueness threshold criteria can be formulated as follows:

$$T < \frac{N}{2} \tag{7}$$

This is the uniqueness threshold condition criteria for the prevension of having alternative branches on the ledger in the PoI blockchain systems. In other words, total amount of cryptocurrency coins with good reputation scores controlled by adversaries in PoI blockchain system should be less than half of the total amount of cryptocurrency coins with good reputation scores in PoI blockchain system in order not to have alternative branches on blockchain.

In terms of uniqueness for the prevension of having block extension on the ledger, PoI blockchain systems do not promise to create any number of blocks within a vertain of time in average. However, PoI blockchain system says that the blocks are considered to be secure and be surely appended to the blockchain after every 360 blocks. Therefore, indirectly it can be estimated and accepted that PoI blockchain system can partially perform uniqueness against block extension on the ledger.

4.7.4 Necessary Measurements for Uniqueness in PoI

Beside theoretical uniqueness threshold condition described by N and T variables, the research describes what necessary real world measurements and observations need to be done along with specifying their measurabilities in order to finalize the expression of verifiable uniqueness in PoI based blockchain consensus protocols.

Measurability of Determining N: It is needed to determine the total amount of cryptocurrency coins with good reputation scores in PoI blockchain system. Total amount of cryptocurrency coins with good reputation scores is large, but it can be determined based on the contents of the ledger, so that it is measurable.

Measurability of Determining T: T cannot be computed because mostly it cannot be known who the adversaries are and how much cryptocurrency coins with good reputation scores they have in PoI blockchain system. That is why T is not measurable.

4.7.5 Uniqueness of Ledger in PoI

Regarding to the theoretical uniqueness threshold criteria and the necessary physical real world measurements and observations of N and T variables, as a result, it can be

concluded that PoI type blockchain consensus protocol provides the uniqueness of ledger against having alternative branches on the ledger as long as adversaries don't have more than 50% of the total amount of cryptocurrency coins with good reputation scores in PoI blockchain system, so that at that time it can be claimed that PoI type blockchain system provides verifiable uniqueness. In other words, only under the condition described in the formula (7) with the necessary physical real world measurements and observations, it can be told that there is only one, single, valid, and unique ledger in entire PoI type blockchain system. In addition, PoI type blockchain system promises partially prevention for block extention on the ledger by the estimated number of blocks needed in average to considered as secure.

4.7.6 Potential Attacks against Uniqueness in PoI

Here are two possible attacks for PoI as follows: [71]

Sybil Attack

For taking the control of the PoI blockchain system, attackers try to create many accounts PoI blockchain system, which is secure against Sybil attacks.

Loop Attack

The main logic behind the attack is that attackers send NEM to their accounts in a loop. Therefore, the result of the attack may end up with profit gain between 4% and 7%. However, attack can cause losing many transaction fees. Therefore, once being calculated, it wouldn't be worth to carry out the relevant attack.

4.8 Proof of Stake Velocity (PoSV)

A sample blockchain system that is chosen while explaining the fundamental work principle of PoSV type blockchain consensus protocol is Reddcoin. However, other PoSV based cryptocurrencies also have a lot of similaries in terms of their fundamental work principles.

4.8.1 General Information

Reddcoin was released in February 2014. In addition, cryptographic hash function, which is used in Reddcoin is Scrypt. Number of confirmations needed and considered to be

secure in Reddcoin blockchain is 120 blocks. A new block is created and gets added to the Reddcoin blockchain in every 1 minute in average. [55]

4.8.2 Fundamental Work Principle

In PoS, all of the cryptocurrency coins have the same weight. That means that if someone has more cryptocurrency coins, the more chance s/he is chosen to be as validators. In PoSV, all of the cryptocurrency coins don't have the same weight. Weight of the coins is not equal. That means that newer cryptocurrency coins are worthier in terms of being chosen as validators in the blockchain system. [61]

Newer doesn't refer to the age of the cryptocurrency coin. It refers how long the cryptocurrency coin has been held. For example, newer cryptocurrency coins that have 1000$ value is worthier than older cryptocurrency coins that have 1000$ value.

PoI adds reputation scores to stakeholders' account, and it is linked to stakeholder. In other words, it uses the cryptocurrency coin and the stakeholder's account activity to calculate the stakeholder's reputation score. The reputation score determines the chances of the actively chosen to be as validator. However, PoSV, it is linked to cryptocurrency coins themselves. In other words, it uses the cryptocurrency coin and the stakeholder's account activity to calculate the cumulative weight of the cryptocurrency coins and the cumulative weight of the cryptocurrency coins gives the stakeholder higher chance to be chosen as validator. [63]

4.8.3 Uniqueness Threshold in PoSV

Two variables N and T are described in order to decide uniqueness of ledger in the PoSV blockchain system.

Let **N** be the total amount of newer cryptocurrency coins in PoSV blockchain system.

Let **T** be the total amount of newer cryptocurrency coins controlled by adversaries in PoSV blockchain system.

Therefore, the theoretical uniqueness threshold criteria can be formulated as follows:

$$T < \frac{N}{2} \tag{8}$$

This is the uniqueness threshold condition criteria for the prevension of having alternative branches on the ledger in the PoSV blockchain systems. In other words, total amount of newer cryptocurrency coins controlled by adversaries in PoSV blockchain system should be less than half of the total amount of newer cryptocurrency coins in PoSV blockchain system in order not to have alternative branches on blockchain.

In terms of uniqueness for the prevension of having block extension on the ledger, PoSV blockchain systems promise to create 1 block per minute in average. In addition, it promises number of blocks needed for block confirmation, which are 120 blocks. Therefore, by looking at the promised block creation time and number of blocks needed for block finalization, it can be estimated and accepted that PoSV blockchain system can fully perform uniqueness against block extension on the ledger.

4.8.4 Necessary Measurements for Uniqueness in PoSV

Beside theoretical uniqueness threshold condition described by N and T variables, the research describes what necessary real world measurements and observations need to be done along with specifying their measurabilities in order to finalize the expression of verifiable uniqueness in PoSV based blockchain consensus protocols.

Measurability of Determining N: It is needed to determine the total amount of newer cryptocurrency coins in PoSV blockchain system. Total amount of newer cryptocurrency coins is large, but it can be determined based on the contents of the ledger, so that it is measurable.

Measurability of Determining T: T cannot be computed because mostly it cannot be known who the adversaries are and how much newer cryptocurrency coins they have in PoSV blockchain system. That is why T is not measurable.

4.8.5 Uniqueness of Ledger in PoSV

Regarding to the theoretical uniqueness threshold criteria and the necessary physical real world measurements and observations of N and T variables, as a result, it can be concluded that PoSV type blockchain consensus protocol provides the uniqueness of ledger against having alternative branches on the ledger as long as adversaries don't have more than 50% of the total amount of newer cryptocurrency coins in PoSV blockchain system, so that at that time it can be claimed that PoSV type blockchain system provides verifiable uniqueness. In other words, only under the condition described in the formula (8) with the necessary physical real world measurements and observations, it can be told that there

is only one, single, valid, and unique ledger in entire PoSV type blockchain system. In addition, PoSV type blockchain system promises full prevention for block extention on the ledger by the estimated block creation time in average and the number of blocks needed for confirmation.

4.8.6 Potential Attacks against Uniqueness in PoSV

51% Attack

51% of total amount of newer cryptocurrency coins is needed to be controlled in PoSV blockchain system in order to conduct a double spending attack as a result of 51% attack.

There is an exponential delay function called coin age function, which is a function of time is calculated. The asymptotic limit of coin age function, which increases the difficulty for 51% attacks significantly gives extra security for the network. [63]

Malicious Stakeholders Attack

Misuse case of the signature of stakeholders. In other words, if one block is signed by malicious stakeholders firstly, then majority can be achieved by malicious stakeholders. If a different block is signed by malicious stakeholders, then bigger majority can be achieved malicious stakeholders. However, the blockchain system will immediately recognize the relevant signatures just right after the majority is achieved. Signatures will be ignored. Therefore, the attackers will not be able to get succeeded. [94]

4.9 Proof of Stake Time (PoST)

A sample blockchain system that is chosen while explaining the fundamental work principle of PoST type blockchain consensus protocol is VeriCoin. However, other PoST based cryptocurrencies also have a lot of similaries in terms of their fundamental work principles.

4.9.1 General Information

VeriCoin was released by two innovative PhD students from Rutgers University in 2014. It was the first time developers were not anonymous. In addition, cryptographic hash function, which is used in VeriCoin is Scrypt. Number of confirmations needed and considered to be secure in VeriCoin blockchain is 10 blocks. A new block is created and gets added to the VeriCoin blockchain in every 1 minute in average. [82]

4.9.2 Fundamental Work Principle

In PoS, all of the cryptocurrency coins have the same weight. That means that if someone has more cryptocurrency coins, the more chance s/he is chosen to be as validators. In PoST, all of the cryptocurrency coins don't have the same weight. Weight of the coins is not equal. That means that older cryptocurrency coins are worthier in terms of being chosen as validators in the blockchain system. [43]

Older doesn't refer to the age of the cryptocurrency coin. It refers how long the cryptocurrency coin has been held. For example, older cryptocurrency coins that have 1000$ value is worthier than newer cryptocurrency coins that have 1000$ value.

PoST is actually in opposition of PoSV.

4.9.3 Uniqueness Threshold in PoST

Two variables N and T are described in order to decide uniqueness of ledger in the PoST blockchain system.

Let **N** be the total amount of older blockchain system coins in PoST blockchain system.

Let **T** be the total amount of older blockchain system coins controlled by adversaries in PoST blockchain system.

Therefore, the theoretical uniqueness threshold criteria can be formulated as follows:

$$T < \frac{N}{2} \tag{9}$$

This is the uniqueness threshold condition criteria for the the prevension of having alternative branches on the ledger in the PoST blockchain systems. In other words, total amount of older cryptocurrency coins controlled by adversaries in PoST blockchain system should be less than half of the total amount of older cryptocurrency coins in PoST blockchain system in order not to have alternative branches on blockchain.

In terms of uniqueness for the prevension of having block extension on the ledger, PoST blockchain systems promise to create 1 block per minute in average. In addition, it promises number of blocks needed for block confirmation, which are 10 blocks. Therefore, by looking at the promised block creation time and number of blocks needed for block finalization, it can be estimated and accepted that PoST blockchain system can fully

perform uniqueness against block extension on the ledger.

4.9.4 Necessary Measurements for Uniqueness in PoST

Beside theoretical uniqueness threshold condition described by N and T variables, the research describes what necessary real world measurements and observations need to be done along with specifying their measurabilities in order to finalize the expression of verifiable uniqueness in PoST based blockchain consensus protocols.

Measurability of Determining N: It is needed to determine the total amount of older cryptocurrency coins in PoST blockchain system. Total amount of older cryptocurrency coins is large, but it can be determined based on the contents of the ledger, so that it is measurable.

Measurability of Determining T: T cannot be computed because mostly it cannot be known who the adversaries are and how much older cryptocurrency coins they have in PoST blockchain system. That is why T is not measurable.

4.9.5 Uniqueness of Ledger in PoST

Regarding to the theoretical uniqueness threshold criteria and the necessary physical real world measurements and observations of N and T variables, as a result, it can be concluded that PoST type blockchain consensus protocol provides the uniqueness of ledger against having alternative branches on the ledger as long as adversaries don't have more than 50% of the total amount of older cryptocurrency coins in PoST blockchain system, so that at that time it can be claimed that PoST type blockchain system provides verifiable uniqueness. In other words, only under the condition described in the formula (9) with the necessary physical real world measurements and observations, it can be told that there is only one, single, valid, and unique ledger in entire PoST type blockchain system. In addition, PoST type blockchain system promises full prevention for block extention on the ledger by the estimated block creation time in average and the number of blocks needed for confirmation.

4.9.6 Potential Attacks against Uniqueness in PoST

51% Attack

Taking the control of 51% of total amount of older cryptocurrency coins in PoST blockchain system is necessary to conduct a double spending attack as a result of 51% attack [82].

4.10 Proof of Burn (PoB)

A sample blockchain system that is chosen while explaining the fundamental work principle of PoB type blockchain consensus protocol is Counterparty. However, other PoB based cryptocurrencies also have a lot of similaries in terms of their fundamental work principles.

4.10.1 General Information

Counterparty was launched in 2014. It is a protocol, a set of specifications and an API that allows cryptocurrency users to create and trade assets using Bitcoin's blockchain. In addition, cryptographic hash function, which is used in Counterparty is SHA256 and encryption is governed by ARC4. Number of confirmations needed and considered to be secure in Counterparty blockchain is 6 blocks. A new block is created and gets added to the Counterparty blockchain in every 10 minutes in average. [90]

4.10.2 Fundamental Work Principle

There are miners like in PoW type blockchain system. There is special type of addresses called eater addresses that no one has access to. They are just used to store cryptocurrency coins, so that cryptocurrency coins, which are stored in there can never be spent. [15]

Eater addresses are actually Bitcoin addresses. They are randomly generated by using nonspecific private keys. In other words, they are unspendable addresses, which effectively burn cryptocurrency coins, so that cryptocurrency coins, which are sent to eater addresses and stored there cannot be accessed and spent anymore even though they are still part of all existing cryptocurrency coins to be generated. [20]

Miners send as many coins as they would like to eater addresses. The more coins someone has burned, the better chance for him or her to be chosen to mine the next block.

The main idea behind is that miners try to show their desires to be exposed to short term loss in order for a long-term investment and gain. So, some coins cannot be just burned and left there. It is needed to keep burning cryptocurrency coins periodically in order to

have the same chance to be chosen to mine the next block. [44]

4.10.3 Uniqueness Threshold in PoB

Two variables N and T are described in order to decide uniqueness of ledger in the PoB blockchain system.

Let **N** be the total amount of cryptocurrency coins in the eater address in PoB blockchain system.

Let **T** be the total amount of cryptocurrency coins in the eater address controlled by adversaries in PoB blockchain system.

Therefore, the theoretical uniqueness threshold criteria can be formulated as follows:

$$T < \frac{N}{2} \tag{10}$$

This is the uniqueness threshold condition criteria for the prevension of having alternative branches on the ledger in the PoB blockchain systems. In other words, total amount of cryptocurrency coins in the eater address controlled by adversaries in PoB blockchain system should be less than half of the total amount of cryptocurrency coins in the eater address in PoB blockchain system in order not to have alternative branches on blockchain.

In terms of uniqueness for the prevension of having block extension on the ledger, PoB blockchain systems promise to create 1 block per 10 minutes in average. In addition, it promises number of blocks needed for block confirmation, which are 6 blocks. Therefore, by looking at the promised block creation time and number of blocks needed for block finalization, it can be estimated and accepted that PoB blockchain system can fully perform uniqueness against block extension on the ledger.

4.10.4 Necessary Measurements for Uniqueness in PoB

Beside theoretical uniqueness threshold condition described by N and T variables, the research describes what necessary real world measurements and observations need to be done along with specifying their measurabilities in order to finalize the expression of verifiable uniqueness in PoB based blockchain consensus protocols.

Measurability of Determining N: It is needed to determine the total amount of

cryptocurrency coins in the eater address in PoB blockchain system. Total amount of cryptocurrency coins in the eater address is large, but it can be determined based on the contents of the ledger, so that it is measurable.

Measurability of Determining T: T cannot be computed because mostly it cannot be known who the adversaries are and how much cryptocurrency coins in the eater address they have in PoB blockchain system. That is why T is not measurable.

4.10.5 Uniqueness of Ledger in PoB

Regarding to the theoretical uniqueness threshold criteria and the necessary physical real world measurements and observations of N and T variables, as a result, it can be concluded that PoB type blockchain consensus protocol provides the uniqueness of ledger against having alternative branches on the ledger as long as adversaries don't have more than 50% of the total amount of cryptocurrency coins in the eater address in PoB blockchain system, so that at that time it can be claimed that PoB type blockchain system provides verifiable uniqueness. In other words, only under the condition described in the formula (10) with the necessary physical real world measurements and observations, it can be told that there is only one, single, valid, and unique ledger in entire PoB type blockchain system. In addition, PoB type blockchain system promises full prevention for block extention on the ledger by the estimated block creation time in average and the number of blocks needed for confirmation.

4.10.6 Potential Attacks against Uniqueness in PoB

51% Attack

Taking the control of 51% of total amount of cryptocurrency coins in the eater address in PoB blockchain system is required in order to conduct a double spending attack as a result of 51% attack [15, 20, 44].

4.11 Proof of Reputation (PoR)

A sample blockchain system that is chosen while explaining the fundamental work principle of PoR type blockchain consensus protocol is GoChain. However, other PoR based cryptocurrencies also have a lot of similaries in terms of their fundamental work principles.

4.11.1 General Information

GoChain is a platform that supports smart contracts and distributed applications can be built up on top of it. A new block is created and gets added to the GoChain blockchain in every 5 seconds in average. [36]

4.11.2 Fundamental Work Principle

Voting structure, where each user votes the other users. A user's reputation is the sum of the all ratings of the other user and multiplied by the rate of rating. The higher reputation score someone has, more likely s/he will be picked to mine the next block. [36]

There may be the other variant of PoR type blockchain system. In other words, it utilizes the power of the infrastructure that is already in place in the real world.

What a business would not want to lose apart from money is "Reputation".

The quantification of the business reputation can be expressed as follows: [25]

- **Market cap**: If a company has a big market cap, they have many to lose. They normally have a big sort of reputation standard.
- **Public/private**: A public company loses more money if something goes wrong.
- **Brand significance**: Significance of a brand is somewhat a subjective method. That means the company relies on the brand more. For example, Apple Inc. Namely, brand image.

If these three metrics are combined together, a score for reputation can be built and called as reputation score. There would need to have such kind of a centralized party to decide what his or her reputation score is. It would be more suited to the private blockchains.

4.11.3 Uniqueness Threshold in PoR

Two variables N and T are described in order to decide uniqueness of ledger in the PoR blockchain system.

Let **N** be the total good reputation score in PoR blockchain system.

Let **T** be the total good reputation score controlled by adversaries in PoR blockchain system.

Therefore, the theoretical uniqueness threshold criteria can be formulated as follows:

$$T < \frac{N}{2} \tag{11}$$

This is the uniqueness threshold condition criteria for the prevension of having alternative branches on the ledger in the PoR blockchain systems. In other words, total good reputation score controlled by adversaries in PoR blockchain system should be less than half of the total good reputation score in PoR blockchain system in order not to have alternative branches on blockchain.

In terms of uniqueness for the prevension of having block extension on the ledger, PoR blockchain systems promise to create 1 block per 5 seconds in average. However, it obviously does not promise any number of blocks needed for block confirmation. Therefore, by only looking at the promised block creation time, it can be estimated and accepted that PoR blockchain system can partially perform uniqueness against block extension on the ledger.

4.11.4 Necessary Measurements for Uniqueness in PoR

Beside theoretical uniqueness threshold condition described by N and T variables, the research describes what necessary real world measurements and observations need to be done along with specifying their measurabilities in order to finalize the expression of verifiable uniqueness in PoR based blockchain consensus protocols.

Measurability of Determining N: It is needed to determine the total good reputation score in PoR blockchain system. Total good reputation score is large, but it can be determined based on the contents of the ledger, so that it is measurable.

Measurability of Determining T: T cannot be computed because mostly it cannot be known who the adversaries are and how much good reputation score they have in PoR blockchain system. That is why T is not measurable.

4.11.5 Uniqueness of Ledger in PoR

Regarding to the theoretical uniqueness threshold criteria and the necessary physical real world measurements and observations of N and T variables, as a result, it can be concluded that PoR type blockchain consensus protocol provides the uniqueness of ledger against having alternative branches on the ledger as long as adversaries don't have more than 50% of the total good reputation score in PoR blockchain system, so that at that time it can be claimed that PoR type blockchain system provides verifiable uniqueness. In other words, only under the condition described in the formula (11) with the necessary physical real world measurements and observations, it can be told that there is only one, single, valid, and unique ledger in entire PoR type blockchain system. In addition, PoR type blockchain system promises partially prevention for block extention on the ledger by using the estimated block creation time in average.

4.11.6 Potential Attacks against Uniqueness in PoR

Bad-mouthing Attack

In order to improve the reputation reliability rankings, malicious nodes continuously give bad marks, dishonest recommendations to good nodes [37].

Replay Attack

In order to increase the impact of the same transactionts, transactions are replayed. Therefore, an attacker can participate in a transaction that is multiple times profitable. [37]

On-off Attack

In order to remain undetected, they can perform well or badly while malicious nodes are causing damage [37].

Newcomer Attack

Attackers can switch to a new ID by creating more than a single ID legally, if one ID gets low reputation because of performing bad behaviors [37].

4.12 Proof of Authority (PoA)

A sample blockchain system that is chosen while explaining the fundamental work principle of PoA type blockchain consensus protocol is VeChain. However, other PoA based cryptocurrencies also have a lot of similaries in terms of their fundamental work principles.

4.12.1 General Information

VeChain since 2015 is one of the leading blockchain platform that offers blockchain as a service to the enterprise and corporate companies. In addition, cryptographic hash function, which is used in VeChain is SHA256. Number of blocks needed and considered to be secure in Burstcoin blockchain is 12 blocks. A new block is created and gets added to the VeChain blockchain in every 10 seconds in average. [87]

4.12.2 Fundamental Work Principle

Companies are chosen to be the validators by some external party. Validators are also called as authority master nodes. Authority master nodes have random chance to be picked to validate the next block. So, the common workflow is to pick authority master nodes is by requiring a license that must be obtained from the government. Once picked, it is needed to put personal information and license on the blockchain, so everyone in the private blockchain can verify identity and the license that links to. [100]

PoA is actually not suitable for individuals. It is more geared to companies and private blockchains.

Not every company can request to be in the validator list. They have to do something, so that the blockchain hold the company accountable for any wrong events. In order to get the license, it is needed to sign some documents that would lead the company reliable for any theft or misconduct. However, it provides possible security due to the fact that authority master nodes have to leave identifiable information on the blockchain for everyone on the network to see. [2]

4.12.3 Uniqueness Threshold in PoA

Two variables N and T are described in order to decide uniqueness of ledger in the PoA blockchain system.

Let **N** be the total number of companies with authority licenses in PoA blockchain system.

Let **T** be the total number of companies with authority licenses controlled by adversaries in PoA blockchain system.

Therefore, the theoretical uniqueness threshold criteria can be formulated as follows:

$$T < \frac{N}{2} \tag{12}$$

This is the uniqueness threshold condition criteria for the prevension of having alternative branches on the ledger in the PoA blockchain systems. In other words, total number of companies with authority licenses controlled by adversaries in PoA blockchain system should be less than half of the total number of companies with authority licenses in PoA blockchain system in order not to have alternative branches on blockchain.

In terms of uniqueness for the prevension of having block extension on the ledger, PoA blockchain systems promise to create 1 block per 10 seconds in average. In addition, it promises number of blocks needed for block confirmation, which are 12 blocks. Therefore, by looking at the promised block creation time and number of blocks needed for block finalization, it can be estimated and accepted that PoA blockchain system can fully perform uniqueness against block extension on the ledger.

4.12.4 Necessary Measurements for Uniqueness in PoA

Beside theoretical uniqueness threshold condition described by N and T variables, the research describes what necessary real world measurements and observations need to be done along with specifying their measurabilities in order to finalize the expression of verifiable uniqueness in PoA based blockchain consensus protocols.

Measurability of Determining N: It is needed to determine the total number of companies with authority licenses in PoA blockchain system. Total number of companies with authority licenses is not large and it can be determined based on validator list, so that it is measurable.

Measurability of Determining T: T cannot be computed because mostly it cannot be known who the adversaries are and whether they have authority licenses or not in PoA blockchain system. That is why T is not measurable.

4.12.5 Uniqueness of Ledger in PoA

Regarding to the theoretical uniqueness threshold criteria and the necessary physical real world measurements and observations of N and T variables, as a result, it can be concluded that PoA type blockchain consensus protocol provides the uniqueness of ledger against having alternative branches on the ledger as long as adversaries don't have more than 50% of the total number of companies with authority licenses in PoA blockchain system, so that at that time it can be claimed that PoA type blockchain system provides verifiable uniqueness. In other words, only under the condition described in the formula (12) with the necessary physical real world measurements and observations, it can be told that there is only one, single, valid, and unique ledger in entire PoA type blockchain system. In addition, PoA type blockchain system promises full prevention for block extention on the ledger by the estimated block creation time in average and the number of blocks needed for confirmation.

4.12.6 Potential Attacks against Uniqueness in PoA

51% Attack

Obtaining the control of 51% of total number of companies with authority licenses in PoA blockchain system is necessary and required in order to conduct a double spending attack as a result of 51% attack. However, it is very difficult [100, 2].

DoS Attack

Attackers send a of transactions and blocks to a targeted blockchain system node in order to make it unavailable. However, the lack of a node in a blockchain system is not that important, because at least one of the companies with authority licenses from the list of validating nodes can make the validations done. [17]

4.13 Delegated Byzantine Fault Tolerance (dBFT)

A sample blockchain system that is chosen while explaining the fundamental work principle of dBFT type blockchain consensus protocol is NEO. However, other dBFT based cryptocurrencies also have a lot of similaries in terms of their fundamental work principles.

4.13.1 General Information

NEO was launched as an open source project. NEO was founded in 2104. In 2015, it was open-sourced on GitHub. In addition, cryptographic hash function, which is used in NEO is RIPEMD160 and encryption that is used in NEO is ECC. NEO has immediate finality for the block validation. A new block is created and gets added to the NEO blockchain in every 20 seconds in average. [92]

4.13.2 Fundamental Work Principle

There are two type of consensus nodes.

1. **Speaker node**: Only one and responsible for a block proposal to the blockchain system.
2. **Delegate nodes**: Multiple and responsible for reaching a consensus on the transaction.

When a consensus has started, a speaker node has been chosen to prepare a block of transactions. It sends the proposed block of transactions to the other delegate nodes. Other delegate nodes do two things. They just check if all transactions are valid or not. If there is such a case about double-spending or not. If not, then they ask to the other delegate nodes to make sure that they also have the same result by the speaker node. [34]

- If any of these are wrong, the delegate nodes send out a "change view".
- If all is good, the delegate nodes send out a "prepare request".

All of the delegate nodes do this and they listen out for what they are saying. If 66% sends 'change view', then a new leader is selected, and the process starts again. If 66% sends 'prepare request', then the block is signed and added to the blockchain.

It is needed at least 66% in NEO since NEO uses dBFT, which doesn't make it secure and is not very different than pBFT. The number of them need to be constant. That means the process of becoming a validator is more tightly controlled. [32]

4.13.3 Uniqueness Threshold in dBFT

Two variables N and T are described in order to decide uniqueness of ledger in the dBFT blockchain system.

Let **N** be the total number of delegate nodes in dBFT blockchain system.

Let **T** be the total number of delegate nodes controlled by adversaries in dBFT blockchain system.

Therefore, the theoretical uniqueness threshold criteria can be formulated as follows:

$$T < \frac{N}{3} \tag{13}$$

This is the uniqueness threshold condition criteria for the prevension of having alternative branches on the ledger in the dBFT blockchain systems. In other words, total number of delegate nodes controlled by adversaries in dBFT blockchain system should be less than one third of the total number of delegate nodes in dBFT blockchain system in order not to have alternative branches on blockchain.

In terms of uniqueness for the prevension of having block extension on the ledger, dBFT blockchain systems promise to create 1 block per 20 seconds in average. However, it obviously does not promise any number of blocks needed for block confirmation. Therefore, by only looking at the promised block creation time, it can be estimated and accepted that dBFT blockchain system can partially perform uniqueness against block extension on the ledger.

4.13.4 Necessary Measurements for Uniqueness in dBFT

Beside theoretical uniqueness threshold condition described by N and T variables, the research describes what necessary real world measurements and observations need to be done along with specifying their measurabilities in order to finalize the expression of verifiable uniqueness in dBFT based blockchain consensus protocols.

Measurability of Determining N: It is needed to determine the total number of delegate nodes in dBFT blockchain system. Total number of delegate nodes is large, but it can be determined based on dBFT blockchain system, so that it is measurable.

Measurability of Determining T: T cannot be computed because mostly it cannot

be known who the adversaries are and how many nodes they control in dBFT blockchain system. That is why T is not measurable.

4.13.5 Uniqueness of Ledger in dBFT

Regarding to the theoretical uniqueness threshold criteria and the necessary physical real world measurements and observations of N and T variables, as a result, it can be concluded that dBFT type blockchain consensus protocol provides the uniqueness of ledger against having alternative branches on the ledger as long as adversaries don't have more than 33% of the total number of nodes in the dBFT blockchain system, so that at that time it can be claimed that dBFT type blockchain system provides verifiable uniqueness. In other words, only under the condition described in the formula (13) with the necessary physical real world measurements and observations, it can be told that there is only one, single, valid, and unique ledger in entire dBFT type blockchain system. In addition, dBFT type blockchain system promises partially prevention for block extention on the ledger by using the estimated block creation time in average.

4.13.6 Potential Attacks against Uniqueness in dBFT

34% Attacks

Taking the control of more than 34% of total number of delegate nodes in dBFT blockchain system is mandatory in order to conduct a double spending attack as a result of 34% attack [34, 32].

4.14 Proof of History (PoH)

A sample blockchain system that is chosen while explaining the fundamental work principle of PoH type blockchain consensus protocol is Solana. However, other PoH based cryptocurrencies also have a lot of similaries in terms of their fundamental work principles.

4.14.1 General Information

Solana is the most performant public blockchain in the world and it supports a sustained throughput of more than 50000 transactions per second. In addition, cryptographic hash function, which is used in Solana is SHA256 and encryption that is used in Solana is

CBC. A new block is created and gets added to the Solana blockchain in every minute in average. [18]

4.14.2 Fundamental Work Principle

Instead of trusting the timestamp, a historical transaction record is created. Thereby, it proves that an event has occurred at a specific moment in time. PoH uses a high frequency verifiable delay function, which produces a unique output that can be efficiently and publicly verified. In the implementation of Solana, a sequential pre-image resistant hash that runs over itself continuously. It uses with the previous output used as the next input. The current output and the count are recorded periodically. Then it can be certain that real time has passed between each counter. [18]

It is impossible to create an input, which can generate that desired hash in the future. In other words, it is impossible to create an alternative history with the same hashes as long as cryptographic hash function is pre-image and collision resistant.

4.14.3 Uniqueness Threshold in PoH

PoH prevents creating forks in backdating manner, but does not prevent simultaneous creation of alternative branches.

In terms of uniqueness for the prevension of having block extension on the ledger, PoH blockchain systems promise to create 1 block per minute in average. However, it obviously does not promise any number of blocks needed for block confirmation. Therefore, by only looking at the promised block creation time, it can be estimated and accepted that PoH blockchain system can partially perform uniqueness against block extension on the ledger.

4.14.4 Necessary Measurements for Uniqueness in PoH

No measurement will prove the uniqueness in PoH type blockchain system.

4.14.5 Uniqueness of Ledger in PoH

PoH does not provide uniqueness against having alternative branches on the ledger. However, PoH type blockchain system promises partially prevention for block extention on the

ledger by using the estimated block creation time in average.

4.14.6 Potential Attacks against Uniqueness in PoH

No specific attacks are known against PoH type blockchain system.

4.15 Proof of Weight (PoWeight)

A sample blockchain system that is chosen while explaining the fundamental work principle of PoWeight type blockchain consensus protocol is Algorand. However, other PoWeight based cryptocurrencies also have a lot of similaries in terms of their fundamental work principles.

4.15.1 General Information

Cryptography pioneer, Silvio Micali founded Algorand. His main focus was on decentralization, scalability and security in blockchain systems. In addition, cryptographic hash function, which is used in Algorand is SHA256 and encryption that is used in Algorand is IBE. Number of blocks needed and considered to be secure in Algorand blockchain is 6 blocks. [66]

4.15.2 Fundamental Work Principle

Algorand uses Byzantine consensus protocol capable of scaling to many users. Algorand confirms transactions very quickly.

There are weighted stakeholders in PoWeight blockchain system. They play an integral role in PoWeight blockchain system. A weight is attached to every stakeholder on PoWeight blockchain system. In PoS, only the cryptocurrency coins that a stakeholder holds is taken into account while being a validator. In PoWeight, while being a validator, some other relatively weighted values are used as follows: [66]

- cryptocurrency coins
- honesty

Therefore, weight is based on how much money that a user holds in his or her account and how reliable s/he is.

PoWeight creates a committee, which is made up of random PoWeight blockchain system stakeholders, so that it makes sure that the majority of committee members are honest while also proposing some centralization [16].

4.15.3 Uniqueness Threshold in PoWeight

Two variables N and T are described in order to decide uniqueness of ledger in the PoWeight blockchain system.

Let **N** be the total amount of weighted cryptocurrency coins in PoWeight blockchain system.

Let **T** be the total amount of weighted cryptocurrency coins controlled by adversaries in PoWeight blockchain system.

Therefore, the theoretical uniqueness threshold criteria can be formulated as follows:

$$T < \frac{N}{3} \tag{14}$$

This is the uniqueness threshold condition criteria for the prevension of having alternative branches on the ledger in the PoWeight blockchain systems. In other words, total amount of weighted cryptocurrency coins controlled by adversaries in PoWeight blockchain system should be less than one third of the total amount of weighted cryptocurrency coins in PoWeight blockchain system in order not to have alternative branches on blockchain.

In terms of uniqueness for the prevension of having block extension on the ledger, PoWeight blockchain systems do not promise to create any number of blocks within a vertain of time in average. However, PoWeight blockchain system says that the blocks are considered to be secure and be surely appended to the blockchain after every 6 blocks. Therefore, indirectly it can be estimated and accepted that PoWeight blockchain system can partially perform uniqueness against block extension on the ledger.

4.15.4 Necessary Measurements for Uniqueness in PoWeight

Beside theoretical uniqueness threshold condition described by N and T variables, the research describes what necessary real world measurements and observations need to be done along with specifying their measurabilities in order to finalize the expression of verifiable uniqueness in PoWeight based blockchain consensus protocols.

Measurability of Determining N: It is needed to determine the total amount of weighted cryptocurrency coins in PoWeight blockchain system. Total amount of weighted cryptocurrency coins is large, but it can be determined based on the contents of the ledger, so that it is measurable.

Measurability of Determining T: T cannot be computed because mostly it cannot be known who the adversaries are and how much weighted cryptocurrencycoins they have in PoWeight blockchain system. That is why T is not measurable.

4.15.5 Uniqueness of Distributed Ledger in PoWeight

Regarding to the theoretical uniqueness threshold criteria and the necessary physical real world measurements and observations of N and T variables, as a result, it can be concluded that PoWeight type blockchain consensus protocol provides the uniqueness of ledger against having alternative branches on the ledger as long as adversaries don't have more than 33% of the total amount of weighted cryptocurrency coins in PoWeight blockchain system, so that at that time it can be claimed that PoWeight type blockchain system provides verifiable uniqueness. In other words, only under the condition described in the formula (14) with the necessary physical real world measurements and observations, it can be told that there is only one, single, valid, and unique ledger in entire PoWeight type blockchain system. In addition, PoWeight type blockchain system promises partially prevention for block extention on the ledger by the estimated number of blocks needed in average to considered as secure.

4.15.6 Potential Attacks against Uniqueness in PoWeight

34% Attack

Taking the control of more than 34% of total amount of weighted cryptocurrency coins in PoWeight blockchain system is needed in order to conduct a double spending attack as a result of 34% attack [66, 16].

5 Conclusions

The unique ledger in a blockchain system can be in two forms:

In terms of alternative branches (Table 1);

1. The "PoW" and "PoC" have uniqueness conditions parameters of which are, in principle, measurable, but based on the observations and best knowledge, the uniqueness conditions do not hold for the practical implementations of blockchains of these types (e.g. Bitcoin).
2. The "PoS" and other similar type of PoS related consensus protocols such as DPoS, PoSV, PoST, and so on and Byzantine consensus related consensus protocols such as pBFT, dBFT, and so on tend to have unmeasurable parameters in their uniqueness conditions. For example, the "cryptocurrency coins controlled by adversaries" seems to be unmeasurable, at least any physical real world measurements cannot be imagined to reliably determine and keeping track of such parameters.
3. The "PoH" is a good timestamping mechanism, but does not prove the uniqueness of the ledger that uses this mechanism only, because nothing prevents adversaries from building two alternative ledgers in parallel.

Therefore, as long as the adversary-dependent parameters are not measured, the potential risk for compromise of the whole blockchain system always exist and the uniqueness of ledger is under danger. Research in social science may convince us better about the truth of the assumptions based on such parameters.

In terms of blockchain extensions (Table 1); there are two ways of prevension as follows: Fully and partially.

1. DPoS, PoR, dBFT, and PoH can prevent block extensions partially by using the promised estimated block creation time property.
2. PoI and PoWeight can prevent block extensions partially by using the promised block confirmation number property.
3. The other types of blockchain systems can prevent block extensions fully.

	PoW	PoS	DPoS	PoC	pBFT	RPCA	PoI	PoSV	PoST	PoB	PoR	PoA	dBFT	PoH	PoWeight
BS	Bitcoin	Peercoin	Bitshares	Burstcoin	Hyperledger Fabric	Ripple	NEM	Reddcoin	Vericoin	Counterparty	GoChain	VeChain	NEO	Solana	Algorand
N	Total amount of electrical energy in the world	Total amount of cryptocurrency coins in the blockchain	Total amount of cryptocurrency coins in the blockchain	Total amount of data storage in the world	Total number of nodes in the blockchain	Total number of nodes in UNL in the blockchain	Total amount of cryptocurrency coins with good reputation in the blockchain	Total amount of newer cryptocurrency coins in the blockchain	Total amount of older cryptocurrency coins in the blockchain	Total amount of cryptocurrency coins in the eater address in blockchain	Total good reputation score in the blockchain	Total number of companies with authority license in the blockchain	Total number of delegate nodes in the blockchain	NA	Total amount of weighted cryptocurrency coins in the blockchain
MN	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	NA	Yes
T	Total amount of electrical energy consumed by miners	Total amount of cryptocurrency coins controlled by adversaries	Total amount of cryptocurrency coins controlled by adversaries	Total amount of data storage consumed by miners	Total number of nodes controlled by adversaries	Total number of nodes in UNL controlled by adversaries	Total amount of cryptocurrency coins with good reputation controlled by adversaries	Total amount of newer cryptocurrency coins controlled by adversaries	Total amount of older cryptocurrency coins controlled by adversaries	Total amount of cryptocurrency coins in the eater address controlled by adversaries	Total good reputation score controlled by adversaries	Total number of companies with authority license controlled by adversaries	Total number of delegate nodes controlled by adversaries	NA	Total amount of weighted cryptocurrency coins controlled by adversaries
MT	Yes	No	No	Yes	No	No	No	No	No	No	No	No	No	NA	NA
UL (AB)	$T > \frac{N}{2}$	$T < \frac{N}{2}$	$T < \frac{N}{2}$	$T > \frac{N}{2}$	$T < \frac{N}{3}$	$T < \frac{N}{5}$	$T < \frac{N}{2}$	$T < \frac{N}{2}$	$T < \frac{N}{2}$	$T < \frac{N}{2}$	$T < \frac{N}{2}$	$T < \frac{N}{2}$	$T < \frac{N}{3}$	NA	$T < \frac{N}{3}$
UL (BE)	Fully	Fully	Only estimated block creation time	Fully	Fully	Fully	Only promised block confirmation number	Fully	Fully	Fully	Only estimated block creation time	Fully	Only estimated block creation time	Only estimated block creation time	Only promised block confirmation number

Table 1: Uniqueness condition criterias for different blockchain systems

6 Description of the Conclusion Table

Here are the explanations of the abbreviations used in the Conclusion Table (Table 1).

BS: blockchain system.

N: the variable described in the uniqueness conditions for each blockchain system.

MN: the measurability of the variable N.

T: the variable described in the uniqueness conditions for each blockchain system.

MT: the measurability of the variable T.

UN(AB): the unique ledger criteria against Alternative Branches.

UN(BE): the unique ledger criteria against Blockchain Extensions.

References

[1] I. A. I. AlMallohi, A. S. M. Alotaibi, R. Alghafees, F. Azam, Z. S. Khan, "Multi-variable based checkpoints to mitigate the long range attack in proof-of-stake based blockchains", Proceedings of the 3rd International Conference on High Performance Compilation, Computing and Communications, Xi'an, China, March 08-10, 2019.

[2] S. D. Angelis, L. Aniello, R. Baldoni, F. Lombardi, A. Margheri and V. Sassone, "PBFT vs Proof-of-Authority: Applying the CAP Theorem to Permissioned Blockchain," EU H2020 SUNFISH - N.644666 , Southampton, UK, 2018.

[3] A. Ansper, A. Buldas and J. Willemson, "Cryptographic algorithms lifecycle report 2017," Estonian Information System Authority, Tallinn, Estonia, 2018.

[4] M. Apostolaki, A. Zohar and L. Vanbever, "Hijacking Bitcoin: Routing Attacks on Cryptocurrencies," IEEE Symposium on Security and Privacy 2017, San Jose, CA, 2017.

[5] L. M. Bach , B. Mihaljevic and M. Zagar, "Comparative analysis of blockchain consensus algorithms," 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), Opatija, Croatia, 2018.

[6] A. Baliga, "Understanding Blockchain Consensus Models," Persistent Systems, Inc., Santa Clara, CA 95054, 2017.

[7] D. Bayer, Stuart Haber, and W. Scott Stornetta. Improving the Efficiency and Reliability of Digital Time-Stamping, pages 329–334. Springer New York, New York, NY, 1993.

[8] N. Bozic, G. Pujolle and S. Secci, "A tutorial on blockchain and applications to secure network control-planes," 3rd Smart Cloud Networks & Systems (SCNS), Dubai, United Arab Emirates, 2016.

[9] G. Bracha, "Asynchronous Byzantine Agreement Protocols," Information and Computation, vol. 75, pp. 130-143, 1987.

[10] R. M. Bradley and J. M. E. Harper, "Theory of ripple topography induced by ion bombardment," Journal of Vacuum Science & Technology, vol. 6, no. 4, p. 2390, 1988.

[11] C. Cachin, E. Androulaki, A. De Caro, A. Kind, M. Osborne, S. Schubert, A. Sorniotti and M. Vukolic, "Blockchain, cryptography, and consensus," IBM Research Lab., Zurich, June 2017.

[12] C. Cachin and M. Vukolic, "Blockchain Consensus Protocols in the Wild," European Commission through the Horizon 2020 Framework Programme (H2020-ICT-2014-1), Zurich, 2014

[13] M. Castro and B. Liskov, "Practical Byzantine Fault Tolerance and Proactive Recovery," ACM Transactions on Computer Systems, vol. 20, no. 4, p. 398–461, 2002.

[14] C. Catalini and J. S. Gans, "Some Simple Economics of the Blockchain," National Bureau of Economic Research, Cambridge, MA 02138, June 2019.

[15] N. Chalaemwongwan and W. Kurutach, "Notice of Violation of IEEE Publication Principles: State of the art and challenges facing consensus protocols on blockchain," International Conference on Information Networking (ICOIN), Chiang Mai, Thailand, 2018.

[16] J. Chen and S. Micali, "Algorand," arXiv:1607.01341v9 , NY, MA, USA, 2017.

[17] V. Clincy and H. Shahriar, "Blockchain Development Platform Comparison," IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC), Milwaukee, WI, USA, USA, 2019.

[18] T. Crain, V. Gramoli, M. Larrea and M. Raynal, "DBFT: Efficient Byzantine Consensus with a Weak Coordinator and its Application to Consortium," arXiv:1702.03068v3, Sydney, Australia, 2018.

[19] B. David, P. Gaži, A. Kiayias, A. Russell, "Ouroboros Praos: An Adaptively-Secure, Semi-synchronous Proof-of-Stake Blockchain, In: Nielsen J., Rijmen V. (eds) Advances in Cryptology – EUROCRYPT 2018. EUROCRYPT 2018. Lecture Notes in Computer Science," vol 10821. Springer, Cham, 2018.

[20] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher and F. Wang, "Secure and Trustable Electronic Medical Records Sharing using Blockchain," AMIA Annu Symp Proc., p. 650–659, 2017.

[21] D. Dolev and R. Reischuk , "Bounds on Information Exchange for Byzantine Agreement," IBM Research Laboratory, San Jose, CA 95155, 1982.

[22] D. Dolev and H. R. Strong, "Authenticated algorithms For Byzantine Agreement," Society for Industrial and Applied Mathematics, vol. 12, no. 4, 1983.

[23] D. Dolev, R. Reischuk and H. R. Strong, "Early Stopping in Byzantine Agreement," Journal of the Association for Computing Machinery, vol. 37, no. 4, pp. 720-741, 1990.

[24] M. J. Fischer, N. A. Lynch and M. S. Paterson, "Impossibility of Distributed Consensus with One Faulty," Journal of the Asscktion for Computing Machinery, vol. 32, no. 2, pp. 374-382, April 1985.

[25] F. Gai, B. Wang, W. Deng, W. Peng, "Proof of Reputation: A Reputation-Based Consensus Protocol for Peer-to-Peer Network. In: Pei J., Manolopoulos Y., Sadiq S., Li J. (eds) Database Systems for Advanced Applications. DASFAA 2018. Lecture Notes in Computer Science", vol 10828. Springer, Cham, 2018.

[26] M. Glinz, "On Non-Functional Requirements," in 15th IEEE International Requirements Engineering Conference, Delhi, India, 2007.

[27] M. Glinz , "Rethinking the Notion of Non-Functional Requirements," in Third World Congress for Software Quality, Zurich, Switzerland, 2005.

[28] V. Gramoli, "From blockchain consensus back to Byzantine consensus," Elsevier B.V, Amsterdam, 2017.

[29] R. Guerraoui, N. Knezevic, V. Quema, and M. Vukolic. The next 700 BFT protocols. In Eurosys '10: Proceedings of the 5th ACM SIGOPS/EuroSys European Conference on Computer Systems, pages 363–376, 2010.

[30] P. J. Haas and J. M. Hellerstein, SIGMOD '99 Proceedings of the 1999 ACM SIGMOD international conference on Management of data, vol. 28, no. 2, pp. 287-298, 1999.

[31] S. Haber, W.S. Stornetta, "How to time-stamp a digital document," In Journal of Cryptology, vol 3, no 2, pages 99-111, 1991.

[32] J. Hackfeld, "A lightweight BFT consensus protocol for blockchains," arXiv:1903.11434v2, CA, USA, 2019.

[33] E. Heilman, A. Kendler, A. Zohar and S. Goldberg, "Eclipse Attacks on Bitcoins Peer-to-Peer Network," in 24th Usenix Security Symposium Security 15, Washington, D.C., Usenix Association, 2015, pp. 129-144.

[34] D. HongFei and E. Zhang, "NEO White Paper," https://docs.neo.org/docs/en-us/basic/whitepaper.html, China, 2014.

[35] S. King and S. Nadal. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. peercoin.net, 2013.

[36] S. Kitts and Nevis, "GoChain: Blockchain at Scale Version 1.0," https://neironix.io/documents/whitepaper/3901/gochain-whitepaper-v1.pdf, 2018.

[37] A. Kolonin, B. Goertzel, D. Duong and M. Ikle, "A Reputation System for Artificial Societies," Aigents Group and SingularityNET Foundation, Novosibirsk, Russia and Amsterdam, Netherlands, 2017.

[38] R. Kotla and M. Dahlin, "High throughput Byzantine fault tolerance," International Conference on Dependable Systems and Networks, Florence, Italy, 2004, pp. 575-584, 2004.

[39] L. Lamport, R. Shostak and M. Pease, "The Byzantine Generals Problem," ACM Transactions on Programming Languages and Systems, vol. 4, no. 3, pp. 382-401, July 1982.

[40] L. Lamport, R. Shostak and M. Pease, "Reaching Agreement in the Presence of Faults," Journal of the Association on for Computing Machinery, vol. 27, no. 2, pp. 228-234, 1980.

[41] D. Leffingwell, "Agile Software Requirements: Lean Requirements Practices for Teams, Programs, and the Enterprise," Addison-Wesley Professional, Westford, Massachusetts, 2010.

[42] W. Li, S. Andreina, J. M. Bohli and G. Karame, "Securing Proof-of-Stake Blockchain Protocols," NEC Laboratories Europe, Germany, 2017.

[43] W. Li, S. Andreina, J. M. Bohli, G. Karame, "Securing Proof-of-Stake Blockchain Protocols. In: Garcia-Alfaro J., Navarro-Arribas G., Hartenstein H., Herrera-Joancomartí J. (eds) Data Privacy Management, Cryptocurrencies and Blockchain Technology. DPM 2017, CBT 2017. Lecture Notes in Computer Science," vol 10436. Springer, Cham, 2017.

[44] J. Mattila, "The Blockchain Phenomenon - The Disruptive Potential of Distributed Consensus Architectures," Berkeley Roundtable on the International Economy (BRIE), Berkeley, CA 94720, 2016.

[45] J. P. Martin and L. Alvisi, "Fast byzantine consensus," IEEE Trans. Dependable Secur. Comput., 3(3):202–215, July 2006.

[46] R. C. Merkle. Secrecy, Authentication, and Public Key Systems. PhD thesis, Stanford, CA, USA, 1979. AAI8001972.

[47] R. C. Merkle, "Protocols for public key cryptosystems," In Proc. 1980 Symposium on Security and Privacy, IEEE Computer Society, pages 122-133, April 1980.

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

[49] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," www.bitcoin.org, 2008.

[50] M. Nofer, P. Gomber, O. Hinz and D. Schiereck, "Blockchain," Bus Inf Syst Eng., vol. 59, no. 3, pp. 183-187, 2017.

[51] G. Pîrlea and I. Sergey, "Mechanising blockchain consensus," in Proceedings of the 7th ACM SIGPLAN International Conference on Certified Programs and Proofs, Los Angeles, CA, USA , 2018.

[52] A. Poelstra, "Distributed Consensus from Proof of Stake is Impossible," 2014.

[53] H.F. Ouattara, D. Ahmat, F.T Ouédraogo, T.F. Bissyandé, O. Sié, "Blockchain Consensus Protocols", In: Odumuyiwa V., Adegboyega O., Uwadia C. (eds) e-Infrastructure and e-Services for Developing Countries. AFRICOMM 2017. Lecture Notes of the Institute for Computer Sciences, Social Informatics and Telecommunications Engineering, vol 250. Springer, Cham, 2018.

[54] M. Rabin, "Digitalized signatures and public-key functions as intractable as factorization", MIT Laboratory for Computer Science, 1979.

[55] L. Ren, "Proof of Stake Velocity: Building the Social Currency of the Digital Age," www.redcoin.com, 2014.

[56] F. Saleh, "Blockchain Without Waste: Proof-of-Stake," Available at SSRN: https://ssrn.com/abstract=3183935 or http://dx.doi.org/10.2139/ssrn.3183935, May 2019.

[57] L. S. Sankar , M. Sindhu and M. Sethumadhavan, "Survey of consensus protocols on blockchain applications," 4th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2017.

[58] S. Schmid, "The Distributed Computing Column," Aalborg University Selma Lagerlöfs Vej 300, DK-9220, Aalborg, Denmark, 2017.

[59] D. Schwartz, N. Youngs and A. Britto, "The Ripple Protocol Consensus Algorithm," https://arxiv.org/abs/1802.07242, 2018.

[60] B. Shehar, A. Sonnino, M. A. Bassam, S. Azouvi, P. McCorry, S. Meiklejohn, and G. Danezis. 2019. SoK: Consensus in the Age of Blockchains. In 1st ACM Conference on Advances in Financial Technologies (AFT '19), October 21–23, 2019, Zurich, Switzerland. ACM, New York, NY, USA, 16 pages. https://doi.org/10.1145/3318041.3355458

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

[62] N. Stifter, A. Judmayer, . P. Schindler, A. Zamyatin and E. Weippl, "Agreement with Satoshi – On the Formalization of Nakamoto Consensus," Christian Doppler Laboratory for Security and Quality Improvement in the Production System Lifecycle, London, 2018.

[63] M. Tarasiewicz and A. Newman, "Chapter 10 - Cryptocurrencies as Distributed Community Experiments," in Handbook of Digital Currency, Elsevier Inc., 2015, pp. 201-222.

[64] O. Vashchuk and R. Shuwar, "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, no. 9, p. 106–112, 2018.

[65] L. Wong, "NEM Tehcnical Reference Version 1.2.1," Dragonfly Fintech Pte. Ltd, 2018.

[66] A. Yakovenko, "Solana: A new architecture for a high performance blockchain v0.8.14," https://solana.com › solana-whitepaper, San Francisco, CA, 2017.

[67] J. Yli-Huumo, D. Ko , S. Choi, S.Park, K. Smolander, "Where Is Current Research on Blockchain Technology?—A Systematic Review," PLoS ONE 11(10): e0163477. https://doi.org/10.1371/journal.pone.0163477, 2016.

[68] G. Yuval. How to Swindle Rabin. Cryptologia, 3(3):187–191, 1979.

[69] Z. Zheng, S. Xie, H. N. Dai, X. Chen and H. Wang, "Blockchain challenges and opportunities: a survey," Int. J. Web and Grid Services, vol. 14, no. 4, 2018.

[70] Z. Zheng, S. Xie, H. N. Dai, X. Chen and H. Wang, "An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends," in IEEE 6th International Congress on Big Data, Honolulu, Hawaii, USA, 2017.

[71] J. Buntinx, "Themerkl," 21 May 2017. https://themerkle.com/what-is-proof-of-importance/

[72] E. Deirmentzoglou, "Rewriting History: A Brief Introduction to Long Range Attacks," 31 May 2018. https://blog.positive.com/rewriting-history-a-brief-introduction-to-long-range-attacks-54e473acdba9

[73] Feyd27, "On 51% Attacks: The Architecture Of Aggression," 22 October 2018. https://medium.com/datadriveninvestor/on-51-attacks-the-architecture-of-aggression-57f105517328

[74] D. Frumkin, A. Dean and T. Shaddox, "Nothing-at-stake problem," https://golden.com/wiki/Nothing-at-stake_problem, August 2015.

[75] S. Gauld, . F. . v. Ancoina and R. Stadler, "The Burst Dymaxion," CryptoGuru PoC SIG, 2017.

[76] N. Houy, "It Will Cost You Nothing to 'Kill' a Proof-of-Stake Crypto-Currency," Available at SSRN: https://ssrn.com/abstract=2393940 or http://dx.doi.org/10.2139/ssrn.2393940, January 2014.

[77] J. Hovell and D. Yziz, "What's a Sybil attack?," https://bitcoin.stackexchange.com/questions/50922/whats-a-sybil-attack, 2017.

[78] O. Kharif and C. Yasiejko, "Man Who Claims To Be Bitcoin's Inventor Registers Copyright for Its Code," 21 May 2019. https://www.bloomberg.com/news/articles/2019-05-21/bitcoin-s-supposed-inventor-says-he-won-copyright-registration

[79] M. Moos, "Analysis: Bitcoin Costs $1.4 Billion to 51% Attack, Consumes as Much Electricity as Morocco," https://cryptoslate.com/analysis-bitcoin-costs-1-4-billion-to-51-attack-consumes-as-much-electricity-as-morocco/, 2018.

[80] H. Mossh, clam0 and hylsceptic, "What is a Long Range Attack," 2018. https://delegatecall.com/questions/what-is-a-long-range-attack-59546170-a313-4eb6-bd0c-7505c6096e90

[81] A. N. Osato, "Bitcoin 51% Attack is unrealistic, New Study Concludes," https://bitcoinist.com/bitcoin-51-percent-attack-study/, 2018.

[82] D. Pike, P. Nosker, D. Boehm, D. Grisham, S. Woods and J. Marston, "Proof-of-Stake-Time," VeriCoin, 2014.

[83] A. Rosic, "Hypothetical Attacks on Cryptocurrencies," https://blockgeeks.com/guides/hypothetical-attacks-on-cryptocurrencies/, 2017.

[84] P. Vasin, "BlackCoin's Proof-of-Stake Protocol v2," www.blackcoin.co.

[85] D. Vranjicic, "Peercoin Explained: The Proof of Stake Pioneer," 11 March 2018. https://bitfalls.com/2018/03/11/peercoin-explained-proof-stake-pioneer/

[86] Announcements, Tech, Updates, " "Fake Stake" Official PIVX Report," 20 Feburary 2019. https://pivx.org/fake-stake-official-pivx-report/

[87] "The Blockchain Company," GoChain, https://gochain.io/?source=post_page——

[88] B. B. Foundation, "Bitshares Blockchain," 29 November 2018. https://github.com/bitshares-foundation/bitshares.foundation/blob/master/download/articles/Bit-SharesBlockchain.pdf.

[89] "CoinMarcetCap - Peercoin," 1 Jully 2019. https://coinmarketcap.com/currencies/-peercoin/

[90] "CounterpartyXCP/Documentation," https://github.com/Counterparty-XCP/Documentation/blob/master/Developers/protocol_specification.md, 2018.

[91] "Delegated Proof-of-Stake Consensus," BitShares Blockchain Foundation, https://bitshares.org/technology/delegated-proof-of-stake-consensus

[92] V. Foundation, "Medium," 8 May 2018. https://medium.com/@vechainofficial/defining-the-vechainthor-blockchain-consensus-proof-of-authority-8cf3f51a5fa0

[93] "Functional and Non-Functional Requirements: What's the Difference?," Lvivity HQ, 20 Feburary 2019. [Online]. Available: https://lvivity.com/functional-and-non-functional-requirements.

[94] Gitbook, "Proof of Stake Velocity," Tokens-economy.gitbook.io, August 2018. https://tokens-economy.gitbook.io/consensus/chain-based-proof-of-stake/proof-of-stake-velocity

[95] IBM, "Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains," https://arxiv.org/pdf/1801.10228.pdf, 2018.

[96] "Peercoin - Pioneer of Proof of Stake," 19 August 2012. https://www.peercoin.net/.

[97] Qtum, "Re: "Fake Stake" attacks on chain-based Proof-of-Stake cryptocurrencies," 2018. https://blog.qtum.org/re-fake-stake-attacks-on-chain-based-proof-of-stake-cryptocurrencies-f26d58dc8f46

[98] Quibus, "Technical information about mining and block forging," 21 October 2017. https://forums.getburst.net/t/technical-information-about-mining-and-block-forging/943

[99] "Total market cap: $293,890,510,485," 1 July 2019. https://cryptolization.com/bitshares

[100] "Vechain - Development Plan and Whitepaper Version 1.0," https://cdn.vechain.com/vechainthor_development_plan_and_whitepaper-_en_v1.0.pdf, China, 2018