sustainability

MDPI

Article

Robust Proof of Stake: A New Consensus Protocol for Sustainable Blockchain Systems

Aiya Li [1], Xianhua Wei [1] and Zhou He [1,2,*]

[1] School of Economics and Management, University of Chinese Academy of Sciences, Beijing 100190, China; liaiya17@mails.ucas.ac.cn (A.L.); weixh@ucas.ac.cn (X.W.)

[2] Key Laboratory of Big Data Mining and Knowledge Management, Chinese Academy of Sciences, Beijing 100190, China

* Correspondence: hezhou@ucas.ac.cn

Received: 1 March 2020; Accepted: 31 March 2020; Published: 2 April 2020

Abstract: In the digital economy era, the development of a distributed robust economy system has become increasingly important. The blockchain technology can be used to build such a system, but current mainstream consensus protocols are vulnerable to attack, making blockchain systems unsustainable. In this paper, we propose a new Robust Proof of Stake (RPoS) consensus protocol, which uses the amount of coins to select miners and limits the maximum value of the coin age to effectively avoid coin age accumulation attack and Nothing-at-Stake (N@S) attack. Under a comparison framework, we show that the RPoS equals or outperforms Proof of Work (PoW) protocol and Proof of Stake (PoS) protocol in three dimensions: energy consumption, robustness, and transaction processing speed. To compare the three consensus protocols in terms of trade efficiency, we built an agent-based model and find that RPoS protocol has greater or similar trade request-satisfied ratio than PoW and PoS. Hence, we suggest that RPoS is very suitable for building a robust digital economy distributed system.

Keywords: distributed digital economy system; blockchain; robust; consensus protocol; agent-based model

1. Introduction

The essence of blockchain technology is to build a robust distributed database that does not rely on any center based on cryptography [1]. The recorded data can be shared by all nodes and not controlled by any nodes. The architecture of a blockchain system can be divided into six layers as in Figure 1: data layer, network layer, consensus layer, incentive layer, contract layer, and application layer [2]. The incentive layer and consensus layer, as the core parts of the blockchain system architecture, can ensure that rational participants do not have the motivation or ability to tamper with records or undermine the system in most scenarios [3].

Consensus refers to the ideals and values sought by people of different strata and interests in a society [4]. The more dispersed or more participants seeking consensus, the lower the efficiency of reaching consensus, but the higher the satisfaction after forming a consensus, the more stable the consensus. Consensus protocol in blockchain results in an identical distributed ledger. In the literature, the consensus protocol refers to an algorithm that achieves a consensus on the order of transactions within a period of time and the verification and confirmation of transactions in a short time [5]. For example, the entire voting process to select outstanding employees and related methods compose a consensus protocol that allows the entire collective to reach a consensus on who should be elected. In the process of sharing data in a distributed system, the nodes that have the right to pack the blocks append the newly-packed block on the existing ledger and broadcast them over the entire network. After other nodes receive the information and verify that the blocks are correct, they will synchronize this newly-packed block. However, consensus-based blockchain system can also be attacked. A famous attack occurred in June 2015, named the DAO attack [6]. The DAO attack was a group of hackers who attacked the Ethereum system [7] and stole the digital currency ETH (Ether, the digital currency of Ethereum system). The DAO attack caused great damage to the original Ethereum chain, and its destructive power almost destroyed the entire Ethereum network. In 2018, there were over 49 security accidents in the EOS (Enterprise Operation System) public chain [8]. These accidents were basically due to the attack events such as random number attack and transaction rollback caused by the system nodes outbreak growth of the EOS DApp (Decentralized Application). Attacks not only caused direct economic loss as high as 747,209 EOS (the digital currency of EOS system, is the same name as EOS system), but also brought a huge threat to the stable and sustainable development of the EOS system [9]. Therefore, the distributed blockchain system can maintain the high stability and sustainability only if it is robust enough.

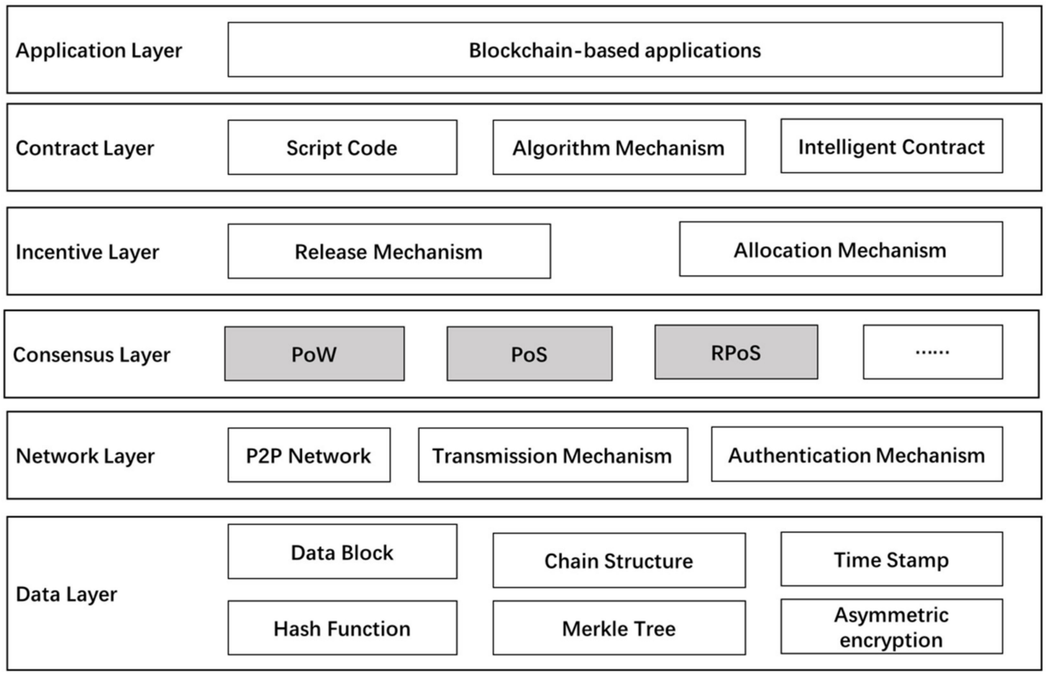

Figure 1. The architecture of a blockchain system. The abbreviations in the figure are shown in follows. PoW: Proof of Work, PoS: Proof of Stake, RPoS: Robust Proof of Stake, P2P: Peer-to-peer networking, is a distributed application architecture that partitions tasks between peers. See the table in Appendix A for a brief introduction to the acronyms.

This paper first proposed a framework for consensus protocol comparison, which contains four dimensions: energy-saving, robustness, TPS (Transaction Per Second, see a table of acronyms in Appendix A) and trade request-satisfied ratio. We show that the first three dimensions are often analyzed theoretically or qualitatively, while the last one can be quantitatively evaluated via simulation. Next, after introducing the Proof of Work (PoW) and Proof of Stake (PoS) consensus protocols, we presented a new Robust Proof of Stake (RPoS) consensus protocol based on PoS. The RPoS selects the data-writing node based on the coin balance, and others will accept the new data to keep the ledger consistent.

In the comparison part, we showed that RPoS is more energy-saving than PoW, faster than PoS, and more robust against PoS-related attacks such as Nothing-at-Stake (N@S) attack [10] and coin age accumulation attack [11]. Regarding fourth aspect (i.e., trade request-satisfied ratio), we developed an agent-based blockchain model, and conducted three experiments in which PoW, PoS, RPoS consensus protocols and random, small-world, scale-free trade networks were implemented. Experimental results show that the proposed RPoS protocol leads to similar or better trade efficiency than PoW. In particular, the trade request-satisfied ratio in scale-free trade network is about 13-14%, while it is 63-65% (almost five-fold) in the other two networks. In sum, RPoS outperforms PoW in all the four features, and thus we suggest that RPoS is suitable for today's blockchain system.

Our contribution is three-fold. First, we propose a framework for consensus protocol comparison, which includes four dimensions, i.e., energy-saving, robustness, TPS, and trade request-satisfied ratio. Second, we develop a new RPoS protocol which outperforms mainstream consensus protocols such as PoW and PoS. Third, we quantified the trade request-satisfied ratio of three tested consensus protocols using the agent-based modeling and simulation technique.

The rest of the paper is organized as follows. In Section 2 we survey related research streams, followed by Section 3 where we introduce the existing consensus protocols and their problems. We describe the RPoS in detail in Section 4. In Section 5, we design the simulation experiments and present the experimental results. Finally, we conclude the paper and suggest potential topics for future research in Section 6.

2. Literature Review

In this section, we review the literature on blockchain consensus protocols.

The first blockchain consensus protocol is PoW, Proof of Work. Bitcoin uses a PoW protocol to achieve consensus, and its core idea is to ensure the consistency of data and the security of consensus by introducing the computing power competition of distributed nodes. New transactions are always being generated in the Bitcoin system, and nodes need to put legitimate transactions into blocks [1]. Antonopoulos proposed that the block header contains six parts, which are the version number, the previous block hash value, the Merkle root, the timestamp, the difficulty target noise, and the random number [12]. The node which can fastest solve this problem will get the block accounting right and the Bitcoin reward automatically generated by the system. PoW protocol exists more or less in digital currencies such as Dogecoin [13] and Litecoin [14]. However, to keep energy use sustainable, some scientists also did a lot research work for this goal [15], by introducing a method of applying blockchain to a new and renewable energy transaction system by presenting a consensus protocol that can improve its infrastructure and performance. Fadeyi pointed out that sustainability is a crucial goal in the design of smart cities nowadays; the truth is, currently there are no assurances of sustainable cities where cryptocurrency mining is at full scale [16]. International trade players may benefit from the technological reengineering of financial processes through the implementation of blockchain, and the security and sustainability of the trading system is guaranteed [17]. In the energy industry, by using the new blockchain technology that stimulates innovation and growth in the energy and a high level of automation though smart contracts, the industry avoids energy waste and misappropriation "attacks" happen in the system [18]. Some countries attempt to achieve the goal of creating a new and renewable energy transaction system by presenting a consensus protocol that can improve its infrastructure and performance in security through utilizing a blockchain system [15]. As for the scalability of PoW system, Back et al. [19] proposed to transfer transactions on Bitcoin to other cryptocurrency blockchain systems, thereby increasing the throughput of transaction processing and improving the transaction per second of the system. Narayanande et al. [20] pointed out that the consensus protocol itself requires a large amount of communication and computing resources, and the number of transactions will continue to increase over time, while the node's computing limited will cause bottlenecks in the transaction process. Luu et al. [21] proposed a public blockchain distributed consensus protocol which reaches consensus of the group members through Byzantine agreement. This protocol enhances the transaction process capability of the Bitcoin system by dividing nodes into groups randomly and by verifying different transactions.

Another important blockchain consensus protocol is PoS protocol [11]. Its main feature is the proof of equity instead of the proof of workload, and the node with the highest equity realizes the addition of new blocks and the acquisition of incentive income. Compared with PoW, Houy [22] stated that PoS is more like a lottery, accumulating more coin ages to win opportunities, but once a certain value is consumed, the probability of winning again is reduced, thereby reducing the impact of centralization brought by the richer people.

There are also some other commonly used consensus protocols. Delegated PoS consensus protocol, proposed by Daniel Larimer [23] in April 2014, can further speed up the transaction speed, and solves the security problem that the nodes in PoS accumulate coin age unlimitedly. RPCA (Ripple Consensus Algorithm) protocol [24] is a network transaction synchronization protocol that prioritizes data accuracy. It is based on the consensus reached by special nodes (also called "gateways"). PBFT protocol is studied by Castro et al. [25], which also most commonly used BFT (Byzantine Fault Tolerance) consensus protocol which solves the problem of the inefficiency of the original Byzantine fault tolerance algorithm. PBFT protocol [26] reduces the complexity of the algorithm from the exponential level of the number of nodes to the square level of the number of nodes, making the fault tolerance algorithm of Byzantium more feasible in practical system applications. PAXOS protocol [27] is a consensus protocol based on message passing, and highly fault-tolerant. RAFT protocol [28] is where the core idea is that if the initial state of each database is consistent, the consistent data can be guaranteed by performing consistent operations. POOL (verification pool) protocol [29] is based on traditional distributed consistency technology, plus a data verification protocol.

The blockchain technology is relatively new and the competition among consensus protocols are intense. Hence, the merits and demerits of many consensus protocols are not strictly evaluated, and it is also very costly, if not impossible, to test them extensively in reality. Currently, the literature on comparing consensus protocols is growing, some of which implicitly analyzed these protocols under several dimensions. We summarized these papers in Table 1, as well as their considered dimensions and research methods. It can be found that there is a lack of a universal framework for consensus protocol comparison.

Table 1. Existing frameworks for consensus protocol comparison.

Papers	Considered Dimensions	Research Method
Saleh [30]	energy-saving, robustness	qualitative research and game theoretical analysis
Han et al. [31]	energy-saving, efficiency, coherence, error-tolerant rate, extensibility	qualitative research and quantitative research
Zhou [32]	energy-saving, computing power distribution	qualitative research and
Wei et al. [33]	coin price index, request-satisfied ratio, Gini index	agent-based modeling and simulation
Bach et al. [34]	energy-saving, tolerated power of adversary, TPS, market capitalization	qualitative research and quantitative research

In sum, researchers have proposed many protocols and architectures, but the related studies on consensus protocols of the blockchain technology and their issues are scarce. Hence, we introduce two consensus protocols and their problems in the next section, followed by a section of a new RpoS consensus protocol.

3. The Proposed Comparison Framework and Two Consensus Protocols

In this section, we first propose a new framework for comparing consensus protocols, and then introduce the PoW and PoS under this framework.

3.1. The Proposed Framework

Motivated by the studies in Table 1, we propose a comparison framework with four aspects:

(1) Energy-saving. With rapid economic development, a large amount of energy consumption result in a large amount of carbon dioxide emissions, which has significantly changed the global climate

and seriously affected the living environment of human beings. Therefore, it is crucial to design a distributed economy system with low energy conservation and carbon dioxide emission [30]. This is why most of the papers in Table 1 considered the dimension of energy-saving.

(2) Robustness. As mentioned in the Introduction section, blockchain systems are also under many types of cyber-attacks, such as the DAO attack [6] and random number attack [8], which became a huge threat to the stable and sustainable development of blockchain systems [9]. Hence, many frameworks in Table 1 considered the related dimensions such as robustness [30] and error-tolerant rate [31].

(3) TPS. TPS is an important indicator to measure the efficiency of a financial system, as it represents the transaction volume completed by the system per second [35]. Alibaba's Alipay carried a world record 256,000 TPS for 5 minutes and 22 seconds on 11 Nov 2017, and VISA can handle on average around 1700 TPS [36]. In contrast, the well-known blockchain systems (such as Bitcoin and Ethereum) can only reach less than 40 TPS, making them impossible to manage the transaction volume in the real world [37]. Therefore, we see that Han et al. [31] and Bach et al. [34] included the TPS in their frameworks.

(4) Trade request-satisfied ratio. A blockchain system can be viewed as a trade network among autonomous traders who have the request to either buy, sell or hold coin. Unlike the stock market, traders in the blockchain system have no central counter party which provides clearing and settlement services. The ones who want to buy or sell coins need to find the trade partner to fulfill their demands. Hence, the trade request-satisfied ratio is defined as the division of total satisfied coin requests by total coin requests [33]. The larger the ratio is, the higher the trade request-satisfied ratio of a blockchain system is.

After determining the four dimensions above based on Table 1, we see that the first three dimensions can barely be quantified, in a research article, for the following reasons. First, the actual energy consumption is directly affected by the number of users, especially the miners, in the blockchain system. However, it is quite difficult to forecast the user numbers and the energy consumption, especially when PoW or some energy-related consensus protocol is applied. Second, the robustness of a consensus protocol is often discussed using game theoretical analysis, which requires relatively strict assumptions. Hence, we compare consensus protocols in terms of robustness theoretically, as in Saleh [30]. Third, the maximum TPS of a consensus protocol is very difficult to evaluate because it relies on many computer and network-related factors [33]. Hence, researchers usually discussed it theoretically [35]. However, the agent-based model developed by Wei et al. [33] can be modified to compare different consensus protocols quantitatively.

In the next two subsections, we introduce the two mainstream consensus protocols in blockchain systems: PoW and PoS. We also discuss their performances in three dimensions: energy-saving, robust against attacks, and TPS. In Section 4 we propose the RpoS protocol, and compare it with PoW and PoS in Section 5.

3.2. PoW, Proof of Work Protocol

PoW protocol was originally proposed to prevent spam [38]. In the Bitcoin system, the PoW protocol is used to ensure that all nodes agree on a set of transactions to be confirmed. Only the node that has completed the proof of work can propose the pending block at this stage. After that, the nodes in the network continue to try to complete the proof of work after this block and generate new blocks. When a node receives two different pending blocks, the one with the longer chain is selected for verification. A longer chain means that the chain contains more work.

PoW usually includes three algorithms [39]: a random algorithm that generates challenge c (random variable nonce), an algorithm that generates s (the total hash value of the block) to solve challenge c , and an algorithm that verifies whether challenge c is solved by s . The miner in a PoW system is to obtain packing chance after they nonce hash value satisfy the following inequality:

$$\mathrm{Hash}(\mathrm{s},\mathrm{c}) < \mathrm{d} \tag{1}$$

The miner wants to find a string nonce, represented by its state (based on SHA-256) by c . s is the hash value of the nonce find by the miner represented by the total hash value of the block. D is the current fixed difficulty of the PoW system. Then, the system combines the content of c and s, mapping the combined result to a binary difficulty coefficient that starts with several consecutive zeros through SHA-256. After the system gets the difficulty hash value and compares the hash value with the d, the compared result will decide whether the miner is eligible for packing.

However, there are some problems with the PoW protocol. (1) The process of PoW usually consumes a lot of computing resources and energy and thus it is unsustainable. Currently, it is estimated that the Bitcoin system consumes more energy than Switzerland, roughly 0.25 percent of the world's entire electricity consumption [40]. (2) There is a serious efficiency problem with PoW. The generation of each block takes time, and at the same time, the newly generated block requires the confirmation of subsequent blocks to ensure validity, which requires longer time and seriously affects the system efficiency. For example, the Bitcoin system needs ten minutes on average to generate a block and needs to wait for six subsequent blocks for confirmation. In this way, a transaction takes approximately sixty minutes to be confirmed under PoW. (3) The security of the PoW protocol requires that the computing resources occupied by the attacker do not exceed 50% of the entire network. However, from the current mining power of the Bitcoin mining pool, the top five mining pools have the total computing power [41]. The proportion has already exceeded half, posing a serious threat to the security and sustainability of the system. Since PoW relies on computing power to compete for packing opportunities, the probability of a 51% attack is relatively high. In this situation, PoW system often happens with a low level of robustness.

3.3. PoS, Proof of Stake Protocol

As PoW protocol consumes a lot of resources and the computing resources tend to be centralized, PoS protocol has received widespread attention, which assumes that richer owners of the equity are more willing to maintain the consistency and security of the system. In particular, at the beginning of each round, the node can be selected as a representative to propose a new block after the packing condition has been verified by the PoS system. The representative proposes a new pending block after receiving the longest valid blockchain, and broadcasts the new blockchain generated by himself, waiting for confirmation. At the beginning of the next round, the PoW system reselects the representative to confirm the results of the previous round. Honest representatives will continue to work behind the longest valid blockchain.

Similar to PoW protocol, the miners in a PoS system obtain packing chance after their nonce hash value satisfy the following inequality (2). The difference from the PoW is that whether the challenge c can be solved is only related to the equity owned by the node, and has nothing to do with the computing resources owned by the node. The more equity a node has, the bigger probability the node could be selected as a representative. Challenge c is determined by the current state of the block, including the longest valid blockchain and equity distribution obtained. An unpaid transaction s owned by the node as the input satisfies the following conditions, that is,

$$\mathrm{Hash}(\mathrm{s},\mathrm{c}) \leq \mathrm{N}_{\mathrm{coin}} * \mathrm{T}_{\mathrm{coin}} \tag{2}$$

where the current time is gradually increased in seconds, $\mathrm{T}_{\mathrm{coin}}$ as the time accumulation for the coins, $\mathrm{N}_{\mathrm{coin}}$ as the amount of coins. The node can make a new attempt per second to verify whether it is selected as a representative. The chance of a node being able to pack depends on whether it satisfies the inequality (2). So the $N_{coin}*T_{coin}$ here is the coin age of the node, and the nodes with a bigger coin age will get the bigger chance to satisfy the formula (2) when at the same difficulty level.

As for PoS protocol's performance, PoS consensus protocol has another three features: energy-saving, fast trade speed, a risk of coin age accumulation attack and N@S attack. The details of PoS protocol's features are shown in the following.

First, the TPS of the PoS is higher than PoW. As the opportunities for competitive packing do not rely on computing power, PoS protocol relies on the stake that the nodes have and relies on the way nodes vote. The result is that PoS protocol saves the transaction time and leads to a higher TPS than PoW protocol.

The second is that the robustness of PoS is relatively low due to two kinds of attack: coin age accumulation attack and N@S attack.

The coin age accumulation attack leads to a low level of robustness. In the earliest version of PoS, the difficulty of mining was not only related to the current account balance, but also linked to the hold time of each coin. In this case, after a period of waiting, some nodes will reach to a bigger T_{coin} . At the same level of coin number N_{coin} and the same difficulty d , it is easier for bigger T_{coin} to satisfy the formula (2). Then these nodes will have the ability to control the entire network by the increasing coin age. If these nodes passively packing or conspire to tamper with system data, then a negative impact on the entire system will be caused.

Another attack is the famous N@S attack; we can see the attack process in Figure 2.

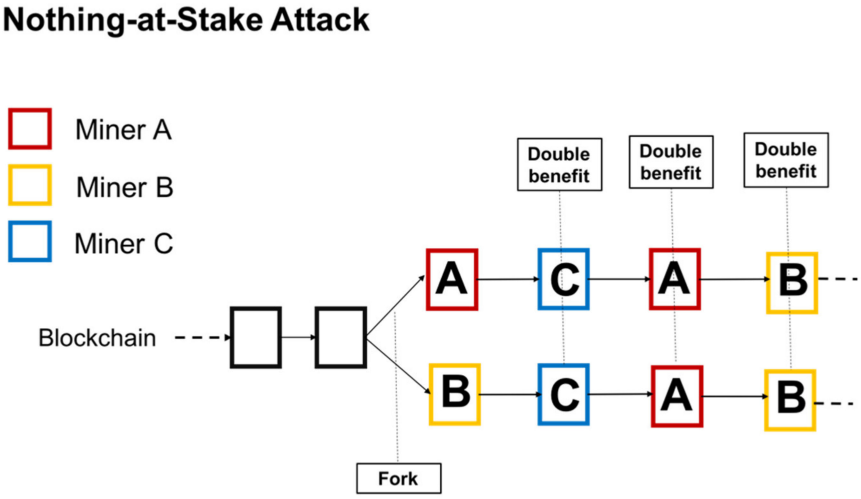

Figure 2. N@S attack process. When N@S attack occurs, the miners in this blockchain system choose to mine on both chains at the same time. In this situation, for the double benefit, every miner has an incentive to cheat.

The N@S attacker loses nothing when behaving badly, but stands to gain everything. When the system forks, the malicious node can get the benefits on both chains without paying any competition cost. Take Figure 2, for example, where there are two branch chains in the system, for the "miner" (either miner A, B, or C) who holds the coin, the best strategy is to "mine" on the two branches at the same time. Then the miner A, B, C who mines on the two branches will get a double benefit before the system chooses one chain as the only approved chain, the unselected chain may be scrapped, or becomes a new blockchain system. Such attacks often happen when there is a fork which may be randomly generated by the system, or may be generated by some malicious attack. More importantly, such attacks are likely to succeed, because all nodes reached a consensus on this fork chain and did not even need more than 51% of nodes in cooperative cheating.

It can be seen from the above that PoW protocol has a large waste of power resources when competing for packing opportunities, and it performs poorly in terms of sustainability. The PoS consensus protocol reflects a low level of robustness when competing for packing opportunities, due to there being a risk of coin age accumulation attack or N@S attack.

4. The RPoS Consensus Protocol

Aiming at the problems of coin age accumulation attack and N@S attack, this paper constructs a Robust Proof of Stake consensus protocol (RPoS), which attempts to tackle the problems of mainstream consensus protocols aforementioned.

4.1. RpoS Consensus Protocol

(1) Dynamic coin age. As there are too many mining nodes, we propose the concept of "dynamic coin age", which serves as a threshold. Only the node which meets this coin age condition (the coin age is defined in Formula (3)) can compete for the packing chance, and get the system reward.

(2) Calculation of coin age. Before calculating the coin age of the node, we first compute the accumulation of time and the number of coins. Each block has a timestamp, and the accumulated time can be obtained by the timestamp, that is,

$$\mathrm{Age}_t = (\mathrm{D_t} - \mathrm{D_{t-1}}) * \mathrm{N_{coin}} + \mathrm{Age}_{t-1} \tag{3}$$

The amount of coins $\mathrm{N_{coin}}$ is a current value. The newly added days are the result of the current block time $\mathrm{D_t}$ and subtract the previous time $\mathrm{D_{t-1}}$. The added days multiply the $\mathrm{N_{coin}}$ and lead to a newly added coin age. Then, we get the final coin age Age_t by the newly added coin age plus the previous coin age Age_{t-1} . After the blocks are packed, the node's coin age Age_t will be cleared.

(3) RPoS mining process. The definition of the target value $\mathrm{V_{target}}$ is a value that is dynamically adjusted according to the block production time, and is used to identify the difficulty of the block production; we define it in Formula (4).

$$\mathrm{Hash}\ (\mathrm{Cont_{block}}, \mathrm{Var_{nonce}}) < \mathrm{Age}_t * \mathrm{AV_{target}} \tag{4}$$

where the variable $\mathrm{Cont_{block}}$ is the content of the block, $\mathrm{Var_{nonce}}$ is the variable of the nonce. The $\mathrm{Age}_t * \mathrm{gV}_{target}$, as a difficulty to this hash inequality, can be understood as a dynamic coin age.

In PoS system, miners use their coin age to compete for packing chance. The node who reaches the coin age benchmark for block production will start packing and broadcast in the blockchain system. If the value of the $\mathrm{Age}_t * \mathrm{AV_{target}}$ is the highest coin age value in the entire network, and no nodes reach the block age for benchmark, then an internal stopwatch timer is started to accumulate time. When some nodes reach the coin age benchmark, then the block can be packed and broadcast. After a node generates a block, the coin age of this node is cleared and re-accumulated, and other nodes continue to accumulate coin age.

4.2. RpoS Consensus Protocol Implementation

When using coin age, there will be a risk of coin age accumulation attack in PoS system, so we remove the coin age and use the amount of coins for miner selection. In Figure 3, we can see the differences between the three consensus protocols: PoW, PoS, RPoS.

By the differences with PoW protocol and PoS protocol, we prove that the hash value of RPoS protocol satisfies the following formula,

$$\mathrm{Hash}\ (\mathrm{Cont_{block}}, \mathrm{Var_{nonce}}) < \mathrm{N_{coin}} * \mathrm{V}_{\ target} \tag{5}$$

The final hash value of the competition process in RPoS is $\mathrm{Hash}\ (\mathrm{Cont_{block}}, \mathrm{Var_{nonce}})$. The target value $\mathrm{V}_{\ target}$ changes dynamically according to the block production time of the parent block. In this inequality, the difficulty is the result of N_{coin} * V $_{target}$. When the system retrieves which node in the system meets the inequality condition, this node will be selected and added to the packing node queue. In order to adjust the difficulty of system nodes competing for packing opportunities, we can adjust the target value V $_{target}$ forward and reverse, then the number of miners who can get packing opportunities will change. The larger target value means a bigger difficulty value in the system, which will add more opportunity for the miners to get the packing chance in RPoS system. Similarly, the node, who with higher amount of coins N_{coin}, is easier to get the chance to packing and produce blocks.

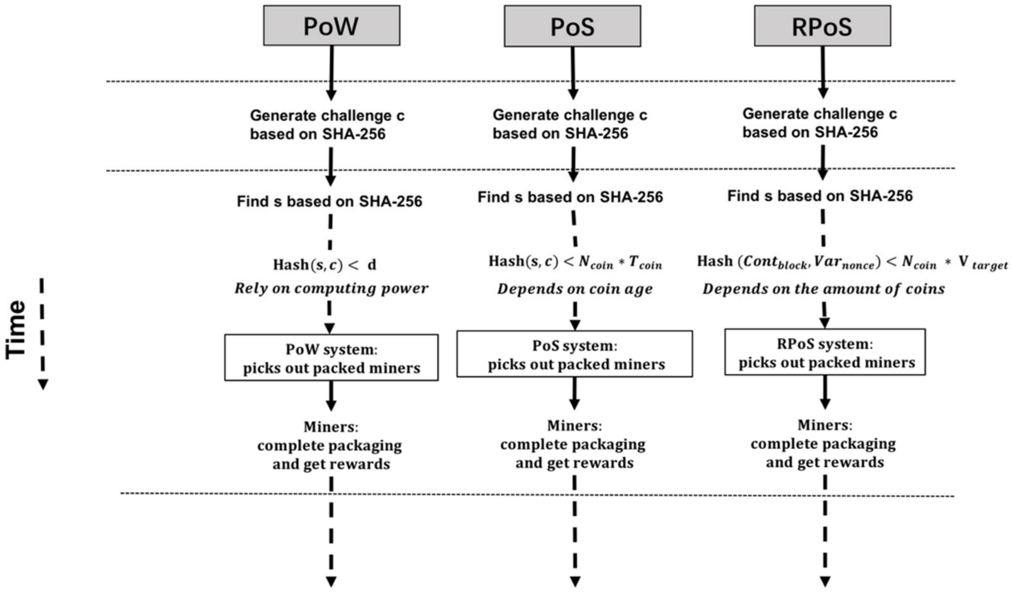
PoW
PoS
RPoS
Generate challenge c based on SHA-256
Generate challenge c based on SHA-256
Generate challenge c based on SHA-256
Find s based on SHA-256
Find s based on SHA-256
Find s based on SHA-256
$\mathrm{Hash}(s, c) < d$
Rely on computing power
$\mathrm{Hash}(s, c) < N_{coin} * T_{coin}$
Depends on coin age
$\mathrm{Hash}\,(Cont_{block}, Var_{nonce}) < N_{coin} * V_{target}$
Depends on the amount of coins
Time
PoW system: picks out packed miners
PoS system: picks out packed miners
RPoS system: picks out packed miners
Miners: complete packaging and get rewards
Miners: complete packaging and get rewards
Miners: complete packaging and get rewards

Figure 3. The process of obtain packing chance by the three consensus protocols: Pow, PoS, RPoS.

By adding the dynamic adjustment through V $_{target}$ and the maximum number of rollbacks, it is possible to limit the double benefit (as described in Figure 2) of nodes that cheat on different forks when N@S attack occurs. By the maximum number of rollbacks, the upgraded nodes are the maximum extent degraded and returned to the un-upgraded state, so that all data will return to the original state, then the fork is eliminated. The assignment of the specific maximum number of rollbacks needs to be adjusted according to the comprehensive situation of the system nodes' cheating ability. The N@S attack can be recognized by verifying the rollback block, but when the rollback number of the block is greater than the maximum rollback number, the chain is not merged, so the cheating nodes can only perform "mining" on the original chain. If the block is verified, the number of rollbacks is less than the maximum rollback number, then the valid block is considered, the information is merged, and the subsequent transaction behavior is continued. In summary, the maximum number of rollbacks in RPoS system can effectively resist N@S attack.

5. Comparison of the Three Consensus Protocols

5.1. Theoretical Comparison

Under the framework proposed in Section 3, we compare and analyze the performance of the three consensus protocols as shown in Table 2.

Table 2. The feature comparison of the three consensus protocols: PoW, PoS, RPoS.

Feature \ Protocol		PoW	PoS	RPoS
Power consumption		high	low	low
Robustness	51% attack	high	low	low
	Coin age accumulation attack	n/a	high	low
	N@S attack	n/a	high	low
Transactions Per Second (TPS)		~7	30-40	>40

Table 2 reports the key differences between the consensus protocols. We introduce the comparison results as follows.

(1) Power consumption. In PoW systems, miners consume a lot of power to compete for packing opportunities using a large number of mining machines, making the system energy-intensive and unsustainable. As mentioned in Section 3, the Bitcoin system consumes more energy than the entire nation of Switzerland [40]. Hence, the power consumption of PoW is high in Table 2. In PoS systems, miners rely on the stake (the amount of coins held and coin age) for packing competition, and the power consumption of PoS is low in Table 2, which is much more energy-saving and sustainable than PoW. In RPoS systems, miners compete for packing opportunity based on the amount of coins. Similar to PoS, without using mining machines, the power consumption of RPoS is also low in Table 2. Hence, both PoS and RPoS have the advantage over PoW in terms of energy-saving.

(2) Robustness. PoW systems (taking the Bitcoin system as an example) are becoming increasingly centralized due to a small number of mining pools, leading to a high risk of 51% attack in the system [42]. Hence, PoW systems often have low robustness, as we indicated in Table 2. The weaknesses of PoS systems are coin age accumulation attack and N@S attack, as we introduced in Section 3.3. Hence, PoS faces high risk of these two attacks as in Table 2. This motivated us to propose RPoS, making the blockchain system robust against these attacks. RPoS uses the amount of coins to compete for packing opportunities, instead of coin age, so there is almost no risk of coin age accumulation attack and N@S attack in the system. PoW, of course, is immune (not applicable, n/a) to these PoS attacks as it does not have the concept of stake. Meanwhile, rational nodes in PoS and RPoS systems will not launch 51% attack because their payoff will be negative [11]. Hence, we suggest that the risk of 51% attack in PoS and RPoS systems is low.

(3) TPS. The TPS of PoW system is about 7, and the TPS of PoS system is 30-40, which is more efficient than PoW [43]. RPoS protocol is a PoS-based protocol which removed the process of currency age selection and clearing, hence it is very likely that RPoS should be faster than PoS.

5.2. *Simulation Comparison*

The research goal of this section is to understand how the trade request-satisfied ratio is affected by different consensus protocols and trade network topologies. We consider the trade network topologies because the nodes have to trade with the neighbors in the trade network, and thus the connection patterns matter. We build an agent-based model using the agent-based modeling and simulation (ABMS) technique, which can directly simulate the actions and interactions of autonomous agents (both individual or collective entities such as organizations or groups) with a view to assessing their effects on the system as a whole [44]. Based on the complex adaptive systems theory, ABMS has been applied in many studies, such as supply chains, biological systems, financial systems and economic systems [45].

5.2.1. Assumptions and Settings in the Agent-based Model

We extended an existing agent-based blockchain model [33] by simulating the proposed RPoS consensus protocol. Hence, there are three key assumptions in the model which capture the essential differences of the three consensus protocols.

Assumption A1: Under PoW consensus protocol, the probability that a miner gets coin reward is positively associated with his/her computation power.

Assumption A2: Under PoS consensus protocol, the probability that a miner gets coin reward is positively associated with his/her stake.

Assumption A3: Under RPoS consensus protocol, the probability that a miner gets coin reward is positively associated with his/her coin balance.

Next, we consider three common network topologies: random, small-world, or scale-free. We have to assume that the type of trade network topology could be one of them because typical users have multiple coin accounts and the transactions are anonymous [46], making it extremely difficult to identify the network topology of traders.

More assumptions and settings can be found in the paper [33], in which the major ones are: three groups of traders (300 noisy traders, 300 herd traders, and 300 game traders) and each group can be further divided into two agent types (200 trader agents and 100 miner agents); the model thus contains 600 trader agents, 300 miner agents, and 1 system agent; the noisy traders make random decisions on buying/selling/holding coins; herd traders are very sensitive to the fluctuation of coin price index, because such agents represent the coin investors; game traders buy coins while others are selling and sell coins while others are buying, for the purpose of chasing larger profits than behaving as herd traders; and miners are special traders with additional attributes (e.g., computation power, stake) because some of them will be selected by the system agent to create blocks and get a certain number of coins as reward.

5.2.2. Simulation Design

We first conduct nine experiments—(A1, A2, A3 in random, small-world, or scale-free networks, respectively)—with different consensus protocols and trade network topologies. We develop the model using Python, and perform each experiment 100 times to ensure robust outputs against randomness in initializing the computation power, miner selection, policy selection, and so on. All the 100 independent tests of each experiment can be well compared and reproduced by assigning $\{0, 1, 2, \ldots, 99\}$ as random seeds, which means that the differences among experiments almost only depend on the configuration of its consensus protocol and trade network topology.

Each simulation stops after 1000 time steps. Therefore, the total computation load is: 9 experiments × 100 tests with different random seeds × 1000 time steps. During simulation, we collect the system-wide trade request-satisfied ratio data to evaluate the performance of a blockchain.

5.2.3. Results and Discussion

The averaged time series data of trade request-satisfied ratio is illustrated in Figure 4. The simulation results at the final time step are presented in Table 3, in which the values are averaged across 100 samples, and the standard deviations are given in brackets.

We can observe that the two subplots in the random and small-world networks are very alike. Besides, in these two subplots, PoW and RPoS have similar trade request-satisfied ratio, while the PoS has the highest trade efficiency. This is because both PoW and RPoS will not reset the computation power or the coin balance of the selected miner, while the PoS will empty the stake of selected miner, leading to smaller wealth inequality. In particular, PoW and RPoS tend to build a positive feedback between "large probability of being selected" and "better condition in miner selection", and only few miners will be rewarded with new coins under PoW and RPoS. Then, a rich agent has to deal with many relatively poorer agents to fulfill his/her coin request, leading to the low request-satisfied ratio. In contrast, the miner under PoS will be unlikely to be selected in several time steps later, leading to the situation that more miners will be rewarded. Since the wealth inequality is smaller under PoS, agents are more likely to trade with each other in random and small-world networks.

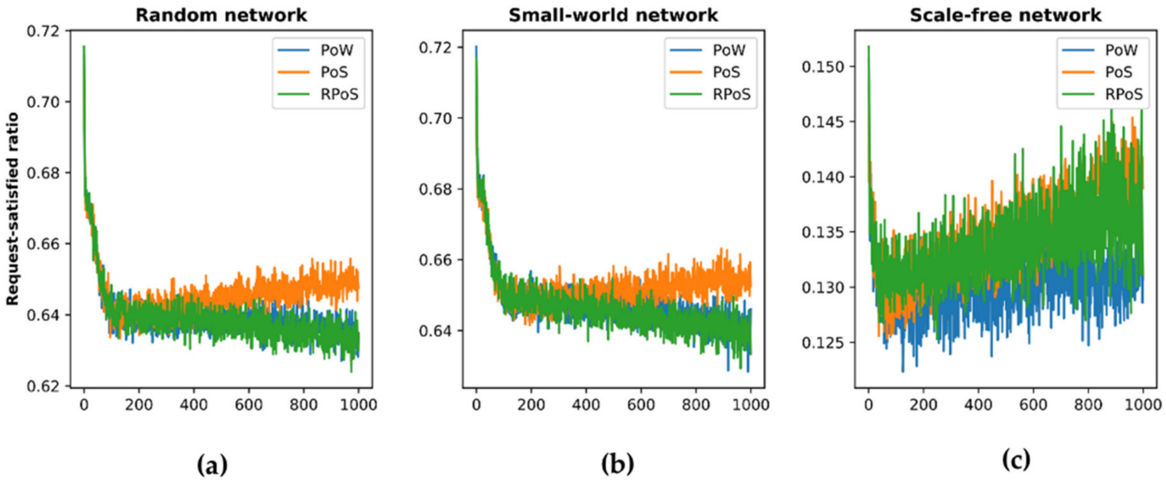

Figure 4. The averaged time series data of trade request-satisfied ratio based on 100 samples. Figure (**a**): Request-satisfied ratio performance of PoW, PoS and RPoS protocol in Random network; Figure (**b**): Request-satisfied ratio performance of PoW, PoS and RPoS protocol in Small-world network; Figure (**c**): Request-satisfied ratio performance of PoW, PoS and RPoS protocol in Scale-free network.

Table 3. The trade request-satisfied ratio based on 100 samples.

Network Topology	PoW	PoS	RpoS
Random	0.634(0.031)	0.648(0.026)	0.635(0.029)
Small-world	0.643(0.029)	0.653(0.028)	0.645(0.036)
Scale-free	0.131(0.027)	0.139(0.020)	0.135(0.038)

Next, we examine the impact of trade network topology on trade request-satisfied ratio. The third subplot in Figure 4 shows that the trade request-satisfied ratios are much smaller than those in random and small-world networks. In particular, the trade request-satisfied ratio in scale-free trade network is about 13-14%, while it is 63-65% (almost five-fold) in other two networks. This big difference is probably caused by the serious connectivity inequality of scale-free trade network, i.e., the probability that a node gains a connection is proportional to its current degree. In a scale-free blockchain system, very few agents have a lot of connections for trade, while most nodes only have one or two connections. Although the high-degree node is connected with many neighbors, a deal can only be reached with his/her partial neighbors when the node has non-zero trade request. Hence, this finding suggests that the scale-free network topology should not be preferred due to its high connectivity inequality. If possible, the blockchain system designer or operator should attempt to increase the connectivity among participants by, e.g., incentivizing apathetic or newly-joined participants to link with others. In addition, we see that the RPoS obtained larger trade request-satisfied ratio in the scale-free network compared with PoW, but still smaller than that under PoS. The main reason is compared to PoS protocol, and RPoS protocol uses the amount of coins to replace the age of coins to choose the packing miner. Therefore, PoS system has more miners who have enough qualification to be selected for packing than RPoS system. In addition, the time required to select a suitable packaged miner becomes longer in RPoS system, so that the trade request-satisfied ratio of RPoS system becomes a little lower than in PoS system.

To conclude, the proposed RPoS leads to similar or better trade efficiency than PoW, and it is very energy-saving, robust against 51% attack, and efficient in terms of TPS according to Table 2. In other words, RPoS outperforms PoW in all the four features. Compared with PoS, RPoS is much more robust against the coin age accumulation attack and N@S attack, and it also has higher TPS than PoS. Therefore, we suggest that RPoS is suitable in today’s blockchain system.

6. Conclusion

This paper analyzes the characteristics and problems of the existing consensus protocols (in particular, PoW and PoS), and proposes a new protocol RPoS by improving the PoS protocol. The main improvement is that RPoS protocol uses the amount of coins instead of the age of coins to reduce the risk of coin age accumulation attack in the system. Another improvement is that RPoS protocol adds the maximum number of rollbacks, which can effectively prevent N@S attack which may occur in the system. After comparing the differences between the three consensus protocols: PoW, PoS, and RPoS, we use an agent-based blockchain model to simulate the impact of different consensus protocols and trade network topologies on the fourth aspect: trade request-satisfied ratio.

We conducted three experiments in which PoW, PoS, RPoS consensus protocols and random, small-world, scale-free trade networks are implemented. Experimental results show that the proposed RPoS protocol leads to similar or better trade efficiency than PoW, and it is very energy-saving, robust against 51% attack, and efficient in terms of TPS. In other words, RPoS outperforms PoW in all the four features. Compared with PoS, RPoS is much more robust against the coin age accumulation attack and N@S attack, and it also has higher TPS than PoS. Therefore, we suggest that RPoS is suitable for today's blockchain system.

We suggest some further research directions: 1. The maximum number of nodes that ensures the stability and robustness of RPoS system cannot be determined. The further research can use the number of nodes as a variable for RPoS system, and then find the largest value using simulation-based optimization techniques. 2. The verification of trade request-satisfied ratio in our research is based on simulation and does not use empirical data, because we have no way to obtain real data of RPoS system as typical users have multiple coin accounts and the transactions are anonymous. With fast-developing methods, the trade request-satisfied ratio of RPoS protocol could be verified with real-world data.

Author Contributions: Conceptualization, formal analysis, writing—original draft preparation by A.L.; validation and supervision by X.W.; methodology and writing—review and editing by Z.H. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by National Natural Science Foundation of China, grant number 71932002, 71932008, 71901202 and University of Chinese Academy of Sciences.

Acknowledgments: The authors greatly appreciate the editor and anonymous referees for their comments, which helped to improve this paper.

Conflicts of Interest: The authors declare no conflict of interest.

Appendix A

Table A1. The list of acronyms.

Acronyms	Term	Brief Introduction
RpoS	Robust Proof of Stake	The proposed consensus protocol for blockchain system
PoW	Proof of Work	The first consensus protocol for blockchain system
PoS	Proof of Stake	A popular consensus protocol for blockchain system
P2P	Peer to Peer	A distributed application architecture that partitions tasks between peers
ETH	Ether	A blockchain system based on PoW and PoS
EOS	Enterprise Operation System	A blockchain system based on Delegated PoS
DApp	Decentralized Application	Application in decentralized blockchain systems
RPCA	Ripple Consensus Algorithm	A consensus protocol for blockchain system
BFT	Byzantine Fault Tolerance	A consensus protocol for blockchain system
ABMS	Agent-based Modeling and Simulation	A research method to understand agent interactions
N@S	Nothing-at-Stake	A type of attack which can happen in PoS blockchain system
TPS	Transaction Per Second	An index to describe the trade efficiency of a financial system

References

1. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. In *Manubot*; Satoshi Nakamoto Institute: Panama, Pananma, 2019.
2. Yuan, Y.; Wang, F.Y. Blockchain: The state of the art and future trends. *Acta Autom. Sin.* **2016**, *42*, 481–494.
3. Restuccia, F.; Das, S.K.; Payton, J. Incentive mechanisms for participatory sensing: Survey and research challenges. *ACM Trans. Sens. Netw.* **2016**, *12*, 1–40. [CrossRef]
4. Baliga, A. Understanding blockchain consensus models. *Persistent* **2017**, *4*, 1–14.
5. Zhang, H.; Dong, Y.; Chiclana, F.; Yu, S. Consensus efficiency in group decision making: A comprehensive comparative study and its optimal design. *Eur. J. Oper. Res.* **2019**, *275*, 580–598. [CrossRef]
6. Mehar, M.I.; Shier, C.L.; Giambattista, A.; Gong, E.; Fletcher, G.; Sanayhie, R.; Kim, H.M.; Laskowski, M. Understanding a revolutionary and flawed grand experiment in blockchain: The DAO attack. *J. Cases Inf. Technol.* **2019**, *21*, 19–32. [CrossRef]
7. Ethereum Home Page. Available online: https://ethereum.org (accessed on 15 February 2020).
8. EOSIO Home Page. Available online: https://eos.io (accessed on 15 February 2020).
9. PeckShield. The Top 10 Security Events of Blockchain in 2008. Available online: https://blog.csdn.net/PeckShield/article/details/88801450 (accessed on 11 February 2020).
10. Li, W.; Andreina, S.; Bohli, J.; Karame, G. Securing proof-of-stake blockchain protocols. In *Data Privacy Management, Cryptocurrencies and Blockchain Technology*; Springer: California, America, 2017; pp. 297–315.
11. King, S.; Nadal, S. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake." self-published paper. 2012, pp. 1–6. Available online: https://download.csdn.net/download/vinsuan1993/9963770 (accessed on 1 April 2020).
12. Bitcoin, M. Unlocking Digital Cryptocurrencies. In *Antonopoulos*; Andreas, M., Ed.; O'reilly Media: Sebastopol, America, 2014; pp. 36–62. Available online: https://www.foxebook.net/mastering-bitcoin-unlocking-digital-crypto-currencies/ (accessed on 1 April 2020).
13. DOGECOIN Home Page. Available online: https://dogecoin.com (accessed on 16 February 2020).
14. Litcoin Home Page. Available online: https://litecoin.org (accessed on 16 February 2020).
15. Huh, J.; Seong-Kyu, K. The blockchain consensus algorithm for viable management of new and renewable energies. *Sustainability* **2019**, *11*, 3184. [CrossRef]
16. Fadeyi, O.; Krejcar, O.; Maresova, P.; Kuca, K.; Brida, P.; Selamat, A. Opinions on Sustainability of Smart Cities in the Context of Energy Challenges Posed by Cryptocurrency Mining. *Sustainability* **2020**, *12*, 169. [CrossRef]
17. Chang, S.E.; Luo, H.L.; Chen, Y. Blockchain-Enabled Trade Finance Innovation: A Potential Paradigm Shift on Using Letter of Credit. *Sustainability* **2019**, *12*, 1–16. [CrossRef]
18. Enescu, F.M.; Bizon, N.; Onu, A.; Răboacă, M.S.; Thounthong, P.; Mazare, A.G.; Șerban, G. Implementing Blockchain Technology in Irrigation Systems That Integrate Photovoltaic Energy Generation Systems. *Sustainability* **2020**, *12*, 1540. [CrossRef]
19. Back, A.; Bentov, I. Note on fair coin toss via bitcoin. *arXiv* **2014**, arXiv preprint. arXiv:1402.3698. Available online: https://arxiv.org/abs/1402.3698 (accessed on 5 February 2020).
20. Narayanan, A.; Bonneau, J.; Felten, E.; Miller, A.; Goldfeder, S. *Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction*; Princeton University Press: Princeton, NJ, USA, 2016.
21. Luu, L.; Narayanan, V.; Zheng, C.; Baweja, K.; Gilbert, S.; Saxena, P. A secure sharding protocol for open blockchains. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security, Vienna, Austria, 24–28 October 2016; pp. 17–30.
22. Houy, N.; The economics of Bitcoin transaction fees. SSRN Electronic Journal 2014. Available online: https://www.researchgate.net/publication/272244412_The_Economics_of_Bitcoin_Transaction_Fees (accessed on 1 April 2020).
23. Larimer, D. Delegated proof-of-stake (dpos) Bitshare whitepaper (2014). Available online: https://bitshares.org/technology/delegated-proof-of-stake-consensus/ (accessed on 1 April 2020).
24. David, S.; Youngs, N.; Britto, A. The ripple protocol consensus algorithm. *Ripple Labs Inc White Paper* **2014**, *5*, 2–8.
25. Miguel, C.; Liskov, B. Practical Byzantine Fault Tolerance. In Proceedings of the Third Symposium on Operating Systems Design and Implementation, New Orleans, LA, USA, 22–25 February 1999.

26. Sukhwani, H.; Martínez, J.M.; Chang, X.; Trivedi, K.S.; Rindos, A. Performance Modeling of PBFT Consensus Process for Permissioned Blockchain Network (hyperledger fabric). In Proceedings of the 2017 IEEE 36th Symposium on Reliable Distributed Systems (SRDS), Hong Kong, China, 26–29 September 2017.
27. Lamport, L. Paxos Made Simple. *ACM Sigact News* **2001**, *32*, 18–25.
28. Diego, O.; Ousterhout, J. In search of an understandable consensus algorithm. 2014 USENIX Annual Technical Conference (SENIX ATC 14)., Philadelphia, PA, USA, 19–20 June 2014; 2014.
29. Stallings, W. *Operating Systems*; Simon & Schuster Trade: New York, America, 1994.
30. Saleh, F.; Blockchain without waste: Proof-of-stake. Available at SSRN 3183935. 2019. Available online: https://www.researchgate.net/publication/325891130_Blockchain_Without_Waste_Proof-of-Stake (accessed on 1 April 2020).
31. Han, X.; Liu, Y. Research on the consensus Mechanisms of Blockchain Technology. *Netinfo Secur.* **2017**, *9*, 147–152.
32. Zhou, Y. The evolution of blockchain core technology-consensus mechanism evolution. *Comput. Educ.* **2017**, *4*, 5–9. (In Chinese)
33. Wei, X.; Li, A.; Zhou, H. Impacts of consensus protocols and trade network topologies on blockchain system performance. *Journal of Artificial Societies and Social Simulation.*. In Press.
34. Bach, L.M.; Mihaljevic, B.; Zagar, M. Comparative analysis of blockchain consensus algorithms. In Proceedings of the 2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics, Opatija, Croatia, 21–25 May 2018; pp. 1545–1550.
35. Zheng, Z.; Xie, S.; Dai, H.; Chen, X.; Wang, H. An overview of blockchain technology: Architecture, consensus, and future trends. In Proceedings of the 2017 IEEE international congress on big data (BigData congress), Honolulu, HI, USA, 25–30 June 2017; pp. 557–564.
36. The soaring currency price and the EOS million-level TPS technology known as Alipay may be empty talk. SoHu Page. 2018. Available online: https://www.sohu.com/a/232647141_100128500 (accessed on 19 February 2020).
37. Mearian, L. MIT's Blockchain-Based 'Spider' Offers 4X Faster Cryptocurrency Processing. 2020. Available online: https://www.computerworld.com/article/3518893/mits-blockchain-based-spider-offers-4x-faster-cryptocurrency-processing.html (accessed on 20 February 2020).
38. Back, A. Hashcash-a Denial of Service Counter-measure. 2002. Available online: https://www.researchgate.net/publication/2482110_Hashcash_-_A_Denial_of_Service_Counter-Measure (accessed on 1 April 2020).
39. Ball, M.; Rosen, A.; Sabin, M.; Vasudevan, P. Proofs of Useful Work. In *Zeitschrift fur Physik*; Springer: New York, NY, USA, 1925.
40. Vincent, J. Bitcoin Consumes More Energy than Switzerland, according to New Estimate. 2019. Available online: https://www.theverge.com/2019/7/4/20682109/bitcoin-energy-consumption-annual-calculation-cambridge-index-cbeci-country-comparison (accessed on 19 February 2020).
41. Bastiaan, M. Preventing the 51%-attack: A stochastic analysis of two phase proof of work in bitcoin. Available online: http://referaat.cs.utwente.nl/conference/22/paper/7473/preventingthe-51-attack-a-stochasticanalysis-oftwo-phase-proof-of-work-in-bitcoin.pdf (accessed on 16 February 2020).
42. Bitcoin Hashing Power. 2020. Available online: https://www.blockchain.com/zh-cn/pools? (accessed on 18 March 2020).
43. Yu, H. TPS Comparison of Blockchain Mainstream Chains. 2019. Available online: https://blog.csdn.net/ccr1001ccr1001/article/details/88529808 (accessed on 19 March 2020).
44. Macal, C.M.; North, M.J. Agent-based modeling and simulation. In Proceedings of the 2009 Winter Simulation Conference, Austin, TX, USA, 13–16 December 2009.
45. Lin, J.L.; Kiladis, G.N.; Mapes, B.E.; Weickmann, K.M.; Sperber, K.R.; Lin, W.; Wheelerf, M.C.; Schubertg, S.D.; del Genioh, A.; Donner, L.J.; et al. Tropical Intraseasonal variability in 14 IPCC AR4 climate models. *Part I: Convective signals. J. Clim.* **2006**, *19*, 2665–2690.
46. Antonopoulos, M.A.; Wood, G. *Mastering Ethereum: Building Smart Contracts and Dapps*; O'reilly Media: Sebastopol, America, 2018.