Article

A Study on Public Blockchain Consensus Algorithms: A Systematic Literature Review

Islahuddin Jalal [1]*, Zarina Shukur [2] and Khairul Azmi Abu Bakar [2,]

Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Malaysia [1, 2]

Faculty of Computer Science, Shaheed Rabbani Education University, Afghanistan [1]

islahuddinjalal@yahoo.com (I.J.); zarinashukur@ukm.edu.my (Z.S.); khairul.azmi@ukm.edu.my (K.A.)

* Correspondence: islahuddinjalal@yahoo.com; Tel.: +93-77-734-0828

Abstract: The purpose of this study is to present a systematic review of the literature on public blockchain consensus algorithms. Blockchain consensus algorithms have gain much popularity in last few years especially in the cryptocurrency field. Based on a systematic review of the relevant literature, we provide a classification of blockchain consensus algorithms, philosophy behind creation of blockchain consensus algorithms and as well as the rewards and incentive strategies of various public blockchain consensus algorithms. On the basis of these results, the research gaps and future work directions are identified for further study.

Keywords: blockchain consensus; consensus algorithms; rewards; incentives

1. Introduction

The evolution of consensus technology has more than four decades of history. It is re-birth with the evolution of blockchain technology [1]. It is the basic technology of the most popular cryptocurrency of the world "Bitcoin" proposed in the white paper [2] of an unknown person called "Satoshi Nakamoto". Blockchain is the most addressable technology, which caught the attention of different societies like businesses, education industries and researchers [3], [4] etc. in the world is blockchain. This attraction or interest is due to its unique nature of decentralization, anonymity, irreversibility, integrity and security [5].

Consensus is the agreement among different nodes in a distributed system and is considered a problem. This research topic has long history in the field of distributed and fault tolerant computing [6] but got hype in blockchain technology. Consensus is at the heart of many distributed algorithms and is one of the most fundamental problems in distributed and fault tolerant computing [7]. For example, it can be used as a basis for performing active replication, as in a replicated state machine approach [8], or used to apply data object simultaneously without waiting between a set of processes.[9].

These consensus algorithms are designed with different concepts behind, such as scalability, liveness, safety, latency, energy consumption, fault tolerance, throughput issues and more. Some consensus algorithms like [10], [11] and [12] cover the order of transactions, the choice of leaders, and transaction selection for block but lacking the fairness in mining strategy for ordinary users in the public blockchain system.

The rest of this article is compiled as follows. In part 2 we provide background of blockchain technology, blockchain anatomy and its classification. The methodology of this study, research questions, search process, article selection process and specified collected public blockchain consensus algorithms are discussed in Section 3. Section 4 presents the results of the study. Further, the discussion of this study is presented in Section 5 along with answers to the research questions. This article is concluded with conclusion along with future work in Section 6.

 doi:10.20944/preprints202011.0355.v1

2. Materials and Methods

The purpose of this study is to point out the available public blockchain consensus algorithms, their incentive strategy, consensus strategy and whether they provide fairness to ordinary users in terms of gaining incentives as a miner. In order to fulfill the goal, we designed the research questions as *RQ1: What are the available consensus algorithm for public blockchain systems which provide fairness?* and *RQ2: What are the reward winning and incentive strategies of various consensus algorithms for public blockchain systems?*

The RQ1 aims to discover the available public blockchain consensus algorithms in the literature and also to know the fairness they possess for the ordinary users to become a miner and gain incentives from the system. The RQ2 tries to showcase the incentive and consensus strategy they have been using, in order to know whether these incentive and consensus strategy helps the ordinary user to participate as a miner without any expenses.

2.1 Search Process

In this study, systematic literature review method was used in accordance with the principles put forward by Kitchenham [13]. To cover a large number of relevant publications, we decided to look for the following widely known and widely used electronic libraries: Google Scholar, IEEE Xplore, SpringerLink, Science Direct and SSRN.

The strings of keyword used were: "Public blockchain consensus algorithms". In the next step, we decided in which section of the articles we will use the search terms. To get a reasonable number of results, we searched the keyword strings in the title and abstract of the article. We limited our search to publications written in the English language and selected as a content type journals, white papers and conference papers. No restrictions on the article release date were used.

We applied the same query "Public blockchain consensus algorithms" to all the specified electronic libraries, they retrieved the following results shown in the following Table 1.

Table 1. Search Results

S/No	Electronic Library Name	Retrieved Results
1	Google Scholar	4330
2	SpringerLink	488
3	IEEE Xplore	35
4	ScienceDirect	1219
5	SSRN	2
	Total Retrieved Result	6074

2.2 Articles Selection Process

Some search engines (like google scholar and springer link) do not have advance search option for confining the search towards the required purpose so, therefore we pre-defined some terms ("Consensus protocol", "Consensus mechanism", "Consensus algorithm" and "Blockchain consensus") for scanning the title and abstract to exclude the un-necessary articles shown in the search.

Our articles selection process has two phases (1. Title scanning phase and 2. Abstract scanning phase). In the title scanning phase, we scan for the pre-defined terms in the title and selected those titles which include the pre-defined terms and excluding all other articles from selection process. After the title scanning phase, we included 173 articles for the second phase which are shown in Table 2.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 November 2020 doi:10.20944/preprints202011.0355.v1

Table 2: Summary of Title Scanning Phase

S/No	Electronic Library Name	Title scanning Result
1	Google Scholar	117
2	SpringerLink	39
3	IEEE Xplore	9
4	ScienceDirect	8
5	SSRN	0
	Total Retrieved Result	173

In the second phase which is "abstract scanning phase", 173 articles' abstracts were studied for the pre-defined terms in the public blockchain systems as defined in the main query. This phase also defined the scope of the study. The final number of papers that we gathered after removing duplicates and irrelevant articles to our research is 36 as shown in Table 3.

Table 3. Summary of Abstract Scanning Phase

S/No	Electronic Library Name	Abstract scanning Result
1	Google Scholar	10
2	SpringerLink	15
3	IEEE Xplore	7
4	ScienceDirect	4
5	SSRN	0
	Total Retrieved Result	36

From these 36 papers, we extracted information for the research questions. After studying these articles in detail, we collected 25 blockchain consensus algorithms which are mostly studied by different researchers and industries. The collected blockchain consensus algorithms are as shown in Table 4.

Table 4. Blockchain Consensus Algorithms

Blockchain Consensus Algorithms (BCA)				
S/No	BCA	Authors	Years	Reference
1	Proof of Work (PoW)	Satoshi Nakamoto	2008	[2]
2	Proof of Stake (PoS)	QuantumMechanic	2012	[14]
3	Delegated PoS (DPoS)	Dan Larimer	2013	[15]
4	Tindermint	Jae Kwon	2014	[16]
5	Ripple	Schwartz, D Youngs, N Britto, A	2014	[17]
6	PoS Velosity (PoSV)	Ren, Larry	2014	[18]
7	BFT SMart	Bessani, Alysson Sousa, João Alchieri, Eduardo E P	2014	[19]
8	Raft	Diego Ongaro and John Ousterhout	2014	[20]
9	Proof of Authority (PoA)	Gavin Wood	2015	[21]
10	Stellar Consensus Protocol (SCP)	Mazieres, David	2016	[22]
11	Hashgraph	Leeman Baird	2016	[23]
12	HoneyBadgerBFT	Miller, Andrew Xia, Yu Croman, Kyle Shi, Elaine	2016	[11]

 doi:10.20944/preprints202011.0355.v1

13	Proof of Luck	Song, Dawn Mitar Milutinovic, Warren He, Howard Wu and Maxinder Kanwal	2016	[24]
14	Proof of Elapsed Time (PoET)	Intel	2016	[25]
15	Proof of Vote (PoV)	Li, Kejiao Li, Hui Hou, Hanxu Li, Kedan Chen, Yongle	2017	[26]
16	PoS Casper	Buterin, Vitalik Griffith, Virgil	2017	[27]
17	Proof of Personhood (PoP)	Borge, Maria Kokoris-Kogias, Eleftherios Jovanovic, Philipp Gasser, Linus Gailly, Nicolas Ford, Bryan	2017	[28]
18	Proof of Contribution (PoC)	Tengfei Xue	2018	[29]
19	YAC-BFT	Fedor Muratov, A. Lebedev, Iushkevich, Nasrulin, Taemiya	2018	[30]
20	Proof of Trust (PoT)	Jun Zou, Bin Ye, Lie Qu, Yan Wang, Mehrnet Orgun and Lei Li	2018	[31]
21	Proof of Participation and Fees (PoPF)	Fu, Xiang Wang, Huaimin Shi, Peichang Mi, Haibo	2018	[32]
22	Proof of Disease (PoD)	Talukder, Asoke K. Chaitanya, Manish Arnold, David Sakurai, Kouichi	2018	[33]
23	CloundPoS	Tosh, Deepak Shetty, Sachin Foytik, Peter Kamhoua, Charles Njilla, Laurent	2018	[34]
24	Proof of Majority (PoM)	Kim, Jun Tae Jin, Jungha Kim, Keecheon	2018	[35]
25	DPBFT	Hao, Xu Yu, Long Zhiqiang, Liu Zhen, Liu Dawu, Gu	2018	[36]

 doi:10.20944/preprints202011.0355.v1

After collected the blockchain consensus algorithms, we classified blockchain consensus algorithms based on the classification scheme of the blockchain system in order to direct our study towards the research aim. Blockchain consensus algorithms are classified as shown in Figure 1.

- Public Blockchain Consensus Algorithms (PuBCA)
- Consortium Blockchain Consensus Algorithms (CBCA)
- Private blockchain consensus algorithms (PrBCA)

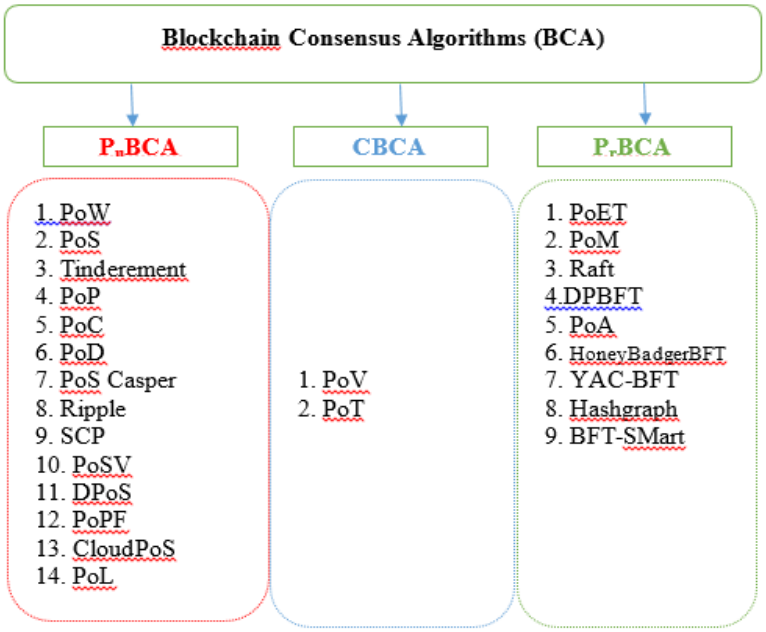

Figure 1. Classification of Blockchain Consensus Algorithms

After the classification of the collected blockchain consensus algorithms, we limited our scope to public blockchain consensus algorithms (PuBCA) and excluded the consortium blockchain consensus algorithms (CBCA) and private blockchain consensus algorithms (PrBCA) from the study. We downloaded the white papers of PuBCA which are not available in the final selected papers for the study. We performed the in-depth study of the white papers and articles related to PuBCA.

3. Results

In this section, the literature review of the study regarding public blockchain consensus algoirthms are organized in order to reflect the answers for the research questions as discussed in the methodology section of the study.

3.1. Overview of Public Blockchain Consensus Algorithms (PuBCA)

The overview of Public blockchain consensus algoirthms (PuBCA) are as follow:

3.1.1. Proof of Work (PoW)

PoW [2] is designed for Bitcoin blockchain. The consensus is made in the Bitcoin system by posting transactions to all nodes in the system. Each node of the blockchain system receives a new transaction and adds it to the block. This process is complicated, and requires a high-performance computing resources like Application Specific Integrated Circuit (ASIC) or Graphics Processing Units (GPU). These computing devices are expensive and ordinary users cannot afford to purchase these devices. Due to which, the system goes to the hands of the rich people. The miner does not know the number of iterations to find the required hash value, but easily verify the process. When a node finds the required Proof-of-Work value, it sends the block to all nodes in the blockchain system. Other nodes accept the block only if all transactions in it are valid and have not been used. Once approved,

 doi:10.20944/preprints202011.0355.v1

each node uses the previous hash value to connect the block to a previously agreed blocks, thus forming a blockchain. The blockchain functions are like a transaction ledger and along with the mining process, the Nakamoto Bitcoin protocol can solve the critical problem of double-spending in cryptocurrency without a central authority, and assumes that honest nodes handle most of the CPU power in the bitcoin network. Honest nodes do not cooperate with malicious nodes to attack the system. More than one miner may discover a hash value at the same time, and it is called a fork. Thus, the longest blockchain represents the consensus of transaction history [37].

The winner gets a reward of 6.25 bitcoins, and it is reduced to half every four years. In the PoW consensus, there is also a chance of 51% attacks where the mining pool controls 51% of mining power. Though, the mining pools are valuable for collecting a large amounts of computing capabilities but it is not fair with new node to connect alone to the network and get the mining reward. Because new node or individual does not have as much computing power as that of mining pool [37]. According to [5], the estimated operating cost of the bitcoin network using PoW as a consensus algorithm is 23.88 billion Euros over four and a half year. This is 45% higher than the actual price of bitcoin.

3.1.2. Proof-of-Stake (PoS)

Proof-of-Stake is designed as an alternative consensus algorithm to PoW, which is the resource wasting, Concentration of hash power and slow speed of transactions [38]. In this, the miner should have a stake which is approximately equal to 2000 USD. The PoS algorithms randomly select miner for block creation, and no miner can predict its turn in advance. The miners produce a block and added to the blockchain. The miner will be rewarded, and if it fails to add a block in the blockchain, then the miner will be fined as much as the reward. The mining depends on the amount of stake a person has in the system. If a miner has more stake in the blockchain, the chances of mining are more. For instance, If the stake in the given crypto-currency is at 1%, you can mint up-to 1% of the transactions [39].

3.1.3. Tindermint

Tindermint [16] is designed to address the speed, scalability, and environmental issues which are available in the PoW. It is based on PBT algorithm. The blockchain using the tendermint can handle about 33% byzantine actors in the network. It is compatible in any programming language. Validator is in charge of validating transactions and committing new blocks to the blockchain. Validators are taking part in the consensus protocol by broadcasting cryptographic signatures which act as votes to extend the blockchain. The user who wants to become a validator in the tendermint network must hold some amount for some time and locked it as voting power. Delegation concept is used in the tendermint system. The delegators are putting their staking tokens at stake with a validator of their choice. Chance of losing these tokens are present if the validator is not working according to the rules defined by the protocol. There are at least four validators required in the tendermint consensus and have no limit for the maximum number of validators.

Cosmos project running tendermint as a consensus protocol having 100 validators, but will increase to 300 validators. Block requires 3 seconds to be finalized, but it can be achieved in a second as well. The finality of a block is dependent on the number of validators. Nothing-at-stake problem which is present in the PoS solved in the tendermint by bond deposit. The releasing of the bond deposits requires un-locking it for some specific period, which is called un-bonding period in the tendermint network. The unlocking period is about two to three months. The chance of the fork is possible. It is due to the 1/3 of the majority of validators signs duplicitously of multiple blocks at the same time in the tendermint blockchain, but the validators identified causing fork will face a substantial charge of losing the amount of 1/3 of the locked stake [40].

3.1.4. Proof of Luck (PoL)

Proof of Luck [24] is applicable in the TEE of Intel SGX platforms and can be applied to other platforms with similar properties of the TEE of the SGX as well. The goal of development of this

 doi:10.20944/preprints202011.0355.v1

protocol is to overcome the issues available in the previously available consensus algorithms like slowness, consumption of energy, and using lots of time.

It uses the hardware which is not commonly available, which causes unfairness to society and only help those people having specific custom hardware. It is secured due to the TEE where the attacker cannot control the blockchain without controlling a majority of CPUs and without breaking the TEE platform. The participant is calling the PoLRound function and passing the latest block to a particular chain at the start of every round. When the ROUND_TIME expires, the participant calls the PoLMine function for creating a new block and will be connected with the previous block by passing the headers of the new block. Sometimes the previous block may be different from the roundblock then we have to see that the last block and round block have the same parents.

It ensures that participants wait for ROUND_TIME between mining blocks while allowing them to switch to the more lucky block if they receive the lucky block while they wait. The PolMine function generates a random value of [0,1] from the uniform distribution, which is used to find out the winning block from all mining blocks of all participants in this round. In this algorithm, a shorter delay time represents the winner, and a longer delay means that the information dependent on f (I) releases the unluckier. If a participant receives a lucky block before the mining is completed, there is no need to broadcast the block.

3.1.5. Proof of Personhood (PoP)

The philosophy behind designing PoP is security in order to protect Sybil and double spending attack. It provides pseudonym accountability by linking the real world people with the minting process. In this process, RandHound algorithm, Pseudonym party and ByzCoin protocol are used. The people who wish to mint the coin, they first join the pseudonym party to become the member of the PoP. They have to go to a specific place where the pseudonym party is hosted and arranged. Without attending the pseudonym party, once cannot become a member of the blockchain system in terms of minting. Each member in the party receive one token which will be used for authentication, validation and RandHound function. This token will be for a specific period of time during which the valid token holder can mint. All minters have equal chance of winning the reward of creation of a new block because each minting pool member's assigned only one token. The RandHound process is repeated until all the token holder get the chance of creating a new block and get of its reward [28].

3.1.6. Proof of Contribution (PoC)

PoC [29] consensus protocol combines the Concept of PoW and PoS algorithms by slight modification of introducing the "Success time" concept and "success time value" as a stake respectively. Success time adjusting the difficulty value for a miner. If success time value is greater, the difficulty value will be simpler to the miner, which causes mining dependency on success time value. If the miner has high value of success time has the high chance of mining reward of a new block creation. In contrast to PoW and PoS, the PoC provides penalty for deceptive activity by setting the success time value to zero and also add the address of the deceptor to blacklist which will be publically available. The miner will ignore the block if the address of the deceptor is found in the blacklist and no one will make transaction with the blacklisted address.

3.1.7. Ripple

Ripple protocol [17] basically designed for the ripple cryptocurrency to focus on latency issues aroused from the Byzantine failures. Each node is communicating with others node in its "Unique Node List" (UNL), which is a server containing others ripple nodes for consensus in the Ripple environment. Each node is defining UNL. Consensus in the ripple environment is done in multiple rounds. In first round, each node receive transactions and add them in a public list called "candidate set" and then relay its candidate sets to other nodes in its UNL. Nodes in the UNL validate the transactions by voting on them and broadcast the result of votes among the nodes in the UNL. Each node arrange its candidate set and transactions received the highest number of votes are passed to the next round. When a candidate set receives approximately 80% or more of votes from all the

 doi:10.20944/preprints202011.0355.v1

available nodes in the UNL, then that candidate set wins the voting and becomes a valid block which is called the "Ledger" in the Ripple environment. This ledger is considered the "Last Closed Ledger (LCL)" and added to the Ripple blockchain by each node in the UNL. The transactions which are not qualified in voting along with the new transactions will join the next round of consensus. In this way the consensus process continues until all the transactions are validated and added to LCL.

3.1.8. Stellar Consensus Protocol (SCP)

The quorums and quorum slices concept are used in Stellar Consensus protocol algorithm [22]. A Quorum is a group of nodes sufficient to reach an agreement. A quorum slice is a part of a quorum that can convince a particular node about agreement. Individual nodes can appear in several parts of the quorum. Stellar introduced quorum slices to allow each individual node to select a group of nodes in its slice so as to allow open participation. These quorum and quorums' slices are based on real-life business relationships between various entities to the point leveraging trust existing in business models. To reach global consensus across the systems, quorums must cross. The overall consensus is reached globally from decisions made by individual nodes. The consensus protocol works as follows. Each node first makes a preliminary vote on transactions, also generally considered a statement. This is the first step in the allied voting process. Each node select its statement and will not select another statement that conflicts with its choice. However, it can accept a different statement if its quorum slice has received a different statement. The second step is the acceptance step. The node receives a statement if it has never received a statement that conflicts the current statement and each node in its v-block group has received that statement. A v-blocking set is a group of nodes each of the quorum slice that constitute the current node. Quorum slices affect each other leading to quorums agreeing with a particular statements. This step is known as confirmation when all quorum members agree with the statement. Verification is the final step in the voting process and signifies system level agreement. This step ensures that nodes send each other confirmation messages until everyone agrees on the final value of the state in the system.

3.1.9. Proof of Stake Velocity (PoSV)

Proof of Stake Velocity [18] is designed for Reddcoin in 2014, which is a digital social currency for both ownership of stake and its velocity. It is opposed to PoW and PoS which are used in the commercial digital currencies such as bitcoin and ethereum etc. it covers the social and commercial weaknesses available in the PoW and PoS based network. PoSV patched up the limitation available in the PoS, which is incentivizing the minter more for keeping the stake for a long period of time which is based on linear coin age function as compared to active members. Coin age function is replaced by exponential decay function used in the PoSV. It means that the PoSV based network encourages the stakeholder to be active and moving their stakes in the network. It also encourage stake holders to stay online and verify the transactions in order to increase the chance of getting incentives.

3.1.10. Proof of Stake Casper (PoS Casper)

Proof of Stake with Casper the Friendly Finality Gadget Protocol [1] is designed for Fair validation Consensus in Ethereum. It is removing the unfair advantage of the richer miners and fair validation of the transactions by proposing a system with Casper Proof of Stake which solved the problem "Nothing at stake problem" which is available in the PoW and PoS based blockchain network. The PoS algorithm is modified with some extra features which are as follow:

- Accountability: Violations of the rule can easily be detected and the guilty verdict are is punished by reducing their deposits
- Dynamic validators: validators can easily join and withdraw from the validators set with certain delay
- Defenses: Casper has the capability to withstand attacks and long-range review attacks where> ½ validators are disconnected

 doi:10.20944/preprints202011.0355.v1

- Modular overlay: The Casper design consists of an overlay on the existing Proof of work chain, making it easy to implement.

The voting for transaction validation criteria which are mentioned in this algorithm are 2/3 of the validator's stake can reach consensus and ½ of validators' votes. If both the conditions are true then the validation of transaction is accepted otherwise vote continues. The validator who validate the wrong transaction will be fined and its stake will be zero and a small amount reward will be given to the person who identified the validator's fault. They identified the checkpoint for the validators to cast vote and the checkpoint is equal to the set of 100 blocks due to which efficiency will be achieved.

Casper Proof of stake has not been implemented yet there is some ambiguity of its implementation in real system, how it will be implemented. There is a need of further study or solution of Casper's problem where the validator's stake burnt and exited from the validators set and rejoining the validator set again. Ethereum is working on these problems.

3.1.11. Proof of Participation and Fee (PoPF)

Proof of Participation and Fees (PoPF) [41] consensus algorithm is designed for blockchain based joint cloud computing. It is based on PoW consensus algorithm. There is no competition among all the users for each block generation. In the PoPF, some percentage of top ranking users are chosen as accountant candidates for each block generation. The ranking is defined by users' participation and fees in the previous transaction. This algorithm is not working at the beginning of the JCLedger because it require certain number of users and its participation and fee, therefore, initially pow consensus algorithm is used until the condition is satisfied. Each node will check the PoPF operation conditions every time it adds a block. When the number of users in the history blocks is greater than the set threshold n. the node will switch the PoW consensus approach to PoPF consensus approach. The mining difficulty of PoPF depends on user's ranking. The mining difficulty value is easier for the higher rank user as compared to the lower rank users. The valid block can be added to the ledger and if the block is not valid, the users dump the block and punish the accountant by setting the difficulty value more difficult for the next block generation.

3.1.12. CloudPoS

Cloud Proof of stake (CloudPoS) [34] consensus algorithm is designed to work well in the integration of blockchain with cloud environment. It modifies the concept of stake of the original PoS. Instead of cryptocurrency, the CPU power, network and memory are holding as a stake with Cloud Service Provider (CSP). CloudPoS works based on epoch and each epoch of the consensus has five phases which are as follow:

- Stake determination
- Resource staking and confirmation
- Leader election
- Block replication and verification
- Reward distribution

In CloudPoS, the validators are flexible in terms of joining and leaving the network as a validator any time but joining the network as a validator is possible only at the start of the epoch. During every epoch, several others task such as leader election, transaction validation and multiparty signature are executed before committing the block. The chance of becoming a leader depends on the amount of stake is locked, if more stake is locked having the high chances of producing the new block as compared to low staking locked.

3.1.13. Delegated PoS (DPoS)

Delegated Proof of Stake (DPoS) is a collaborative algorithm designed for bitshares. It is not competing for creation of a block like PoW and PoS etc. In this algorithm, the stake holders elect a specific number of nodes (witnesses) for block creations for a specific period of time and kept some nodes in a standby mode. All the elected witnesses will create its assigned block, one at a time in a round robin fashion. If anyone is failed to create an assigned block in a fixed period of time, the

 doi:10.20944/preprints202011.0355.v1

witness will be replaced by a node in the standby list [2]. Blocks are produced every three seconds by authorized witnesses and every 21 blocks the list of said witnesses is shuffled, if a producer has not produced any block within the last 24 hours, they are removed from consideration until they notify the blockchain of their intention to commence creating blocks again [3].

3.1.14. Proof of Disease

Proof of Disease (PoD) [33] consensus protocol is designed for medical care blockchain. The philosophy behind creation of this algorithm is to provide assurance of high quality medical care quickly and with cheap price. PoD based system has broadly two types of miners; coin miner, medical miners. The coin miner will check the financial transactions to avoid Sybil and double spending attacks while the medical miners will check and assure that the medical transactions and health status entered into the health's blockchain ledger are correct and satisfactory. The coin miner will follow the process of etherium platform for transaction fee and rewards because it works based on etherium platform while the medical miners will be paid by the users having the token purchased from the medical blockchain system.

3.2 Fairness Issues in Consensus Algorithms of Public Blockchain Systems

A fair exchange protocol has to provide assurance that bad players cannot have advantage over the honest player [42]. Cryptocurrencies such as Bitcoin, Litecoin, Dogecoin, and Ethereum are gaining popularity. While existing blockchain- based cryptocurrency schemes can ensure reasonable security for transactions, they do not assume any sense of justice [43]. The unfair aspects in permissionless blockchain systems are as follow.

3.2.1. Unfair Transaction Selection

The prioritization of transactions in bitcoin, ethereum and litecoin is based on the transaction fees. The transaction with higher fee is given priority. The miners select the transaction having high transaction fee. Realistically, the transaction having low transaction's fee is rarely picked up by the miners [44].

3.2.2. Unfair Incentive

Incentivization is the life of the public blockchain systems such as Bitcoin, Ethereum and etc. in order to get a higher level assurance for the correctness of the blockchain system. Anyone can join the blockchain system at any time and act as a miner to earn reward for the block creation. Lewenberg et al. [45], as well as Eyal et al. [46], worked on blockchain simulation (amongst honest miners), and found out that some miner's reward can be lower than its fair share but no theoretical explanation available about such unfairness in bitcoin. According to [47], an honest node must invest in mining resources such as hashrates, disk space, etc., to win a mathematical puzzle contest under the Nakamoto consensus protocol. Intuitively, the more resources a miner puts in the network, the higher the chances for miners to win contest and thus get mining incentives. However, success cannot be guaranteed as it also depends on the resources of other miners. Because mining resources are often expensive and economic costs (especially electricity usage) make it impractical for any node to participate voluntarily in the consensus process with consistent economic losses [48]. , how to properly invest in mining resources to maximize profits is a major concern for miners [47].

Rachid Guerraoui and Jingjing Wang [49] demonstrate the unfairness observed by [45] and [46] of the Bitcoin blockchain. He emphasized that, if there are even only two honest miners in a real-world environment in a distributed system. The message delivery is not immediately placed. The ratio between the numbers of blocks approved by the two miners (expected) is actually defined by the exponential duration of the product of message delay and the difference between the two miners' hashrates. As a result, honest miners may have disincentivized of maintaining the protocol, leaving room for the most dishonest miners, making them a majority and jeopardizing the overall consistency of the system.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 November 2020 doi:10.20944/preprints202011.0355.v1

This also implies a trade-off between block mining speed and the fairness of committed blocks in the blockchain and its variants (such as Bitcoin-NG [46],and GHOST [50]): namely, the legal temptation to increase blockchain throughput by reducing the time of mining can lead to more unfairness [49].

3.2.3. Unfair Participation Opportunity as a Miner for Poor People

When a blockchain system that is under the control of a single mining pool or a person having high computational power can lead to a capitalistic approach, where rich can be richer and richer and ordinary people cannot participate due to not having money to purchase high computing devices like ASIC in Bitcoin and stack some amount as deposit in the Ethereum. As we see the most the popular consensus algorithms are PoW and PoS. In PoW based Blockchains such as Bitcoin and Ethereum, the miner who wish to create a new block, he/she has to do some work by solving some mathematical puzzle using hash algorithm which require a high performance computing devices or have to join the mining pool to share the resources in order to find the required hash. According to Ryoya Nakahara and Hiroyuki Inaba [51], creation of mining pool is productive to share a large amount of computing power. As the mining pool become growing and growing, it is very hard for new node or miner to join and mine alone. Therefore he/she has no any other way but to join the mining pool.

Due to the aforementioned reasons it is required to have an environment where rich and poor have the same opportunity and rights in terms of getting rewards in the blockchain so therefore, we need to have a consensus algorithm for blockchain system where rich and poor are equal.

3.3. Issues of Different Public Blockchain's Consensus Algorithms

A summary of the problems of the most popular blockchain's consensus algorithms are shown below in Table 5.

TABLE 5: Public Blockchain's Consensus Algorithms with available issues

PuBCA	Available issues
PoW	Energy and Computation Expenditure, Uselessness computation, 51% attack, Forking, Unfair
PoS	Minting dependency on stake, Forking, Nothing-at-stake, Unfair
Tindermint	Forking, chance of nepotism, Unfair
Proof of Luck (PoL)	Forking, Unfair
PoP	Taking time to become miner, Unfair (for people away from the location of the party)
PoC	Forking, Energy and Computation expenditure, Unfair
PoPF	Forking, Energy and Computation expenditure, Unfair
DPoS	Forking, Unfair
CloudPoS	Lead to centralization (CSP involvement for staking the resources for participation), Unfair
PoS Casper	Minting dependency on stake, Forking, Unfair

3.3.1. Energy and computation expenditure

The difficulty level in the PoW keeps increasing in the blockchain. Therefore, more power and dedicated hardware (such as an ASIC) are needed to resolve the hash value, having a specific number of zero in front, which increases the costs of finding the hash value. The cost of finding a hash value is difficult to control. Mining can only be used for mining pools with expensive hardware that leads to system centralization.

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 November 2020 doi:10.20944/preprints202011.0355.v1

3.3.2. Uselessness of Computation

All miners are competing for competition to create new blocks. They are competing to find a specific hash value. The hash value can be calculated from an unknown number of iterations. Therefore, they consume more energy. As a result, one of them succeeded, the hard work of other miners became useless, and their hard work could not be applied anywhere else.

3.3.3. Forking

Due to the greediness of miners, forks are available in consensus algorithms such as PoW, PoS, Tendermint, PoL, PoC, PoPF, DPoS and PoS Casper. They are competing for a new block creation award. Therefore, it causes the blockchain to split into two parts.

3.3.4. 51% Attack

This attack occurs when the group of miners handles the computing power higher than 50% of finding the difficulty value in the PoW system. This attack causes to create the following issues in blockchain[5]:

- Double spending
- Ignoring specific user's transaction

3.3.5. Unfair

All the consensus algorithms mentioned in Table 5, make it very difficult for the poor people who wish to join the blockchain as a miner. Due to the cost of using expensive technology such as ASIC (PoW), TEE (PoL), and holding stake (PoS, PoS Casper, Tindermint, PoSV, PoC and CloudPoS).

3.3.6. Minting dependency on stake

The minting depends on the amount of stake a person has in the system. If a minter has held a high stake, the chances of minting are more as is discussed in [52]. If the stake in the given cryptocurrency is at 1%, the person can mint up-to 1% of the transactions.

3.3.7. Nothing-at-stake

There is no penalty defined for participants of double spending attack and contributing to multiple blockchain forks in the PoS consensus algorithm.

3.4. Reward winning and incentive strategies of PuBCA

Rewards and incentives are the most important attribute of public blockchain system. These help in keeping alive the public blockchain system. If it is not available in the public blockchain systems, people will not show any interest and will not take participation in the system as a validator or verifier which arrange and manage the system.

TABLE 6. Incentive Strategy and Philosophy behind creation of PuBCA

PBCA	Philosophy Behind Creation	Reward winning and Incentive Strategy	Usage
PoW	Cash like payment system To cover double spending problem	Block creation award, Transaction fee (BTC)	Bitcoin, NameCoin, LiteCoin, DogeCoin, Monero
PoS	To build the security model of a crypto currency and part of its minting process Reduce energy	Block creation award, Transaction fee (GAS)	PeerCoin, Cardano, BitShare, NXT, Tedermint

Preprints (www.preprints.org) | NOT PEER-REVIEWED | Posted: 12 November 2020 doi:10.20944/preprints202011.0355.v1

	consumption		
Tindermint	To address the speed, scalability, and environmental issues available in PoW	Transaction fee only	Cosmos Project
Ripple	To solving high latency in distributed payment systems	No incentive strategy: transaction fee is available but it is not for the miner.	Ripple network, MoneyGram, Euro Exim Bank London, CIMBBank
PoSV	Alternative to PoW and PoS To address the economic and social aspects of being a real currency	Ownership stake and activity (velocity) 5% inflation per year	Reddcoin, NEM
SCP	Safe and secure financial network open to anyone	Weekly Voting for a specific destination address and at least 0.05% of the total weekly vote receive.	Stellar
PoL	To cover mining equitably (fair) distributed by preventing the use of ASICs	No info	Luckychain (not implemented yet)
PoS Casper	Fair validation consensus in ethereum To solve nothing at stake problem	Based on correct voting and total deposit amount staked	Ethereum (not implemented yet)
PoP	Resistance against sybil attack To ensure a fair and widely accessible wealth creation process	Block reward but the minter must be the part of minting pool and 5% annual ROI	POPCOIN (not implemented yet)
PoC	Energy Efficiency Mining Efficiency	Difficulty rewards along with the regular mining fee	Theoretical (not implemented yet)
PoPF	To have Energy efficient consensus algorithm for JCLedger	User fees proportional to the contribution to the system	Theoretical (not implemented yet)
DPoS	To overcome the scalability problem	By 5% inflation	BitShare, Steem, EOS, Golos, Ark, Lisk, PeerPlays, Nano,Cardano, KeyChain
PoD	To solve the available challenges in electronic health records (EHR) or Health Information Exchange (HIE)	User fee (Healthchain ERC20 Tokens) for Medical Episode miners and health state miners	VibrantHealthChain (not impelemented yet)
CloudPoS	Securely recording the data operations occurring in cloud environment	Reduce the cost of resource leasing by a certain percentage for the winning validator	Theoretical (not implemented yet)

 doi:10.20944/preprints202011.0355.v1

	for a predefined number of epochs , releasing some of the staked resources back to the validator without decreasing the value of its stake

4. Discussion

In this section of the study, the data gathered from the white papers and other related papers for collected public blockchain consensus algorithms (PuBCA) which are shown in figure 1 and overviewed in section 4.1. in order to answer the research questions RQ1 and RQ2

4.1. RQ1: What are the available consensus algorithm for public blockchain systems which provide fairness?

As we have drawn the conclusion from the literature as discussed in section 4.1 and 4.2 of this study and found out that there are fairness issues available in the available public blockchain systems and public blockchain consensus algorithms. The fairness issues include unfair transaction selection, unfair incentive and unfair participation opportunity for poor people as a miner and discussed in section 4.1.1, 4.1.2 and 4.1.3 respectively. The table 5 also highlights the unfair attribute which is available in all public blockchain consensus algorithms except PoP. The PoP tried to solve unfair issues and it is successful for a small society because the concept of party is involved but it is not covering all the societies. It helps those people where the party is arranged but the people who are far away from the party location can not attend the party due to time and transportation expenditure.

4.2. RQ2: What are the reward winning and incentive strategies of various consensus algorithms for public blockchain systems?

There are various ways incurred from the literature as discussed in section 4.1 and 4.2 of this study for reward winning and incentive strategies. The table 6 highlights reward winning and incentive strategies of various consensus algorithms in which the most common are as follow:

- Block creation
- Transaction fee
- Inflation
- Return on Investment (ROI).

These and others awards and incentive strategies help in the durability of public blockchain system. It is the only way to keep alive the public blockchain system.

5. Conclusions

This study reviewed 25 blockchain consensus algorithms collected from 36 articles. After examining these 25 blockchain consensus algoirthms, we classified the collected blockchain consensus algoirthms into 3 types of blockchain consensus algorithms such as private, consortium and public. Our focus was on the public blockchain consensus algorithms. The analysis of collected algorithms show that Some consensus algorithms like [10], [11] and [12] cover the order of transactions, the choice of leaders, and transaction selection for block but lacking the fairness in mining strategy for ordinary users in the public blockchain system. The fairness issues include unfair transaction selection, unfair incentive and unfair participation opportunity for poor people as a miner which are available in public blockchain consensus algorithms. These issues require more study in the future.

Author Contributions: Conceptualization, I.J,; Methodology I.J.; Resources, I.J.; Supervision, Z.S, and K.A.B.A; Funding acquisition, Z.S. and K.A.B.A.; software, K.A.B.A, and I.J.; validation, Z.S., K.A.B.A and I.J.; formal analysis, Z.S.; investigation, I.J.; resources, I.J.; data curation, I.J. and K.A.B.A; writing—original draft

preparation, I.J.; writing—review and editing, K.A.B.A.;. All authors have read and agreed to the published version of the manuscript.

Funding: Please add: "This research received no external funding" or "This research was funded by NAME OF FUNDER, grant number XXX" and "The APC was funded by XXX". Check carefully that the details given are accurate and use the standard spelling of funding agency names at https://search.crossref.org/funding, any errors may affect your future funding.

Conflicts of Interest: The authors declare no conflict of interest

References

[1] W. T. Tsai and L. Yu, "Lessons Learned from Developing Permissioned Blockchains," *Proc. - 2018 IEEE 18th Int. Conf. Softw. Qual. Reliab. Secur. Companion, QRS-C 2018*, pp. 1–10, 2018.

[2] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system, October 2008," *Cited on*, p. 53, 2008.

[3] I. Konstantinidis, G. Siaminos, C. Timplalexis, P. Zervas, V. Peristeras, and S. Decker, *Blockchain for Business Applications* :, vol. 2. Springer International Publishing, 2018.

[4] and R. G. Atónio Brandão, Henrique São Mamede, "Systematic Review of the Literature, Research on Blockchain Technology as Support to the Trust Model Proposed Applied to Smart Places," *Springer Int. Publ. AG, part Springer Nat. 2018 Á. Rocha al. WorldCIST'18 2018, AISC 745, pp. 1163–1174, 2018. https//doi.org/10.1007/978-3-319-77703-0_113*, vol. 1, no. March, pp. 1163–1174, 2018.

[5] J. Yli-huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where Is Current Research on Blockchain Technology ?— A Systematic Review," pp. 1–27, 2016.

[6] M. J. Fischer, "The consensus problem in unreliable distributed systems (a brief survey)," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 1983, vol. 158 LNCS, pp. 127–140.

[7] N. A. L. and M. S. P. MICHAEL J. FISCHER, "Impossibility of Distributed Consensus with One Faulty Process," *J. Asscctktion Comput. Mach. Vol. 32, No. 2, April 1985, pp. 374-382*, pp. 374–382, 1985.

[8] F. B. Schneider, "Implementing Fault-Tolerant Services Using the State Machine Approach: A Tutorial," *ACM Comput. Surv.*, vol. 22, no. 4, pp. 299–319, 1990.

[9] M. Herlihy, "Wait-Free Synchronization," *ACM Trans. Program. Lang. Syst.*, vol. 13, no. 1, pp. 124–149, 1991.

[10] A. Asayag *et al.*, "Helix: A Scalable and Fair Consensus Algorithm Resistant to Ordering Manipulation," pp. 1–26, 2018.

[11] A. Miller, Y. Xia, K. Croman, E. Shi, and D. Song, "The Honey Badger of BFT protocols," *Proc. ACM Conf. Comput. Commun. Secur.*, vol. 24-28-Octo, no. Section 3, pp. 31–42, 2016.

[12] L. Baird, "The swirlds hashgraph consensus algorithm: fair, fast, byzantine fault tolerance," pp. 1–28, 2018.

[13] Kitchenham, "Guidelines for performing systematic literature reviews in software engineering," *Tech. Rep.*, vol. 4, pp. 5356–5373, 2007.

[14] S. King and S. Nadal, "PPCoin Proof of stake," 2012.

[15] M. Snider, K. Samani, and T. Jain, "Delegated Proof of Stake: Features and Tradeoffs," *Multicoin Cap.*, p. 19, 2018.

[16] J. Kwon, "TenderMint : Consensus without Mining," *the-Blockchain.Com*, vol. 6, pp. 1–10, 2014.

[17] D. Schwartz, N. Youngs, and A. Britto, "The Ripple protocol consensus algorithm," *Ripple Labs Inc White Pap.*, pp. 1–8, 2014.

[18] L. Ren, "Proof of Stake Velocity: Building the Social Currency of the Digital Age," *Self-published white Pap.*, pp. 1–13, 2014.

[19] A. Bessani, J. Sousa, and E. E. P. Alchieri, "State machine replication for the masses with BFT-SMART," in *Proceedings - 44th Annual IEEE/IFIP International Conference on Dependable Systems and Networks, DSN 2014*, 2014, pp. 355–362.

[20] Diego Ongaro and John Ousterhout, "In Search of an Understandable Consensus Algorithm," *Atc '14*, vol. 22, no. 2, pp. 305–320, 2014.

[21] "guide/poa.md at master · ethereum/guide · GitHub." [Online]. Available: https://github.com/ethereum/guide/blob/master/poa.md. [Accessed: 03-Jan-2020].

[22] D. Mazieres, "The Stellar Consensus Protocol: A federated Model for internet level Consensus," *J. Am. Chem. Soc.*, vol. 120, no. 42, pp. 11022–11023, 2016.

[23] L. Baird, "the Swirlds Hashgraph Consensus Algorithm: Fair, Fast, Byzantine Fault Tolerance," *Swirlds Tech Rep.*, vol. 01, pp. 301–302, 2016.

[24] M. Milutinovic, W. He, H. Wu, and M. Kanwal, "Proof of Luck: An efficient blockchain consensus protocol," *SysTEX 2016 - 1st Work. Syst. Softw. Trust. Exec. Coloca. with ACM/IFIP/USENIX Middlew. 2016*, pp. 2–7, 2016.

[25] B. Curran, "What is Proof of Elapsed Time Consensus," p. 1, 2018.

[26] K. Li, H. Li, H. Hou, K. Li, and Y. Chen, "Proof of Vote: A High-Performance Consensus Protocol Based on Vote Mechanism & Consortium Blockchain," *Proc. - 2017 IEEE 19th Intl Conf. High Perform. Comput. Commun. HPCC 2017, 2017 IEEE 15th Intl Conf. Smart City, SmartCity 2017 2017 IEEE 3rd Intl Conf. Data Sci. Syst. DSS 2017*, vol. 2018-Janua, pp. 466–473, 2017.

[27] V. Buterin and V. Griffith, "Casper the Friendly Finality Gadget," pp. 1–10, 2017.

[28] M. Borge, E. Kokoris-Kogias, P. Jovanovic, L. Gasser, N. Gailly, and B. Ford, "Proof-of-personhood: Redemocratizing permissionless cryptocurrencies," *Proc. - 2nd IEEE Eur. Symp. Secur. Priv. Work. EuroS PW 2017*, pp. 23–26, 2017.

[29] T. Xue, Y. Yuan, Z. Ahmed, K. Moniz, G. Cao, and C. Wang, "Proof of Contribution: A Modification of Proof of Work to Increase Mining Efficiency," *Proc. - Int. Comput. Softw. Appl. Conf.*, vol. 1, pp. 636–644, 2018.

[30] F. Muratov, A. Lebedev, N. Iushkevich, B. Nasrulin, and M. Takemiya, "YAC: BFT Consensus Algorithm for Blockchain," 2018.

[31] J. Zou, B. Ye, L. Qu, Y. Wang, M. A. Orgun, and L. Li, "A Proof-of-Trust Consensus Protocol for Enhancing Accountability in Crowdsourcing Services," *IEEE Trans. Serv. Comput.*, vol. 12, no. 3, pp. 429–445, 2019.

[32] X. Fu, H. Wang, P. Shi, and H. Mi, "PoPF: A Consensus Algorithm for JCLedger," *Proc. - 12th IEEE Int. Symp. Serv. Syst. Eng. SOSE 2018 9th Int. Work. Jt. Cloud Comput. JCC 2018*, pp. 204–209, 2018.

[33] A. K. Talukder, M. Chaitanya, D. Arnold, and K. Sakurai, "Proof of disease: A blockchain consensus protocol for accurate medical decisions and reducing the disease burden," *Proc. - 2018 IEEE SmartWorld, Ubiquitous Intell. Comput. Adv. Trust. Comput. Scalable Comput. Commun. Cloud Big Data Comput. Internet People Smart City Innov. SmartWorld/UIC/ATC/ScalCom/CBDCo*, pp. 257–262, 2018.

[34] D. Tosh, S. Shetty, P. Foytik, C. Kamhoua, and L. Njilla, "CloudPoS: A Proof-of-Stake Consensus Design for Blockchain Integrated Cloud," *IEEE Int. Conf. Cloud Comput. CLOUD*, vol. 2018-July, pp. 302–309, 2018.

[35] J. T. Kim, J. Jin, and K. Kim, "A study on an energy-effective and secure consensus algorithm for private blockchain systems (PoM: Proof of Majority)," in *9th International Conference on Information and Communication Technology Convergence: ICT Convergence Powered by Smart Intelligence, ICTC 2018*, 2018,

pp. 932–935.

[36] X. Hao, L. Yu, L. Zhiqiang, L. Zhen, and G. Dawu, "Dynamic practical byzantine fault tolerance," *2018 IEEE Conf. Commun. Netw. Secur. CNS 2018*, pp. 1–8, 2018.

[37] J. Reis, M. Amorim, N. Melao, and P. Matos, "Digital Transformation : A Literature Review and Guidelines for Future Digital Transformation : A Literature Review and Guidelines for Future Research," *10th Eur. Conf. Inf. Syst. Manag. Acad. Conf. Publ. Ltd.*, vol. 1, no. March, pp. 20–28, 2016.

[38] D. Mingxiao, M. Xiaofeng, Z. Zhe, W. Xiangwei, and C. Qijun, "A Review on Consensus Algorithm of Blockchain," pp. 2567–2572, 2017.

[39] A. Jain, S. Arora, Y. Shukla, T. B. Patil, and S. T. Sawant-patil, "Proof of stake with Casper the friendly finality gadget protocol for fair validation consensus in Ethereum," *Int. J. Sci. Res. Comput. Sci. Eng. Inf. Technol.*, vol. 3, no. 3, pp. 291–298, 2018.

[40] A. Baliga, "Understanding Blockchain Consensus Models," no. April, 2017.

[41] X. Fu, H. Wang, P. Shi, and H. Mi, "PoPF: A Consensus Algorithm for JCLedger," *Proc. - 12th IEEE Int. Symp. Serv. Syst. Eng. SOSE 2018 9th Int. Work. Jt. Cloud Comput. JCC 2018*, pp. 204–209, 2018.

[42] N. Asokan, "Fairness in electronic commerce," *Res. Rep. RZ3027*, 1998.

[43] J. Liu, W. Li, G. O. Karame, and N. Asokan, "Toward Fairness of Cryptocurrency Payments," *IEEE Secur. Priv.*, vol. 16, no. 3, pp. 81–89, 2018.

[44] S. Goel, A. Singh, R. Garg, M. Verma, and P. Jayachandran, "Resource fairness and prioritization of transactions in permissioned blockchain systems (industry track)," *Middlew. Ind. 2018 - Proc. 2018 ACM/IFIP/USENIX Middlew. Conf. (Industrial Track)*, pp. 46–53, 2018.

[45] and A. Z. Yoad Lewenberg, Yonatan Sompolinsky, "Inclusive Block Cahin protocols," vol. 8975, pp. 127–146, 2015.

[46] I. Eyal, A. E. Gencer, E. G. Sirer, and R. van Renesse, "Bitcoin-NG: A Scalable Blockchain Protocol," 2015.

[47] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling Blockchain: A Data Processing View of Blockchain Systems," *IEEE Trans. Knowl. Data Eng.*, vol. 30, no. 7, pp. 1366–1385, 2018.

[48] W. Wang *et al.*, "A Survey on Consensus Mechanisms and Mining Strategy Management in Blockchain Networks," *IEEE Access*, vol. 7, no. Vm, pp. 22328–22370, 2019.

[49] R. G. and J. Wang, "On the Unfairness of Blockchain," *LNCS SPringer*, pp. 36–50, 2019.

[50] Y. S. and A. Zohar, "Secure High-Rate Transaction Processing in Bitcoin," vol. 8975, pp. 127–146, 2015.

[51] R. Nakahara and H. Inaba, "Proposal of Fair Proof-of-Work System Based on Rating of User's Computing Power," *2018 IEEE 7th Glob. Conf. Consum. Electron. GCCE 2018*, pp. 248–249, 2018.

[52] L. S. Sankar *et al.*, "Survey of Consensus Protocols on Blockchain Applications," 2017.