Hindawi
Security and Communication Networks
Volume 2020, Article ID 8839047, 11 pages
https://doi.org/10.1155/2020/8839047

Research Article

Rational Protocols and Attacks in Blockchain System

Tao Li,[1,2,3] Yuling Chen,[1,2] Yanli Wang,[3] Yilei Wang,[3] Minghao Zhao,[4] Haojia Zhu,[3] Youliang Tian,[1,2] Xiaomei Yu,[5] and Yixian Yang[1,2]

[1]*State Key Laboratory of Public Big Data, Guizhou University, Guizhou 550025, China*
[2]*College of Computer Science and Technology, Guizhou University, Guizhou 550025, China*
[3]*School of Information Science and Engineering, Qufu Normal University, Rizhao 276825, China*
[4]*School of Software, Tsinghua University, Peking 100084, China*
[5]*School of Information Science and Engineering, Shandong Normal University, Jinan 250014, China*

Correspondence should be addressed to Yuling Chen; ylchen3@gzu.edu.cn

Received 13 July 2020; Revised 25 August 2020; Accepted 15 September 2020; Published 24 September 2020

Academic Editor: Xiaolong Xu

Blockchain has been an emerging technology, which comprises lots of fields such as distributed systems and Internet of Things (IoT). As is well known, blockchain is the underlying technology of bitcoin, whose initial motivation is derived from economic incentives. Therefore, lots of components of blockchain (e.g., consensus mechanism) can be constructed toward the view of game theory. In this paper, we highlight the combination of game theory and blockchain, including rational smart contracts, game theoretic attacks, and rational mining strategies. When put differently, the rational parties, who manage to maximize their utilities, involved in blockchain chose their strategies according to the economic incentives. Consequently, we focus on the influence of rational parties with respect to building blocks. More specifically, we investigate the research progress from the aspects of smart contract, rational attacks, and consensus mechanism, respectively. Finally, we present some future directions based on the brief survey with respect to game theory and blockchain.

1. Introduction

To facilitate data processing, clients prefer to host them to a trusted party. However, the security problems have proliferated due to lack of trust parties. In 2017, 180,000 patient records were stolen by Hackers from clinics such as Aesthetic Dentist in the United States [1]. In September 2017, 140 million clients' personal information in Equifax, an American credit reporting company, was stolen [2]. In April 2018, 87 million customers' data information was leaked on Facebook platform [3]. All these information leakage incidents derive from the heavy dependence upon the centralized trusted parties. Once trusted parties are compromised, system securities are in grave danger. Therefore, it is challenging to discharge the dependence on trusted parties and enhance the nodes' independence of distributed computing [4–7].

Blockchain technology, a "decentralized" underlying support technology, can establish trust among distributed nodes. Thus, it may solve the problems mentioned above. In January 2016, the British Government released a thematic study on blockchain to actively promote the application of blockchain in financial and government affairs. In that same year, the People's Bank of China held a seminar on digital currency to explore the feasibility of using blockchain technology to issue virtual currency in order to improve the efficiency, convenience, and transparency of financial activities. The white paper, issued in 2016 by China Blockchain Technology and Application Development, defines blockchain as a new application framework for computer technology such as distributed data storage, point-to-point transmission, consensus mechanism, encryption algorithm, etc. However, there has also been a tremendous amount of work in the underlying technology of blockchain. The basic framework of blockchain, combined with game theory [8, 9], complex networks, and rational protocols [10, 11], is presented in Figure 1. Note that Figure 1 is different from that of the figure in [12], although it inherits from it, since the combined parts are the focus of this survey.

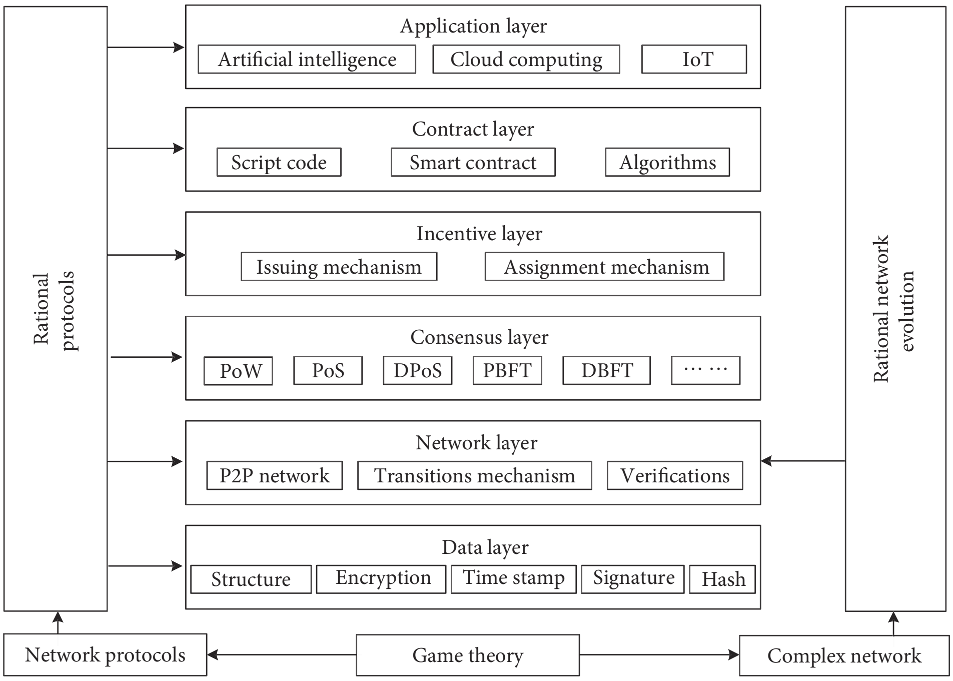

Figure 1: The framework of blockchain combined with game theory.

The underlying technology of blockchain covers a wide range of contents, which can be divided into data layer, network layer, consensus layer, incentive layer, contract layer, and application layer according to their functions. The nodes in the network layer, without mutual trust, achieve verification through a certain consensus mechanism such as proof of work (PoW), proof of stake (PoS), and the practical Byzantine fault tolerance algorithm (PBFT). These mechanisms provide solid foundations for the smooth implementation of the contract layer and the application layer. In effect, the blockchain network is a complex network, which exhibits the character of small world. Therefore, we may leverage the theory of complex network to investigate the topological structure of blockchain network. On the other hand, the nodes in blockchain network are social, whose behaviours may be influenced by the topological structure. The incentive layer connects the bottom data with the upper application through the network layer and the consensus layer. The incentive mechanism (IC) is the core driving source of the technical value of the blockchain [13].

Generally speaking, the main function for the nodes in network layer mechanism is to maximize their economic benefits. Therefore, the incentive layer needs to design the economic incentive mechanism reasonably such that the nodes maximize their economic benefits. Meanwhile, the security and effectiveness of blockchain system should be ensured in order to form a stable consensus on blockchain history. In economics, this kind of behaviours is called rational behaviours. In fact, rationality is a basic concept of economic theory, which mainly focus on the interaction among incentive structures and analyses the optimal strategy for rational participants. In consequence, rational protocols, participated by rational nodes, can describe the characteristics of nodes and provide an efficient solution for some practical problems.

In Figure 1, rational behaviours intersect each layer in blockchain, which can be utilized to achieve some desired conclusions. In this paper, we address the rational behaviours in blockchain, which are common concepts in game theory. That is, we may probe rational behaviours toward the view of game theory since it is a powerful tool for rational behaviours. More specifically, we first investigate the rational behaviours in smart contracts. For example, attackers may adopt rational strategies in rational smart contracts and criminal smart contracts in order to maximize their incomes (refer to Section 3). Since the inspiration of the rational parties is economic incentives, they have enough motivation to sponsor rational attacks by leveraging incentive mechanisms in game theory (refer to Section 4). The main function of the consensus layer is responsible for assigning rewards. It is crux for the whole blockchain system to maintain a sound economic and ecological environment. Therefore, we outline some rational consensus mechanisms (refer to Section 5). Finally, we highlight the future directions with respect to the combination of game theory and blockchain (refer to Section 6).

2. Classical Games Implemented in Blockchain

Parties, in blockchain, manage to maximize their economic incomes, so they have incentives to adopt rational strategies when they participate in protocols. It is not in conflict when the strategies are incompatible with the security requirements of the protocols. Put differently, rational parties in blockchain can achieve maximum incomes by just honestly following the protocols. However, honest behaviours, in most cases, are not harmonious with these rational strategies. That is, rational parties can always get around the secure protocols to maximize their incomes, which breach the secure protocols to some extent. From the above, the interaction between rational parties and secure protocols can be constructed as games. On the other hand, strategies which are incentive compatibility can be solved by mechanism design. Both fall into the field of game theory. Therefore, it is necessary to survey on game theory in blockchain.

In effect, various works (aka rational protocols) analyse the security of protocols with respect to blockchain toward the view of game theory. The basic idea is to establish protocols as games, where an equilibrium exists such that rational parties achieve maximum incomes and meanwhile protocols are secure according to the definitions. Basically, these rational protocols derive from and are constructed as classical games, like prisoner's dilemma game and tragedy of the commons game. In this paper, we just investigate these two games [14].

2.1. Prisoner's Dilemma Game. The derivation of prisoner's dilemma game is as follows: two prisoners (say Alice and Bob) are thrown in jail without confession in collusion. They have two choices: defect and collude. There are altogether four outcomes according to different choices. (1) If both defect, each gets eight years in prison. (2) If both collude, each gets one year in prison. (3) If Alice defects while Bob colludes, Alice is acquitted of a charge while Bob gets ten years in prison. (4) If Bob defects while Alice colludes, Bob is acquitted of a charge while Alice gets ten years in prison.

This is a classical game in game theory, and there is one Nash equilibrium (defect, defect). Put differently, two prisoners have incentives to defect since it is optimal for them. However, it is obvious that mutual collusion may maximize their utilities. Thus, prisoners run into dilemma, where they have to settle for the second-best solution. Normally, we outline it in matrix form as shown in Table 1.

Prisoner's dilemma game applies to such scenarios where parties cannot collude beforehand, and they do not trust each other. Blockchain is rightly such a distributed scenario, where distrustful parties are distributed all over the world. All parties try to maximize their utilities while they may involve deeply the dilemma, where the conflict exists between the security requirements of the protocols and the utility requirements of the rational parties. In Sections 3–5, strategic attacks and rational protocols based on game theory highlight how these blockchain techniques utilize them to solve some vexing problems in their respective fields.

2.2. Tragedy of the Commons Game. The security issues in blockchain come from the conflict between the individual and the collective rationality. The blockchain system is secure if all parties follow the protocols therein, which are incentive compatible with the utility requirements. Otherwise, the security of the protocols is breached since rational parties always manage to maximize their utilities by violating the protocols.

However, if rational parties achieve their utility endlessly at the expense of the security of the whole blockchain system. The blockchain will disappear someday, which lead to undesirable results that rational parties gain nothing. This scenario is similar to the tragedy of the common game, where the security of the blockchain system is the common goods for rational parties.

The basic model of tragedy of the commons game in blockchain is as follows. Say there are n parties in blockchain system and each of them has m strategies $q_1, q_2, \ldots, q_m$ to choose. The revenue $V(i) = Q(q_1, q_2, \ldots, q_m)$ of each strategy is a decreasing function $Q(\cdot)$ of the whole strategies. On the other hand, there exist cost $c_1, c_2, \ldots, c_m$ with respect to each strategy. Therefore, the utility for party i when he chooses strategy q_j is

$$U(i) = q_i \cdot V(i) - q_i \cdot c_i. \tag{1}$$

In fact, the tragedy of the commons game is a social trap for rational parties. They must leverage their strategies such that they may maximize their utilities in the long run. As mentioned above, the interaction between rational parties and protocols in blockchain can be modelled as a tragedy of the commons game, especially in pool mining (refer to Section 4).

3. State of the Art of Smart Contracts

In 1996, Nick Szabo put forward the concept of smart contract. "A smart contract is a set of promises defined in digital form, including agreements on which contract participants can implement these promises." Before the implementation of smart contracts, participants make a commitment. Then the smart contract will be executed automatically when the conditions are triggered, where no participants can bias the contract commitments. Smart contract can be automatically executed without prior review, which may avoid intractable issues such as contract disputes [12]. However, smart contract has not been applied to the actual industry due to the lack of effective technical support and trust platform. Ethereum provides an implementable development platform for smart contract by drawing on the characteristics of blockchain technology such as decentralization, nontamperability, process transparency, traceability, and so on [15]. Ethereum offers complete scripting language of Turing, which can embed more additional information. Therefore, any smart contract, once precisely defined, can be constructed and implemented automatically on Ethereum. The white paper of smart contracts: 12 Use Case for Business & Beyond, published by the Chamber of Digital Commerce and Smart Contracts Alliance in December 2016, points out that smart contract can be applied in various fields like mortgage loans, Internet of things, medical research, etc.

The security problem of smart contract can be summarized into two aspects: internal security and external attack. Luu et al. [16] put forward a new security problem with respect to smart contract and present the corresponding solutions to strengthen the robustness of smart

Table 1: The matrix of prisoner's dilemma game.

Alice, Bob	Defect	Collude
Defect	(−1, −1)	(0, −10)
Collude	(−10, 0)	(−8, −8)

contracts. Kosba et al. [17] propose a decentralization system, Hawk, which addresses the privacy of the content of smart contracts. Bhargavan et al. [18] compile the smart contracts into F^* language to verify the correctness of the smart contract. Atzei et al. [19] summarize the smart contracts on the Ethereum. They focus on the robustness of contracts and categorize programming pitfalls in the programs. Dika categorizes the vulnerabilities of smart contracts [20]. Furthermore, they analyse code security issues in smart contracts on the Ethereum, such as Oyente, Security, and SmartCheck. Recently, Nikolic et al. [21] analyse about a million smart contracts, among which 34,200 are inherently vulnerable to hackers. In addition, they also utilize MAIAN as a tool to analyse the validity of smart contracts. Based on a sample of 3,759 smart contracts, 3,686 of them contain loopholes, with an 89% probability of vulnerability. A loophole in the smart contract will also cause the customer's electronic property to be locked up in Ethereum. In November 2017, about $300 million were permanently frozen in the Ethereum for the maloperation of some users of Ethereum smart contract.

In addition to the inherent security problems in smart contract, there are also many attacks specifically targeting smart contract. Velner et al. [22] introduce an attack model based on smart contract, through which attackers can destroy the normal work of the mine pool. Juels et al. [23] have proposed the concept of criminal smart contract. Criminals can use smart contracts to carry out some illegal activities, such as illegally selling pirated films. They focus on discussing the feasibility and harmfulness of criminal smart contracts. Finally, they appeal to the introduction of relevant laws and policies to improve technical prevention measures. Brunoni and Beaudet-Labrecque also have in-depth discussions on how to use smart contracts to commit cybercrimes [24]. Alharby and van Moorse even think there are no countermeasures to criminal smart contracts at present [25]. The current research has increased people's concern about the harm caused by smart contracts. Furthermore, scholars are trying to resist the negative effects caused by smart contracts. Wang et al. analyse the validity of the criminal smart contracts by setting some parameters reasonably. They prove that, given proper parameters, the successful probability of criminal intelligence contract is extremely low [26]. Zhang et al. further impair the threshold of criminal smart contracts by utilizing Q-learning [27]. Bigi et al. combine game theory and formal method to verify the validity of smart contracts [28]. They mainly analyse the uncertainty brought to the system by the deposit introduced by the smart contract. Consequently, they address the validity of smart contracts. Although smart contracts are not perfect and secure, they still have wide application. For example, when clients outsource some tasks in cloud computing, there are two problems: (1) the client's cost is higher and (2) once most of the clouds collude, the principal still cannot learn the correct value. Dong et al. [29] propose a smart contract to verify anticollusion in cloud computing by combining smart contract with game theory. They assume that both the client and cloud are rational participants, where the former strives to maximize their benefits by providing the correctness of the calculation results.

Figure 2 presents the future directions for smart contracts based on the above related works. The environment for smart contracts must be more complex and practical.

4. Rational Mine Pool Attack and Incentive Mechanism

Toward the economic point of view, the incentive mechanism in bitcoin has solved the problem of miners' motivation. However, the application of game theory in the field of economics has become extraordinarily mature. Therefore, it is natural to analyse some problems in bitcoin and the blockchain from the perspective of game theory. As we all know, the most important mechanism in bitcoin is mining. Tschorsch and Scheuermann provide the basic concepts and workflows of bitcoin [30]. If miners want to get bitcoin, they need to solve a specific mathematical problem. That is, miners, who solve the problem and find a bitcoin block, can get 12.5 bitcoins. By February 5, 2020, the value of a bitcoin is 9217.61 USD, which provides enough motivation for miners. However, it requires a certain amount of computing power to solve these problems. It usually takes several months or even years for a single miner to find a bitcoin block. Normally, a new block will appear on the bitcoin network in about 10 minutes. Therefore, most miners work in vain. For this reason, some miners constitute a mining pool by taking their computing power as a whole. If they find an effective block within a proper time, they will share the rewards according to their computing power. However, toward the view of game theory, miners may achieve additional rewards by leveraging the security vulnerabilities in the incentive mechanism. Therefore, rational miners have incentives to deviate from the honest strategy, which is similar to the noncooperative game in game theory.

Schrijvers et al. [31] define a pool payment function in a single pool from the perspective of game theory. In the mining pools, miners can strategically choose the time to report once they find a new block. They present three properties of the payment function: (a) incentive compatibility, (b) proportional payments, and (c) budget balanced (BB). Schrijvers et al. analyse whether the payment functions based on allocation strategies satisfy these characteristics. Proportional reward function, denoted as *R prop*, refers to the allocation of rewards according to the computing power of each miner, which is an earlier allocation strategy for the mine pool. However, *R prop* only meets the properties of (b) and (c). The Pay-Per-Share (PPS) reward function only meets the property of (a). Eyal and Sirer highlight the incentive compatibility of bitcoin protocols [32], where miners are allowed to collude. They prove that rational miners will

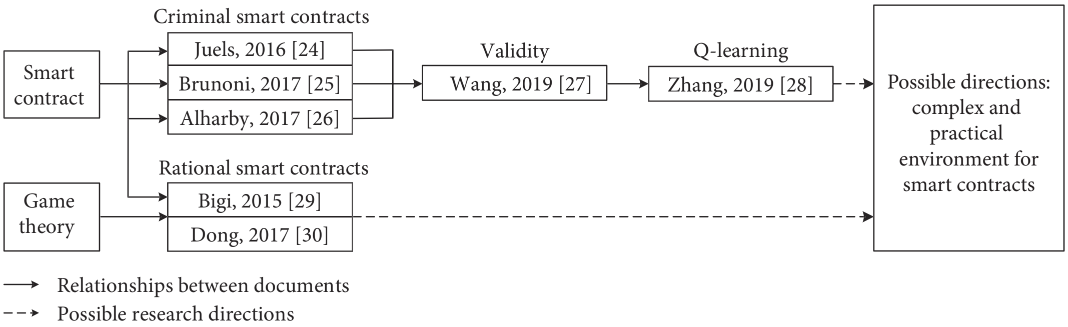

Figure 2: The possible directions for smart contracts.

eventually turn into selfish miners who collude to form a selfish pool. On the other hand, the pool can attract an increasing number of selfish miners. Therefore, the pool may develop into a super pool consisting most miners in the whole system. As a consequence, bitcoin becomes a centralized system again, which goes against the original intention of bitcoin. Put differently, any selfish mining strategy can form a super pool that controls the majority miners. Such selfish mining strategy is known as selfish mining attack. In order to resist such attacks, Eyal and Sirer propose an improved version of the bitcoin protocol which is backwards-compatible.

Nayak et al. [33] expand the space for mining strategies, including "stubborn" strategies. They prove that selfish mining is not a good strategy for a larger strategic space. Nayak et al. mainly survey two types of mining attacks: "selfish mining" style and Eclipse attack. Miners combine eclipse attacks based on the network layer to increase their rewards. In other words, the victims of some eclipse attacks, given the optimal strategy, can benefit from the attack. Kroll et al. [34] regard bitcoin mining as a game between miners and bitcoin holders. Furthermore, they address the impact of 51% attacks on the game and manage to reach an equilibrium. They also propose a new attack: goldfinger attack, where the attackers' incentives derive from exterior motivations other than bitcoin. For example, attackers may be a law enforcement agency or intelligence unit hoping to impair the bitcoin's ability. Finally, they feature the influence of goldfinger attack on the game and point out the necessity of government supervision.

Heilman introduces the freshness preferred (FP) mechanism [35], which punishes selfish miners who do not release blocks in time by using unforgeable timestamps. They increase the threshold, compared with [32], from 0.25 to 0.32. However, FP mechanism is neither incentive compatible nor robust to forgeable timestamps. That is, the implementation of FP mechanism depends on unforgeable timestamps, which are difficult to implement [36, 37]. Therefore, the implementation of FP mechanism has certain limitations. Solat and Potop-Butucaru propose a solution for selfish mining attacks and withholding attack, Zero Block [38], which does not depend on timestamps. In Zero Block scheme, the honest miners will refuse to accept the new block if a selfish miner holds a block for more than a mat interval.

Sapirshtein et al. [39] extend the work of literature and propose an efficient algorithm, which can calculate ε-optimal ($\varepsilon \geq 0$) selfish mining strategy. They prove the correctness of the algorithm and analyse its error bounds. Miners can increase their rewards relying on the efficient algorithm mentioned above. Furthermore, they launch selfish mining attacks. They also prove that if we consider the delay of the block in the network transmission, the threshold value becomes zero again. That is, no matter how many resources the attacker controls, there will always be a selfish mining strategy, which will bring more profits than honest mining. Finally, they summarize the interaction between selfish mining and double spending.

Eyal discusses the withholding attack between two mining pools [40]. There is a contradiction between individual rationality and collective rationality with respect to two mining pools, which is similar to the tragedy of the commons game. Eyal proposes a withholding attack between two mining pools. More specifically, the manager of one attacking pool first registered as a normal miner in the other victim pool. He accepts several tasks from the victim pool and assigns them to infiltrating miners in the attacking pool. The ratio of infiltrating miners in the attacking pool is called infiltration rate. The attacking pool submits part of the work capacity of the infiltrating miners to the victim pool, allowing the victim pool to evaluate the capacity of infiltrating miners. When the infiltrating miners submit full-work certificate, the attacking pool will ignore this work. The drawback of the withholding attack is that the overall calculation capacity of the victim pool has not increased (infiltrating miners do not work), but its average budget has decreased. In effect, it weakens itself for the attacking pool to split the computing power to the victim pool. As a result, withholding attack generally reduces the computing power of the entire network. For two mining pools, withholding attack is the only Nash equilibrium [41]. However, it is better for both mining pools not to conduct withholding attack. Toward the perspective of game theory, it is a miner's dilemma for the pool whether or not to conduct withholding attack. The miners' constant mining process is similar to a repeated prisoner's dilemma game. Rosenfeld suggests modifying the block structure to solve this problem [42].

In the process of mining, there are still various detailed problems to be explored besides constructing selfish mining pools. Miners earn transaction fees once they find a new block, which contain several transactions in the block. However, the number of the transactions is a difficult issue, which should balance the propagation speed and transaction fees. That is, a block with fewer transactions has higher propagation speed while less transaction fees. A block with more transactions has more transactions fees while lower propagation speed. To solve this issue, Houy defines a bitcoin mining game among miners [43], assuming that the number of transactions contained in a block is the outcome of a game. Houy discusses the impact of transaction fees on the block size toward an economic point of view [44]. Any case with fixed transaction fees is equivalent to setting the maximum block size allowed for a block. Moreover, imposing a fixed transaction fee on transactions is equivalent to imposing a compulsive tax on each transaction, which will undoubtedly impair bitcoin's economic and ecological environment. However, the transaction fees will reduce to zero again if the maximum size of each block is not restrained. In this case, the miner is similar to the follower in Stackelberg game. In order to maximize his rewards within the limited block size, the miners manage to include as many transactions as possible in the block. Figure 3 presents the future directions for rational mining attack based on the related works.

5. Consensus Mechanism

The main role of the blockchain consensus layer is to reach consensus in a decentralized system with highly decentralized decision-making power. The consensus issue is a research hotspot with great academic value for a long time. The core indicators are fault-tolerant proportions and convergence speed. The commonly used consensus mechanism is proof of work (PoW) [45] (refer to Algorithm 1). Each node in the PoW calculates SHA256 of an ever-changing block header. The result of the consensus mechanism is to find a hash value that is less than a certain value. A new block is generated if the new hash value is found. In bitcoin, the node that calculates the hash value is called miner and the process of consensus is called mining. Although PoW can implement decentralization and distributed accounting, PoW heavily relies on nodes' power, which are low throughput and of poor scalability. In fact, the PoW mechanism in bitcoin introduces the game theory without forcing the number of faulty (malicious) nodes. PoW assumes that each node in the network is rational and utilizes economic incentives to maintain the operation within PoW. Recently, researchers propose other consensus mechanisms without relying on computing power, such as the proof-of-stake (PoS) mechanism and the delegated-proof-of-stake (DPoS) mechanism [46].

The basic idea of PoS mechanism is to prove ownership of their stakes. PoS is more reliable than PoW since the more stakes the nodes hold, the less likely they will attack the system. Peercoins, for the first time, achieve a true equity certificate, which is based on the age of the coins, and decide who creates the next block. In DPoS mechanism, the equity owner selects the representative to generate the next block. The above consensus mechanisms are based on the game of economic benefits. The nodes will lose some economic benefits once a malicious node destroys the mechanism. Therefore, most nodes have incentives to maintain the mechanism. Meanwhile, the achievement of consensus must be guaranteed probabilistically after the generation of multiple blocks. In distributed systems, the classical Byzantine algorithm can solve the deterministic problem. Castro and Liskov propose a practical Byzantine fault tolerance (PBFT) [47], which solve the problem of low efficiency of the classic Byzantine fault-tolerant algorithm. More specifically, say there are N nodes in the blockchain network, and the number of Byzantine malicious nodes is $f = ((N - 1)/3)$. Then PBFT can ensure that at least $2f + 1$ nodes reach consensus before adding information to the distributed shared ledger. The advantages of PBFT include the following: (1) it is a complete theoretical proof system, (2) each block is generated by a unique master node, and (3) there are no forks.

However, the complexity of the network is $O(N^2)$, which greatly increases network overhead and reduces system efficiency. Therefore, the performance of the system with PBFT is not high, which is more suitable for a blockchain system with a smaller number of nodes, e.g., consortium blockchain. Currently, Hyperledger Fabric 1.0 is developing a consensus module such as BFT-Smart, simplified Byzantine fault tolerance (SBFT), and HoneyBadgerBFT (refer to Algorithm 2) based on plug-in [48, 49]. In addition, it is also a problem needed to be solved regarding how to support the nodes to dynamically join and quit in the consensus mechanism. Miller et al. study the possibility of the PoW mechanism to solve the problem of single-point Byzantine consistency in the presence of a few Byzantine nodes in an asynchronous network [50]. Garay et al., based on the PoW mechanisms, propose two consensus mechanisms for multiple-instance setting [51]. Their mechanism meets all the properties (a), (b), and (c), but it does not consider the asynchronous network and the problem of participation of honest nodes.

Garay et al. denominate the consensus mechanism as Bitcoin's Backbone protocol (refer to Algorithm 3). They first portray three parameters γ, β, and f. γ and β represent the hashing power of honest participants and adversaries in each round. f represents the PoW value that all participants in the bitcoin network expect to achieve in each round. Some basic properties of the two backbone protocols are proposed. (1) The common prefix property: the blockchain maintained by honest participants will have the largest common prefix when $\gamma > \lambda\beta$, where $\lambda \in [1, \infty)$ and $\lambda^2 - f\lambda + 1 \geq 0$. It requires that most participants be honest in order to satisfy the common prefix characteristics when $f \longrightarrow 0$ and λ tends to be 1. (2) The chain-quality property: the proportion of blocks maintained by any honest participant that are contributed by an honest participant is at least $1 - (1/\lambda)$ when $\gamma > \lambda\beta (\lambda \in [1, \infty))$. For example, when $\lambda \longrightarrow 1$, the block contributed by honest participants is only a minority of the blockchain. Garay et al. prove that if the backbone protocol satisfies the common prefix property and the block quality property, it can meet the two basic properties: agreement and validity of the Byzantine protocol with great probabilities. However, the work [49] does

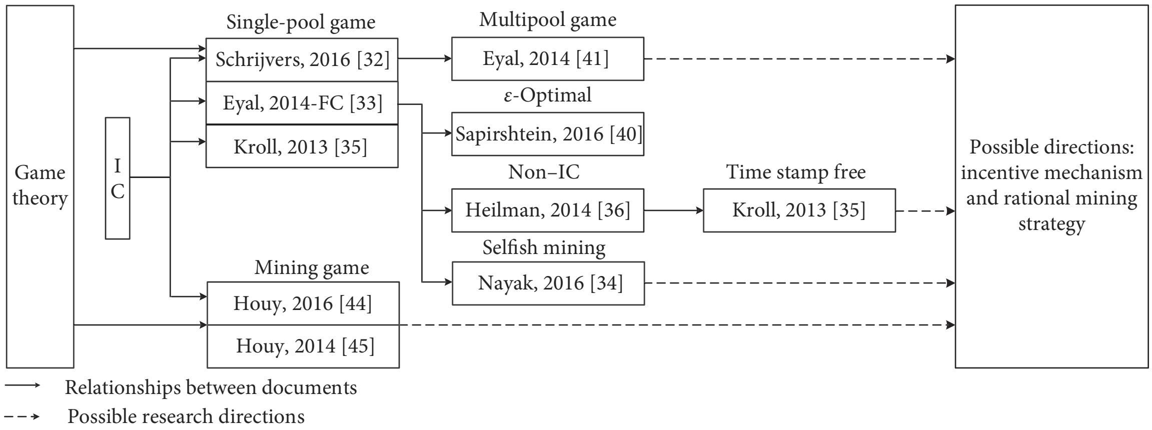

Figure 3: The possible directions for rational mining attacks.

Step 1. The initial voting set V is empty, and each party i has a proposal p_i by solving a hard problem
Step 2. Each party broadcasts p_i and others update their voting set after they verify the validity of the proposal
Step 3. They vote for the proposal p_{most} with the most votes
Step 4. p_{most} is recorded to the blockchain and the one who proposes it wins the rewards

Algorithm 1: The PoW consensus protocol.

Step 1. One proposal $p_i$consisting of $\lfloor B/N \rfloor$ transactions is randomly selected and encrypted to be c_i, where B is the batch size parameter and N is the number of parties
Step 2. Parties agree on these ciphertexts
Step 3. Parties first decrypt c_i if it has passed the verification

Algorithm 2: The HoneyBadgerBFT protocol.

Step 1. Each party i maintains a local chain C and updates it by invoking PoW algorithm (refer to Algorithm 1).
Step 2. However, party i does not update it immediately when C has any change. Instead, i first checks if there are any other "better" chain by verifying its communication tape.
Step 3. An input x is determined by some functions therein and local chain C is updated to be C' by invoking PoW.
Step 4. The updated chain C' is broadcasted to other parties. Note that Backbone consensus protocol is depended on input contribution function $I(\cdot)$ and the chain reading function $R(\cdot)$. Readers may find more details in [51].

Algorithm 3: The Backbone protocol.

not consider the delay in the message delivery process. Before the adversary sends its own information, it can see the information of all honest participants, which will bring privacy issues. Sompolinsky and Zohar propose a longest-chain rule called GHOST [52] in order to reach the consensus of the blockchain. When there is a fork in the blockchain, GHOST selects the subtree with the largest weight at the fork. A variant of GHOST has been adopted by the Ethereum project. However, GHOST does nothing for attacks such as selfish mining. Moreover, [52] only considers limited delays and specific attacks instead of withholding block attacks. Lewenberg et al. improve GHOST [53] to reduce the priority of heavyweight miners and further increase system throughput.

Decker et al. propose PeerCensus [54] to allow nodes dynamically joining and quitting. They implement PeerCensus protocol to Discoin, which achieves strong consistency. Note that Discoin relies not on the blockchain but on the Byzantine protocol. Pass et al. consider the blockchain consensus mechanism in asynchronous networks in a formal model, where new nodes can join the network any time and the adversary can adaptively corrupt the honest nodes [55]. Pass et al. extend the nature of the blockchain consensus protocol: consistency, future self-consistency, g-chain growth, and μ-chain quality. In [52], Sompolinsky and Zohar point out the nature of chain growth, while they only consider the expected growth of the chain. The chain-growth characteristics are also mentioned in one of their documents

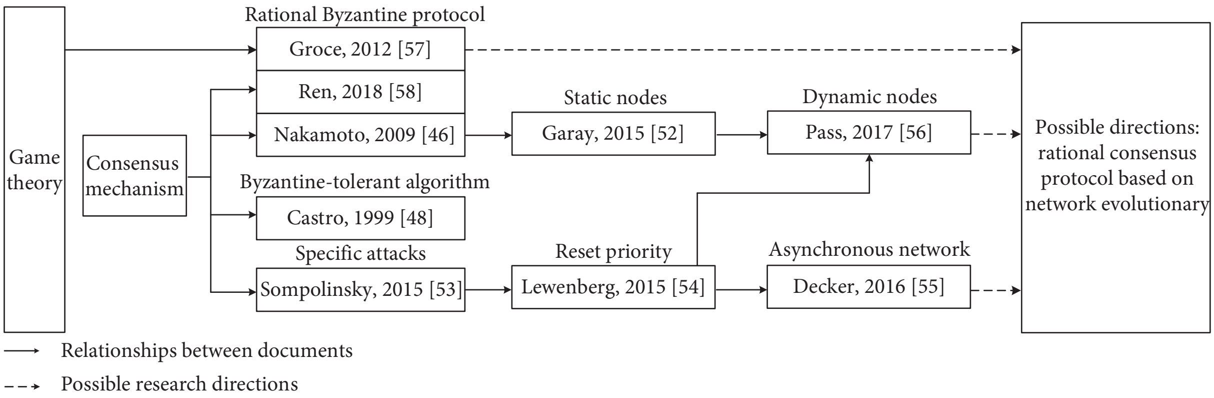

Figure 4: The possible directions for consensus mechanism.

[51]. The nature of chain quality is first proposed and discussed in the Bitcoin forum [32]. To the best of our knowledge, [49] first defines the notion of "chain quality." The study in [55] proves that, given certain conditions, the blockchain consensus protocol satisfies all properties.

Rational behaviours are also implemented in Byzantine agreement protocols. For example, Groce et al. propose a Byzantine agreement based on rational adversaries [56]. They combine game theory and cryptography, assuming that some of the participants in the network are honest and some are rational. Rational participants are controlled by rational adversaries, who try to maximize their rewards by biasing the final outcome. Groce and Katz focus on rational broadcast and Byzantine agreement. They prove that many self-evident conclusions in the classic Byzantine agreement do not establish in a rational adversary environment. For example, a consensus cannot be reached when $t \geq n/2$ and the consensus problem does not stipulate the broadcast problem when $t < n/2$. Finally, they classify the outcomes with respect to rational Byzantine agreement into three categories: (1) agreement on 0, (2) agreement on 1, and (3) inconsistency. Participants have different preferences for outcomes, which depends on the utility function. They highlight the influence of adversary preferences on rational Byzantine agreements: (1) the adversary's preferences are fully known, (2) only the adversary's preference between consistency and inconsistency is known, and (3) it is not known that in consistency, the opponent prefers 0 or 1.

In game theory, these scenarios are called complete information games or incomplete information games. Groce et al. prove that if the traditional Byzantine consistency problem is safe, then the rational adversary strategy in rational Byzantine consistency is the Nash strategy. Ren et al. consider the message type when discussing the Byzantine consensus [57]. They also introduce the concept of rational behaviour. That is, rational issuers of transactions either mine on their own or hire others to mine. Ren et al. define the characteristics of value propagation in the value-transfer ledgers model (VTL model): (1) the rational sender proves the authenticity of the transaction to the recipient, (2) rational recipients should verify the authenticity of the transaction after receiving it, and (3) the authenticity of these transactions is not important if certain transactions have no effect on the transactions that the rational recipient has received. They also prove that if all nodes are rational, then effective transactions in the system can resist double-flower attacks. Figure 4 presents the future directions for consensus mechanism.

6. Future Research Directions

Game theory permeates all levels of blockchain technology, and the behaviours of the entire blockchain rely heavily on the motivation to maintain the blockchain, which is usually an economic incentive. Therefore, it is a hot topic to consider the influence of rational behaviours on key technologies in blockchain technology. At the same time, the blockchain network constructed by the participants has complex network characteristics, and the behaviour of the participants affects the topology of the network, which is closely related to the consensus mechanism. In summary, the future development direction of blockchain technology is mainly concentrated in the following aspects:

(1) The smart contracts automatically run according to the code agreed in advance, which are not affected by the outside world during the execution process. Therefore, it is widely used in various fields in real life. In addition to its own vulnerabilities and external attacks, it becomes a research hotspot to survey on the impacts of the rational behaviours on the effectiveness. Current researches on rational smart contracts focus on the scenario of complete information games. That is, the utility functions are common knowledge. However, there are lots of scenarios with asymmetry information in real life. These asymmetry scenarios result in uncommon knowledge for the utility functions. Therefore, the implementation of incomplete information games in blockchain is one of the future research directions.

(2) The incentive mechanism is one of the core mechanisms of the blockchain technology, which is crucial

to blockchain. At present, game theory is used to discuss the incentive compatibility strategy in single- or multiple-mine pools. So, the miners have enough mining incentives to promote the efficiency of the blockchain. In order to maximize their benefits, rational miners must maintain competition and cooperation with other miners and selectively release the information they have. Therefore, it is one of the future research directions to weigh the information of all parties and reasonably develop the optimal incentive compatibility strategies.

(3) At present, most of the consensus mechanisms based on Byzantine fault-tolerant algorithm assume that there are Byzantine nodes and honest nodes. Most works discuss the proportion of Byzantine nodes and the fault tolerance of consensus mechanism. Some works consider the influence of joining and quitting of nodes under the asynchronous network on the consensus mechanism. Under the assumption that the nodes are rational, the choices of neighbour nodes, when new nodes join the asynchronous network, will also consider the impact on future revenue. Therefore, the phenomenon of small worlds in the process of network evolution is affected by the rational behaviours. Meanwhile, rational Byzantine protocols have certain impacts on information broadcasting and consistency compared to traditional Byzantine protocols. It is one of the future research directions to integrate rational behaviours into network evolution and Byzantine protocols.

Data Availability

The authors claim that all figures are drawn by the tool of Visio. No data were used to support this study.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This study was supported by the Foundation of National Natural Science Foundation of China Grant nos. 62072273, 61962009, 61832012, 61771231, 6150028, 61672321, and 61771289, Major Scientific and Technological Special Project of Guizhou Province (20183001), Foundation of Guizhou Provincial Key Laboratory of Public Big Data (no. 2019BDKFJJ009), Talent Project of Guizhou Big Data Academy, and Guizhou Provincial Key Laboratory of Public Big Data ([2018]01).

References

[1] http://www.360doc.com/content/17/0519/20/30350201655373279.shtml.

[2] https://www.wosign.com/Info/equifax.htm.

[3] http://www.dsj365.cn/front/article/6019.html.

[4] X. Zheng and H. Liu, "A scalable coevolutionary multi-objective particle swarm optimizer," *International Journal of Computational Intelligence Systems*, vol. 3, no. 5, pp. 590–600, 2010.

[5] X. Yu, H. Wang, Zheng, X. Zheng, and Y. Wang, "Effective algorithms for vertical mining probabilistic frequent patterns in uncertain mobile environments," *International Journal of Ad-Hoc Ubiquitious Computing*, vol. 23, no. 3-4, pp. 137–151, 2016.

[6] X. Yu, W. Feng, H. Wang, Q. Chu, and Q. Chen, "An attention mechanism and multi-granularity-based Bi-LSTM model for Chinese Q&A system," *Soft Computing*, vol. 24, no. 8, pp. 5831–5845, 2019.

[7] Y. Tian, Z. Wang, J. Xiong, and J. Ma, "A blockchain-based secure key management scheme with trustworthiness in DWSNs," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 9, pp. 6193–6202, 2020.

[8] X. F. Ding and H. C. Liu, "A new approach for emergency decision-making based on zero-sum game with Pythagorean fuzzy uncertain linguistic variables," *International Journal of Intelligent Systems*, vol. 34, no. 7, pp. 1667–1684, 2019.

[9] R. Ureña, G. Kou, J. Wu, F. Chiclana, and E. Herrera-Viedma, "Dealing with incomplete information in linguistic group decision making by means of interval type-2 fuzzy sets," *International Journal of Intelligent Systems*, vol. 34, no. 6, pp. 1261–1280, 2019.

[10] Y. Wang, M. Zhao, Y. Hu, Y. Gao, and X. Cui, "Secure computation protocols under asymmetric scenarios in enterprise information system," *Enterprise Information Systems*, pp. 1–21, 2019.

[11] Y. Wang, C. Zhao, Q. Xu, Z. Zheng, Z. Chen, and Z. Liu, "Fair secure computation with reputation assumptions in the mobile social networks," *Mobile Information Systems*, vol. 2015, Article ID 637458, 8 pages, 2015.

[12] Y. Ren, Y. Liu, S. Ji, A. K. Sangaiah, and J. Wang, "Incentive mechanism of data storage based on blockchain for wireless sensor networks," *Mobile Information Systems*, vol. 2018, Article ID 6874158, 10 pages, 2018.

[13] Z. Chen, Y. Tian, and C. Peng, "An incentive compatible rational secret sharing scheme using blockchain and smart contract," *SCIENCE CHINA Information Sciences*, Springer, Berlin, Germany, 2020.

[14] M. J. Osborne and A. Rubinstein, *A Course in Game Theory*, MIT Press Books, Cambridge, MA, USA, 1994.

[15] B. V. Ethereum, "A next-generation smart contract and decentralized application platform," 2014, https://github.com/ethereum/wiki/wiki/English-WhitePaper.

[16] L. Luu, D.-H. Chu, H. Olickel, P. Saxena, and A. Hobor, "Making smart contracts smarter," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 254–269, Vienna, Austria, October 2016.

[17] A. E. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: the blockchain model of cryptography and privacy-preserving smart contracts," in *Proceedings of the IEEE Symposium on Security and Privacy*, pp. 839–858, San Jose, CA, USA, May 2016.

[18] K. Bhargavan, A. Delignat-Lavaud, C. Fournet et al., "Formal verification of smart contracts: short paper," in *Proceedings of the 2016 ACM Workshop on Programming Languages and Analysis for Security*, pp. 91–96, Vienna, Austria, October 2016.

[19] N. Atzei, M. Bartoletti, and T. Cimoli, "A survey of attacks on ethereum smart contracts (SoK)," in *Proceedings of the 6th*

International Conference on Principles of Security and Trust, POST 201, pp. 164–186, Uppsala, Sweden, April 2017.

[20] A. Dika, “Ethereum smart contracts: security vulnerabilities and security tools,” Master’s thesis, Norwegian University of Science and Technology, Trondheim, Norway, 2017.

[21] I. Nikolic, A. Kolluri, I. Sergey, P. Saxena, and A. Hobor, “Finding the greedy, prodigal, and suicidal contracts at scale,” in *Proceedings of the 34th Annual Computer Security Applications Conference*, pp. 653–663, San Juan, PR, USA, December 2018.

[22] Y. Velner, J. Teutsch, and L. Luu, “Smart contracts make bitcoin mining pools vulnerable,” in *Proceedings of the FC 2017 International Workshops*, pp. 298–316, Sliema, Malta, April 2017.

[23] A. Juels, A. E. Kosba, and E. Shi, “The ring of gyges: investigating the future of criminal smart contracts,” in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 283–295, Vienna, Austria, October 2016.

[24] L. Brunoni and O. Beaudet-Labrecque, “Smart contracts and cybercrime: a game changer?” *Mathematical Structures and Modeling*, vol. 4, no. 44, 2017.

[25] M. Alharby and A. van Moorsel, “Blockchain-based smart contracts: a systematic mapping study,” 2017, https://arxiv.org/abs/1710.06372.

[26] Y. Wang, A. Bracciali, T. Li, F. Li, X. Cui, and M. Zhao, “Randomness invalidates criminal smart contracts,” *Information Sciences*, vol. 477, pp. 291–301, 2019.

[27] L. Zhang, Y. Wang, F. Li, Y. Hu, and M. H. Au, “A game-theoretic method based on Q-learning to invalidate criminal smart contracts,” *Information Sciences*, vol. 498, pp. 144–153, 2019.

[28] G. Bigi, A. Bracciali, G. Meacci, and E. Tuosto, “Validation of decentralised smart contracts through game theory and formal methods,” *Programming Languages with Applications to Biology and Security*, Springer, Berlin, Germany, pp. 142–161, 2015.

[29] C. Dong, Y. Wang, A. Aldweesh, P. McCorry, and A. van Moorsel, “Betrayal, distrust, and rationality: smart-counter-collusion contracts for verifiable cloud computing,” in *Proceedings of the 2017 ACM SIGSAC Conference on Computer and Communications Security*, pp. 211–227, Dallas, TX, USA, October 2017.

[30] F. Tschorsch and B. Scheuermann, “Bitcoin and beyond: a technical survey on decentralized digital currencies,” *IEEE Communications Surveys & Tutorials*, vol. 18, no. 3, pp. 2084–2123, 2016.

[31] O. Schrijvers, J. Bonneau, D. Boneh, and T. Roughgarden, “Incentive compatibility of bitcoin mining pool reward functions,” in *Proceedings of the FC 2016*, pp. 477–498, Christ church, Barbados, February 2016.

[32] I. Eyal and E. G. Sirer, “Majority is not enough: bitcoin mining is vulnerable,” in *Proceedings of the FC 2014*, pp. 436–454, Christ church, Barbados, March 2014.

[33] K. Nayak, S. Kumar, A. Miller, and E. Shi, “Stubborn mining: generalizing selfish mining and combining with an eclipse attack,” in *Proceedings of the IEEE European Symposium on Security and Privacy*, pp. 305–320, Saarbrücken, Germany, March 2016.

[34] J. A. Kroll, I. C. Davey, and E. W. Felten, “The economics of bitcoin mining, or bitcoin in the presence of adversaries,” *Proceedings of the WEIS*, vol. 2013, pp. 11–32, 2013.

[35] E. Heilman, “One weird trick to stop selfish miners: fresh bitcoins, a solution for the honest miner (poster abstract),” in *Proceedings of the WAHC 2014*, pp. 161-162, Christ Church, Barbados, March 2014.

[36] B. Cohen, “An attack on the timestamp semantics of bitcoin,” 2014.

[37] A. Boverman, “Timejacking & bitcoin,” 2011.

[38] S. Solat and M. Potop-Butucaru, “Zeroblock: preventing selfish mining in bitcoin,” https://arxiv.org/abs/1605.02435v1, 2016.

[39] A. Sapirshtein, Y. Sompolinsky, and A. Zohar, “Optimal selfish mining strategies in bitcoin,” in *Proceedings of the FC 2016*, pp. 515–532, Christ church, Barbados, February 2016.

[40] I. Eyal, “The miner’s dilemma,” in *Proceedinsg of the 2015 IEEE Symposium on Security and Privacy*, pp. 89–103, San Jose, CA, USA, May 2015.

[41] W. Jiang, C. Huang, and X. Deng, “A new probability transformation method based on a correlation coefficient of belief functions,” *International Journal of Intelligent Systems*, vol. 34, no. 6, pp. 1337–1347, 2019.

[42] M. Rosenfeld, “Analysis of bitcoin pooled mining reward systems,” 2011, https://arxiv.org/abs/1112.4980.

[43] N. Houy, “The bitcoin mining game,” *Ledger*, vol. 1, pp. 53–68, 2016.

[44] H. Nicolas, “The economics of bitcoin transaction fees,” *SSRN Electronic Journal*, pp. 1407–1420, 2014.

[45] S. Nakamoto, “Bitcoin: a peer-to-peer electronic cash system,” 2019.

[46] D. Larimer, C. Hoskinson, and S. Larimer, “Bitshares: a peer to-peer polymorphic digital asset exchange,” 2017.

[47] M. Castro and B. Liskov, “Practical byzantine fault tolerance,” in *Proceedings of the Third USENIX Symposium on Operating Systems Design and Implementation (OSDI)*, pp. 173–186, New Orleans, LO, USA, February 1999.

[48] A. N. Bessani, J. Sousa, and E. A. P. Alchieri, “State machine replication for the masses with BFT-SMART,” in *Proceedings of the IEEE/IFIP International Conference on Dependable Systems and Networks*, pp. 355–362, Edinburgh, UK, June 2014.

[49] A. Miller, Y. Xia, K. Croman, E. Shi, and D. Song, “The honey badger of BFT protocols,” in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 31–42, Vienna, Austria, October 2016.

[50] A. Miller and J. J. LaViola Jr., *Anonymous Byzantine Consensus from Moderately-Hard Puzzles: A Model for Bitcoin*, University of Central Florida Tech, Oviedo, FL, USA, 2014.

[51] J. Garay, A. Kiayias, and N. Leonardos, “The bitcoin backbone protocol: analysis and applications,” in *Proceedings of the 34th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 281–310, Sofia, Bulgaria, April 2015.

[52] Y. Sompolinsky and A. Zohar, “Secure high-rate transaction processing in bitcoin,” in *Proceedings of the FC 2015*, pp. 507–527, San Juan, PR, USA, January 2015.

[53] Y. Lewenberg, Y. Sompolinsky, and A. Zohar, “Inclusive block chain protocols,” in *Proceedings of the FC 2015*, pp. 528–547, San Juan, PR, USA, January 2015.

[54] C. Decker, J. Seidel, and R. Wattenhofer, “Bitcoin meets strong consistency,” in *Proceedings of the 17th International Conference on Distributed Computing and Networking*, Singapore, January 2016.

[55] R. Pass, L. Seeman, and A. Shelat, “Analysis of the blockchain protocol in asynchronous networks,” in *Proceedings of the 36th Annual International Conference on the Theory and Applications of Cryptographic Techniques*, pp. 643–673, Paris, France, April 2017.

[56] A. Groce, J. Katz, A. Thiruvengadam, and V. Zikas, “Byzantine agreement with a rational adversary,” in *Proceedings of the ICALP 2012*, pp. 561–572, Warwick, UK, July 2012.

[57] Z. Ren, K. Cong, T. Aerts, B. de Jonge, A. Morais, and Z. Erkin, “A scale-out blockchain for value transfer with spontaneous sharding,” in *Proceedings of the CVCBT 2018*, pp. 1–10, Zug, Switzerland., June 2018.