IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received March 7, 2019, accepted April 1, 2019, date of publication April 9, 2019, date of current version April 19, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2909924

A Survey on Blockchain: A Game Theoretical Perspective

ZIYAO LIU[1], NGUYEN CONG LUONG[1], WENBO WANG[1], (Member, IEEE), DUSIT NIYATO[1], (Fellow, IEEE), PING WANG[2], (Senior Member, IEEE), YING-CHANG LIANG[3], (Fellow, IEEE), AND DONG IN KIM[4], (Fellow, IEEE)

[1]School of Computer Science and Engineering, Nanyang Technological University, Singapore 639798
[2]Department of Electrical Engineering and Computer Science, Lassonde School of Engineering, York University, Toronto, ON M3J 1P3, Canada
[3]Center for Intelligent Networking and Communications (CINC), University of Electronic Science and Technology of China, Chengdu 611731, China
[4]Department of Electrical and Computer Engineering, Sungkyunkwan University, Suwon 16419, South Korea

Corresponding author: Dong In Kim (dikim@skku.ac.kr)

This work was supported in part by the A*STAR-NTU-SUTD Joint Research Grant Call on Artificial Intelligence for the Future of Manufacturing under Grant RGANS1906, in part by the WASP/NTU under Grant M4082187 (4080), in part by the Singapore MOE Tier 1 under Grant 2017-T1-002-007 RG122/17, in part by the Singapore MOE Tier 2 under Grant MOE2014-T2-2-015 ARC4/15, in part by the Singapore NRF2015-NRF-ISF001-2277, in part by the Singapore EMA Energy Resilience under Grant NRF2017EWT-EP003-041, in part by the National Research Foundation of Korea (NRF) Grant funded by the Korean Government (MSIT) under Grant 2017R1A2B2003953, and in part by the National Natural Science Foundation of China under Grant U1801261 and Grant 61631005.

ABSTRACT Over the past decade, blockchain technology has attracted tremendous attention from both academia and industry. The popularity of blockchains was originated from the concept of crypto-currencies to serve as a decentralized and tamper-proof transaction data ledger. Nowadays, blockchains as the key framework in the decentralized public data-ledger have been applied to a wide range of scenarios far beyond crypto-currencies, such as the Internet of Things, healthcare, and insurance. This survey aims to fill the gap between a large number of studies on blockchain networks, where game theory emerges as an analytical tool, and the lack of a comprehensive survey on the game theoretical approaches applied in blockchain-related issues. In this survey, we review the game models proposed to address common issues in the blockchain network. The focus is placed on security issues, e.g., selfish mining, majority attack and denial of service attack, issues regarding mining management, e.g., computational power allocation, reward allocation, and pool selection, as well as issues regarding blockchain economic and energy trading. Additionally, we discuss the advantages and disadvantages of these selected game theoretical models and solutions. Finally, we highlight important challenges and future research directions of applying game theoretical approaches to incentive mechanism design and the combination of blockchain with other technologies.

INDEX TERMS Blockchain, game theory, mining management, security.

I. INTRODUCTION

In the past decade, with the popularity of digital crypto-currencies, e.g., Bitcoin [1], blockchain technology has attracted tremendous attention from both academia and industry [2]. The blockchain was first proposed in [1] to serve as a crypto-currency transaction ledger, and is currently widely adopted for a large number of crypto-currencies, such as Ethereum [3], Ripple [4], and EOS [5]. The blockchain technology guarantees the tamper-proof ledger, transparent transactions, and trustless but secure tradings in a decentralized network. Thus, the blockchain network is recently applied in a wide range of scenarios far beyond crypto-currencies, such as Internet of Things (IoT) [6], healthcare [7] and insurance [8]. In general, blockchain is a distributed public data-ledger maintained by achieving the consensus among a number of nodes in a Peer-to-Peer (P2P) network. More specifically, the verified transaction data is stored in a chain of blocks, i.e., a basic data structure of blockchain, and the chain grows in an append-only manner with all new verified blocks to it. This process involves several operations such as verifying transactions, disseminating blocks, and attaching blocks to the blockchain.

As such, the blockchain requires a number of consensus nodes to participate in the network. The rational nodes perform actions or strategies that aim to maximize their

The associate editor coordinating the review of this manuscript and approving it for publication was Junggab Son.

own utility. Moreover, the malicious nodes may launch attacks that damage the blockchain networks. To address these security challenges, consensus protocols such as Byzantine Fault Tolerance (BFT) protocol [9] can be adopted. However, the consensus protocols require a centralized permission controller and only achieve the consensus among a very small group of nodes. Such a consensus protocol is thus not applicable to the blockchain network that is a decentralized and large-scale system. Different optimization approaches and solutions, e.g., a Markov Decision Process (MDP) [10], are used to analyze and optimize strategies of the blockchain nodes to prevent their misbehaviors. However, the optimization approaches do not take into account the interactions among the nodes. Recently, game theory [11] has been applied as an alternative solution in the blockchain network. Game theory is a study of mathematical models of strategic interaction between rational decision-makers [12]. Thus, game theory can be used to analyze the strategies of the consensus nodes as well as the interactions among them. Through the game theoretical analysis, the nodes can learn and predict mining behaviors[1] of each other, and then choose optimal reaction strategies based on equilibrium analysis. Moreover, game theory can be utilized to develop incentive mechanisms that discourage the nodes from misbehaving or launching attacks. Therefore, game theory is a natural consideration for modeling the decision-making process of all the consensus nodes in the blockchain networks.

Currently, few existing survey on blockchains perceives the organization and applications of blockchains from the game theoretic perspective. In particular, the survey in [13] provides a comprehensive introduction of the Bitcoin network. The surveys in [14]–[16] focus on security and privacy issues in the Bitcoin network. The survey in [17] presents the blockchain applications on Internet of Things (IoT), and the survey in [18] discusses the integrations of blockchain and edge computing. To the best of our knowledge, there is no survey specifically discussing the use of game theory, as an efficient analysis tool, in blockchain networks. This motivates us to deliver the survey with the comprehensive literature review on the game models in the blockchain network. For convenience, the related works in this survey are classified based on a series of sub-issues in the blockchain network. These major issues consist of (i) security issues such as selfish mining attacks and Denial-of-Service (DoS) attacks, (ii) mining management issues such as computational power allocation, fork chain selection, pool selection, and reward allocation, and (iii) applications atop the blockchain such as energy trading.

The rest of this paper is organized as follows. Section II briefly describes the general architecture of blockchains. Section III presents the fundamentals of game theory and game models that are commonly used for analyzing/designing blockchains. Section IV discusses applications of game theory for security issues in blockchains. Section V presents applications of game theory for the mining management in blockchains. Section VI discusses applications of game theory atop blockchain platforms. Section VII outlines challenges and future research directions. Section VIII summarizes and concludes the paper.

[1] In blockchain systems where incentive nodes participate in the consensus process of data record with digital tokens, the consensus nodes are frequently referred as block miners, and their operations are referred as mining.

II. OVERVIEW AND FUNDAMENTALS OF BLOCKCHAIN

In this section, we give an overview of the blockchain on its concepts, data organization, working mechanism, and incentive compatibility.

A. OVERVIEW OF BLOCKCHAIN

The blockchain was first proposed as a decentralized tamper-proof ledger which records an ordered set of transactions. These transactions are verified through a decentralized consensus process among the trustless agents before attaching to the chain. Here, we summarize the key advantages that blockchain networks can offer as follows:

- Decentralized network: The decentralized blockchain network allows every computing unit (i.e., node) to utilize its computational power to participate in the blockchain consensus process. Each transaction on the blockchain must be confirmed upon the agreement among the majority of the nodes through the consensus protocol. Therefore, the monopoly in centralized network can be removed in the blockchain network.
- Tamper-proof ledger: The cryptographic techniques used in blockchain ensure that any change on the transaction data in blockchain can be observed by all the nodes in the network. This means that the transaction recorded in the blockchain cannot be altered and tampered, unless the majority of nodes are compromised.
- Transparent transaction: All the transactions in the blockchain can be traced back for verification, and these transactions are transparent to all the nodes in the blockchain network.
- Trustless but secure trading: By using the digital signature based asymmetric keys, the blockchain network guarantees that only the sender and receiver of the transactional data, which possess the pair of asymmetric key can execute the transaction, without intervention of any trusted third-party.

B. DATA ORGANIZATION AND WORKFLOW OF BLOCKCHAIN

Cryptographic data organization plays an extremely important role in the blockchain structure. We first introduce some basic components supporting the data organization within blockchain networks.

- Transaction: Transactions are the most basic component of blockchains. A transaction is proposed by the blockchain users. It is composed of the transactional data which specifies the value in concern, e.g., the digital

tokens in a crypto-currency, the addresses of the sender and the receiver, as well as the corresponding transaction fee [1].
- Block: A block is composed of a block header and a certain amount of transactions. The block header specifies the hash pointer and Merkle tree data structure.
- Hash pointer [13]: The hash pointer of the current block contains the hash value of the previous block, which also contains the hash pointer to the block before that one. Thereby, the hash pointers can be used to build a chain of records, i.e., blockchain.
- Merkle Tree [19]: A Merkle tree or hash tree is a tree in which each leaf node is marked by the hash value of the transaction data of a block, and those non-leaf nodes are marked by the hash value of the concatenation of its child nodes. This structure makes it impossible for a node to tamper the data in a block without being noticed.

As shown in Fig. 1, a typical blockchain is an appending-only, ever-growing chain of blocks, which are linked sequentially using the hash pointers as a linear linked list. More specifically, the block header includes a hash pointer which is associated with the previous block, and the transactions are organized as Merkle trees.

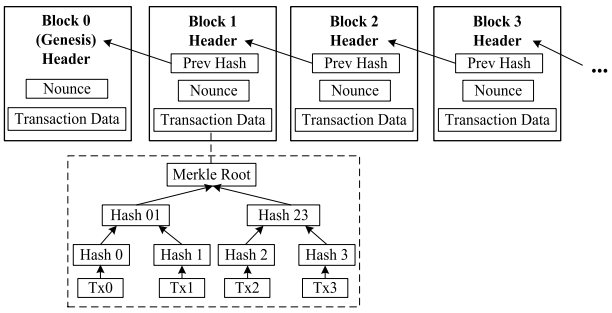


FIGURE 1. An illustrative example of blockchain data structure where the transactions are included in the block and the block is represented by a Merkle root.

Atop the basic cryptographic data organization, maintaining the blockchain network needs nodes in the blockchain network to disseminate the transactions, store the data into blocks, verify the transactions, and eventually reach a consensus about the order of them. The blockchain maintenance mechanism works as follows (see Fig. 2):

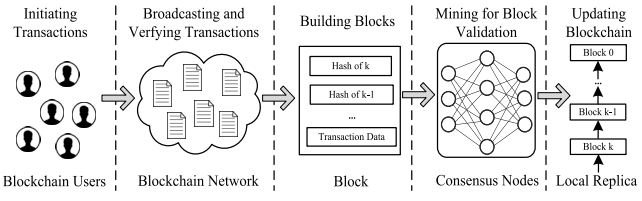


FIGURE 2. An overview of the blockchain workflow.

- An newly initiated transaction is broadcast to the network by its sender.
- The nodes in the blockchain verify the transaction value as well as the identity of the node which initiates the transaction.
- More than one node may bundle different subset of newly verified transactions into their candidate blocks and broadcast them to the entire network.
- All or part of the nodes in the blockchain network participate in the block validation by executing some certain functions defined by the consensus protocol.
- The verified block is attached to the blockchain, and every node updates its local replica, i.e., the local views of whole ledger-data, of the blockchain.

In general, not all the nodes can be authenticated to join the blockchain network to execute the consensus protocol. According to the access control scheme [20] that determines which node can join the network, the blockchain platforms are classified into permissionless schemes, i.e., public blockchains, and permissioned schemes including private and consortium blockchains. When choosing the permissioned access control scheme, e.g., Hyperledger fabric [21], the consensus needs to be reached among only a small group of authenticated nodes, and thus the permissioned blockchain network usually adopts conventional BFT protocols, e.g., Byzantine Paxos [22]. On the contrary, in permissionless blockchain, e.g., Ethereum [3], any node can participate in the network consensus process, and some other consensus protocols are applied, such as Proof of Work (PoW) and Proof of Stake (PoS). We list some widely-used blockchain platforms and their consensus protocols in Table 1.

TABLE 1. Examples of widely-used blockchain platforms.

Platform Name	Ledger type	Consensus Protocol
Bitcoin [1]	Public	Proof of Work (PoW)
Ethereum [3]	Public	PoW & Proof of Stake
Hyperledger Fabric [21]	Consortium	Pluggable algorithm
EOS [5]	Private	Delegated Proof of Stake
Stellar [23]	Public & Private	Stellar consensus protocol
Quorum [24]	Private	Majority voting
Ripple [4]	Private	Probabilistic voting

C. INCENTIVE COMPATIBILITY WITHIN BLOCKCHAIN

In a blockchain network, the consensus protocol guarantees achieving the consensus among the nodes. A reliable consensus protocol needs to satisfy the following properties [25]. (i) Correctness: each node adopts the content and the order of transactions in the confirmed canonical blockchain structure. (ii) Consistency: each node updates its local blockchain structure if a new block header is confirmed. (iii) Traceability: all transactions can be traced back to the genesis block for confirmation. However, in some case, disagreements may exist among the nodes. For example, the local blockchain replica of all the nodes are unable to be synchronized simultaneously due to the delay in a distributed network. In this case, the nodes might maintain different blockchain ledgers, and thereby the fork chains appear. This means that the nodes may

deviate from the protocol of maintaining the longest chain.[2] Therefore, the blockchain consensus protocol is expected to be *incentive compatible* [25] This means that any node will suffer from financial loss, e.g., waste of investment in computing power, whenever the node deviates from the protocol.

Currently, the most popular blockchain consensus protocol is the PoW-based Nakamoto consensus protocol [1]. The Nakamoto protocol achieves the consensus by requiring nodes to solve a mathematical puzzle, i.e., to find a hash value which satisfies a certain pre-image condition. The first node that solves the puzzle can broadcast the verified block to the blockchain network, and obtains the reward and the transaction fee. This process of solving puzzle and obtaining the reward is called mining. The design of the mining mechanism relies on both cryptography [26] and game theory [12].

Although the PoW protocol is widely used among the blockchain platforms, the incentive compatibility of the protocol has been openly questioned from game theoretical perspectives [27]. The reason is that achieving the Nakamoto consensus involves nodes joining the network, executing the protocol, and maintaining the ledger. The nodes may deviate from the protocol to increase their own utilities. For example, the node may not broadcast its newly discovered blocks but choose to withhold the block to increase its utility [25]. The node trades off between the cost of withholding the block which is associated with the other nodes' strategies, and the mining reward and then chooses its strategy. To analyze the interactions among these consensus nodes, the game theoretical models (see Section III) are developed and applied [28]. In addition to the security issues, nodes' mining-strategy management, e.g., computational power allocation [29] and reward allocation [30], adopt game models for the analysis as well. Apart from the Nakamoto protocol, game models are also widely used for analyzing the incentive compatibility with other consensus protocols, e.g., PoS protocol [31]. Therefore, to better understand the applications of game theory in blockchain, the next section presents an overview on fundamentals of the game models used in this survey.

III. OVERVIEW AND FUNDAMENTALS OF GAME THEORY

Game theory provides a set of mathematical tools for analyzing the interaction among rational decision-makers. In a game, each decision-maker as a player chooses its strategy to maximize its utility, given the other players' strategies. The following briefly presents the game theoretic approaches which have been widely applied to analyze the interactions within the blockchain network. To explain the concept of a game, some important terminologies are given below.

- Player: A player is a decision-maker in the game. In the blockchain, players can be miners, mining pools, or the blockchain users.
- Utility: A utility, i.e., a payoff, an interest, or a revenue reflects the player's expected outcome.
- Strategy: A player's strategy is a set of actions, choices or decisions that the player can perform to achieve its expected outcome. In general, the player's utility is determined based on not only the player's own strategy, but also the other players' strategies.
- Rationality: A player is rational, i.e., self-interested, if the player always maximizes its own payoff.

A. NON-COOPERATIVE GAME

In a non-cooperative game, the players do not cooperate by forming coalitions or by reaching agreements. In general, the term *non-cooperative* does not imply that the players do not cooperate with each other. It means that any cooperation which might arise must be with no communication of strategies among the players. In other words, the strategy that a player takes must be spontaneous, and each player is rational.

Consider a blockchain network in which miners as the players invest strategically in computational power to compete for a reward from mining successfully. The miners are rational and the non-cooperative game can be used to model the interaction among the miners. Assume that there are N miners, i.e., players, and P_i is a set of strategies of miner i, where $P = P_1 \times \cdots \times P_N$ is the Cartesian product of the sets of individual strategies. Let $p_i \in P_i$ be the strategy of miner i. A vector of strategies of N miner can be defined as $\mathbf{p} = (p_1, \ldots, p_N)$, and a vector of corresponding payoffs can be defined by $\boldsymbol{\pi} = (\pi_1(\mathbf{p}), \ldots, \pi_N(\mathbf{p})) \in R^N$, where $\pi_i(\mathbf{p})$ is the utility of player i, e.g., mining rewards or the transaction fees, given the miner's chosen strategy and strategies of the others. Each miner chooses its best strategy p_i^* to maximize its utility. A set of strategies $\mathbf{p}^* = (p_1^*, \ldots, p_N^*) \in P$ is the Nash equilibrium if no miner can gain higher utility by changing its own strategy when the strategies of the other miners remain unchanged, i.e.,

$$\forall i, p_i \in P_i : \pi_i(p_i^*, \overline{\mathbf{p}}_\mathbf{i}^*) \geq \pi_i(p_i, \overline{\mathbf{p}}_\mathbf{i}^*), \tag{1}$$

where $\overline{\mathbf{p}}_\mathbf{i} = (p_1, \ldots, p_{i-1}, p_{i+1}, \ldots, p_N)$ is a vector of strategy of all miners except miner i.

The inequality in (1) demonstrates the equilibrium state of the game. At the Nash equilibrium, the players have no incentive to deviate from their current strategies. However, there may exist no Nash equilibrium in some cases, or multiple equilibria in other cases. Thus, it is important to check the existence and uniqueness of the Nash equilibrium to analyze a non-cooperative game. The existence and uniqueness of equilibrium theory [32] demonstrates that the strictly concave game can achieve the unique equilibrium asymptotically. Here, the concave game means that the utility functions of players are concave, and this can be proved by computing the second-order derivative of the utility function [12].

The non-cooperative theory can be applied to a broad range of blockchain based scenarios. For example, it can be used for computational power allocation [29] or fork chain selection [33]. Also, it can be used for pool selection

[2] Due to the different strategies that nodes make to maximize their own utilities, the nodes may attach newly verified blocks to different blocks in their local view of blockchain, and thereby fork chains appear. The consensus protocols regulate the nodes to apply their work on the longest chain.

regarding the mining rewards allocation [30]. Atop the blockchain based platform, the non-cooperative game theory is applied to analyze the interaction between blockchain users and miners, e.g., cheating among the buyers and sellers in blockchain network [34]. Moreover, it is widely adopted in analysis of security issues within the blockchain, e.g., pool block withholding attacks [35].

B. EXTENSIVE-FORM GAME

The aforementioned non-cooperative games typically include the static game, i.e., the game that has no notion of time and where no player has any knowledge of other players' actions in advance. They also include the dynamic game, i.e., the game in which the players' strategies are made following a certain predefined order. The dynamic game can be represented in an extensive form to illustrate the sequencing of players' possible moves, their choices at every decision point, information that each player has about the other players' moves, and their payoffs for all possible game outcomes. In game theory, the extensive-form game describes the interaction among the players using a game tree illustrating decisions made at different points with their payoffs represented at the end of each branch. Consider the scenario of fork chain selection, the miner chooses a certain chain to mine on at the beginning of every round of mining competition, given the actions taken by the other players in previous mining rounds. At some time instance, the blockchain forks and leads to the structure similar to a branching tree. Thus, the tree-like extensive-form game can be efficiently applied for the analysis as shown in Fig. 3, where the players can choose between two chains to mine.

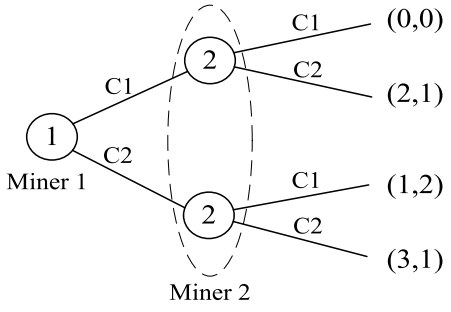


FIGURE 3. The game has two players, i.e., miner 1 and miner 2. The initial node belongs to miner 1 meaning that the miner 1 makes its strategy first. The miner 1 chooses between Chain 1, i.e., C1, and Chain 2, i.e., C2. The miner 2 chooses between C1 and C2 after its observation of the action of miner 1. There are four payoffs represented by the four terminal nodes of the game tree: (C1,C1), (C1,C2), (C2,C1) and (C2,C2).

Assume that an extensive-form game is composed of many smaller games, i.e., subgames. Each subgame can be expressed as a static non-cooperative game. A set of strategies $\mathbf{p}^* = (p_1^*, \ldots, p_N^*) \in P$ is a subgame perfect equilibrium if it represents a Nash equilibrium of every subgame. A common method for obtaining the subgame perfect equilibrium in an extensive-form game is backward induction. The backward induction first considers the decision that might be made in the last move and then reasons back from the end of the problem to the previous one until the induction reaches the first move of the game. In the game as presented in Fig. 3, if miner 1 chooses C2, miner 2 will choose C1 to maximize its utility and miner 1 receives 1. If miner 1 chooses C1, miner 2 will choose C2 and miner 1 receives 2. Therefore, miner 1 prefers choosing C1 and miner 2 choosing C2. The strategies of miners are the Nash equilibrium of each subgame and thus achieve the subgame perfect equilibrium.

In blockchain-based platforms, the extensive-form game is applied for determining whether to enter the blockchain market or not [36], which transactions to be included in the block [37], and the optimal allocation of mining pools' rewards [38]. The extensive-form game has been also adopted for analyzing the security issues within the blockchain. It was used to analyze the selection of fork chain [39], determination of forming the collusion [40], and cheating among the blockchain users [41].

C. STACKELBERG GAME

Similar to the extensive-form game, another game that involves in a certain predefined ordered strategies by players is the *Stackelberg game* [12]. In the Stakelberg game, the players are divided into the *leaders* and the *followers*. The followers decide their strategies after observing the strategies of the leaders. Both the leaders and the followers are typically rational and aim to maximize their own utilities.

To understand how the Stackelberg game works, we consider a blockchain relying on edge computing network, which involves two players, i.e., the service provider and the miner [42]. The service provider possesses the computational power which can be offered to the miner as service, and the provider can set the service price to charge the fee for profit. The miner optimizes its demand of computational power to the provider to maximize its utility, taking its cost into account. As such, the service provider sets the price first, and then the miner decides its demand. Thus, the Stackelberg game can be used to model the interaction between the service provider and the miner. Assume P_1 and P_2 are the sets of strategies of the service provider and the miner, respectively. The service provider chooses its strategy p_1 from set P_1 to maximize its utility $\pi_1(p_1, p_2)$, and the miner chooses its strategy p_2 from set P_2 to maximize its utility $\pi_2(p_1, p_2)$. The optimization problems of the leader and the follower together form the Stackelberg game. The objective of analyzing such a game is to find a Stackelberg equilibrium.

Definition 1: Let $\mathrm{BR}_2(p_1)$ define the best response mapping of the follower. Then, the point (p_1^*, p_2^*) is called the Stackelberg equilibrium of the game if the following conditions hold:

- $p_2^* \in \mathrm{BR}_2(p_1^*)$, and
- $p_1^* \in \arg\max_{p_1} \max_{p_2 \in \mathrm{BR}_2(p_1)} \pi(p_1, p_2)$.

To find the Stackelberg equilibrium, the backward induction method is typically used. Since the leader first takes its strategy and then the follower chooses its strategy, the Stackelberg strategy guarantees the service provider to achieve its payoff at least as much as the corresponding Nash equilibrium. The reason is that when choosing the Stackelberg strategy, the service provider actually optimizes its decision which will maximize its utility. This feature makes the Stackelberg game suitable for many scenarios in blockchain based applications. For example, the Stackelberg game is adopted for setting transaction fees and selection of miners for verification [43], determination of cyber-insurance price [44], and analyzing the supply-demand relationship in the blockchain based edge computing platform [45].

D. STOCHASTIC GAME

A stochastic game can be seen as several static non-cooperative games that are repeated over time. Each static non-cooperative game is called a *state* of the game. The stochastic game executes *stochastic transitions* among the states of the game. In the stochastic game, the players can change their strategies based on the past actions and transitions behaviors of the other players [46].

The stochastic game can be applied efficiently to analyze the miners' selection of chains to mine (see Section II) regarding the transitions of blockchain states. The stochastic game is typically composed of (i) a finite set I of players, e.g., the miners, (ii) a space M of states, e.g., blockchain data structures, (iii) a strategy set S of the players, and (iv) a state transition map P from $M \times S$ to M. Each miner has a payoff function g_n, which is often defined as the discounted sum of the stage payoffs. The game starts at an initial state m_1, and at stage t, each miner observes the blockchain structure m_t and then chooses its strategy s_t^i, i.e., selects a chain to mine. Every miner receives an immediate payoff g_n^i associated with the current state and the miners' strategies. Then, the game moves to a new state m_{t+1}. The game process is repeated until it reaches a common solution called Markov Perfect Equilibrium (MPE) [47] that is the refinement of the subgame perfect equilibrium (see Section III-B). The Markov perfect equilibrium is a set of strategies that achieve the Nash equilibrium of every state of the stochastic game [12]. In the case of fork chain selection, following the Nakamoto protocol, i.e., mining on the longest chain, is the Markov equilibrium.

Apart from the chain selection, the stochastic game can be used for deriving other mining strategies. Examples of such strategy derivation include the selection between investing in computational power or stopping mining [48], and the selection of new blocks to mine upon [49]. Furthermore, the stochastic game has also been widely applied to security issues. It was used to analyze the selection between honest mining and selfish mining [50], the decision of the proper time to release the mined block [28], and the selection of adding a block to the main chain [51].

IV. APPLICATIONS OF GAME THEORY FOR SECURITY

A. SELFISH MINING ATTACK

Selfish mining is a type of subversive strategies in PoW based blockchain systems [52] where attackers, i.e., malicious miners or mining pools, may not broadcast the newly mined blocks but choose to (i) withhold the block or (ii) hold and then release the block at a proper time. In this case, honest miners waste their computational power in finding the block already discovered by other miners, and malicious miners can thereby increase their probability of finding the next block. The Pool Block WithHolding (PBWH) attack is one recently identified selfish mining attack [53]. In the PBWH attack, the attacking pool infiltrates the attacked pool, and the infiltrating miners perform the Block WithHolding (BWH) attack, i.e., to withhold all the blocks newly discovered in the attacked pool. To prevent such an attack, it is crucial to analyze strategies of the miners and pools as well as the interaction among them. A Markov Decision Process (MDP) [54] can be used to analyze the strategy and utility of the individual player, i.e., the miner or the pool. However, the MDP model does not take into account the interaction among multiple players. Alternatively, game theory can be effectively applied.

The authors in [35] adopt a non-cooperative game to analyze the interaction among the pools. This scenario is illustrated in Fig. 4 with two selfish pools as players. The strategy of each player is to determine its infiltration rate, i.e., the fraction of its computational power for performing the infiltration. In the case of attack, the attacking pool obtains its utility not only from its honest miners, but also from the infiltrating miners that perform the BWH attack within the attacked pool. The objective of the player is to optimize its infiltration rate and thereby maximize its utility. In particular, the player's utility is a function of the computational power and the infiltration rate. By using the second-order derivative with respect to the infiltration rate, the utility function is proved to be concave. Thus, there exists a unique Nash equilibrium in which neither players can improve its own utility by changing its strategy of infiltrate rate. At the equilibrium, the infiltrate rate is always greater than zero. This means that launching the PBWH attack is always the best response of each player. Simulation results illustrate that a pool can improve its utility by launching the PBWH attack only when it controls a strict majority of the total computational power. However, in the case that two pools attack each other, the utility of each pool is less than that if neither pool attacks.

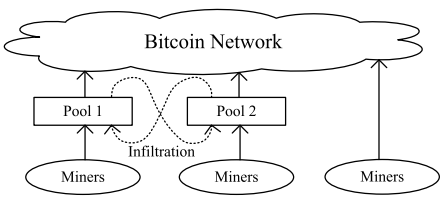


FIGURE 4. A case of two pools where both pools launch the PBWH attack, i.e., by infiltrating the other pool with its miners that perform the BWH attack [35].

TABLE 2. A summary of game theoretical applications for security.

	Ref.	Game Model	Player	Action	Strategy	Payoff	Solution
Selfish Mining Attack	[35]	Non-cooperative game	Mining pools	Infiltrate other pools to launch BWH attack	Determination of the infiltration rate	Mining rewards minus cost	Nash equilibrium
	[55]	Splitting game	One miner and pools	Distribute mining power for selfish mining	Determination of the power distribution	Mining rewards minus cost	Mixed strategy Nash equilibrium
	[56]	Mean-payoff game	Mining pools	Migrate to other pools to launch PBWH attack	Determination of the migration rate	Mean-payoff	Mean-payoff objective
	[50]	Stochastic game	Miners	Block withholding (BWH) attack	Selection between honest mining and selfish mining	Social welfare	Zero-Determinant strategy
	[57]	Non-cooperative game	Miners	Selfish propagation attack	Selection of identity duplication and transactions relaying	Mining rewards	Nash equilibrium
	[33]	Non-cooperative game	Miners	Fork chain	Selection of fork to mine	Transaction fees	Nash equilibrium
	[58]	Non-cooperative game	Miners	Delay submitting shares	Decision of the proper time to submit shares	Mining rewards	Nash equilibrium
	[28]	Non-cooperative game	Miners	Select or create a chain to mine	Selection of the chain to mine	Mining rewards	Nash equilibrium
majority Attack	[28]	Stochastic game	Miners	BWH attack	Decision of the proper time to release the block	Mining rewards	Nash equilibrium
	[59]	Non-cooperative game	Miners	Post smart contract transaction of mining on private chain	Selection between working on smart contract transaction and honestly mining	Transaction fees and mining rewards	Nash equilibrium
	[51]	Stochastic game	Miners	Compete to fork chain	Selection of adding the block to the chain	Mining rewards minus cost	Nash equilibrium
	[60]	Non-cooperative game	Attacking and defending miners	Issue whale transaction to attract miners mine on the private chain	Determination of the threshold of attack cost and block selection	Mining reward minus cost	Nash equilibrium
	[61]	Sequential game	Attacking and defending miners	Buy stake to launch majority attack	Determine the cost of attack and selling selection	Function of profit and interest	Nash equilibrium
	[28]	Non-cooperative game	Attacking and defending miners	Goldfinger attack	Decision of forming cartel and determination of the tax paid to the attacker	Profits minus cost	Nash equilibrium
	[43]	Stackelberg game	Blockchain users and miners	Form cartel to launch majority attack	Setting transaction fee and selection of recruiting miners	Profits minus cost	Stackelberg equilibrium
DoS Attack	[62]	Non-cooperative game	Mining pools	DDoS attack	Selection of launching attack or not	Profits minus cost	Nash equilibrium
	[63]	Sequential game	Mining pools	DDoS attack	Choice of the attack level	Profits minus cost	Nash equilibrium
	[64]	Repeated game	Mining pools	DDoS attack under a reputation-based scheme	Selection of launching attack or not	Profits associate with the loss of reputation	Nash equilibrium
	[65]	Non-cooperative game	One server and devices	DDoS attack in edge network	Selection between executing or sending request and launching attack	Profits minus cost	Nash equilibrium
Other security issues	[66]	Non-cooperative game	Groups of information sharing network	Form group and infiltrate other groups to withhold data	Determination of infiltration rate	Profits minus cost	Nash equilibrium
	[40]	Extensive-form game	Clouds of cloud computing network	Collude to output the same wrong data	Selection of collusion or not	Function of payment and deposit	Sequential equilibrium
	[41]	Extensive-form game	Buyer and seller of the blockchain trading system	Cheats of buyer or seller	Selection of cheating or not	Profits associated with deposits	Subgame perfect Nash equilibrium
	[34]	Non-cooperative game	Buyer and seller of the blockchain trading system	Cheats of buyer or seller	Selection of cheating or not	Profits associated with deposits	Nash equilibrium
	[67]	Coordination game	Voter and verifiers	Manipulate data of data verification system	Statement of the correctness of data	Profits associated with deposits	Nash equilibrium
	[44]	Stackelberg game	Blockchain users, one provider and one insurer	Purchase insurance to compensate for the attack	Determination of the service price, service demand and insurance price	Profits minus cost	Stackelberg equilibrium

The case in [35] is similar to the famous prisoners' dilemma in game theory [12] that results in the utility loss of the miners. To avoid the miners' dilemma, the miners can choose one of the solutions as follows. The first solution is to allow the miners to join private pools that will not involve the PWH attack. As a result, big mining pools may be divided into many small pools spontaneously, and eventually this may lead to a better environment for the Bitcoin system as a whole. The second solution is that the miners perform so-called Zero Determinant (ZD) strategies [68]. This solution is presented in [50], where the authors model a two-miner mining case as a stochastic iterative game.

Different from a typical strategy that aims to improve players' own profits, the ZD strategy is used to control an outcome of the opponents in a certain range so as to avoid a low social welfare, i.e., the whole pool's profit [69]. In this game, the two players are an altruistic miner, i.e., a miner which attempts to maximize the social welfare, and a selfish miner, i.e., a miner which only aims to improve its own profit. Their strategies include cooperation, i.e., mining honestly, and launching the BWH attack to the other miner. Note that the altruistic miner and selfish miner choose their strategies probabilistically based on each other's strategy selected in the last iteration. The analysis shows that so long as the altruistic miner applies strategies according to the determinant function, i.e., a linear function which is associated with players' profit factor, the profit of the selfish miner is in a range from mutual cooperation to mutual attack regardless of strategies adopted by the selfish miner. Thus, the altruistic miner can indeed motivate the selfish miner to mine cooperatively by performing ZD strategies so as to restrict the selfish miner's profit to achieve the highest social welfare. The simulation results show that the proposed game can achieve a higher social welfare than that of the pool game proposed in [35]. However, the proposed game does not consider the profit of the altruistic miner. This means that the altruistic miner may not have an incentive to perform the ZD strategy.

The two-pool-attacker scenario in [50] can also be found in [56]. In addition to the PBWH attack, the authors in [56] consider the miners' migration among the pools. In particular, the miners of a pool can be migrated to another pool and launch the PBWH attack to increase the profit. To analyze the average payoff of the miner in the miners' stochastic migration process, the Concurrent Mean-payoff Game (CMPG) is adopted in [56]. CMPG (see Section III) is a two-player game with a finite state space where at each state, both players choose their strategies simultaneously [46]. Here, the players are pool 1 and pool 2, and the state of the game includes the number of migrated miners of pool 1 and that of pool 2. The strategy of a pool is to determine (i) the number of its miners to be migrated to the other pool and (ii) the miners which perform the PBWH attack. The number of migrated miners is determined according to the attractiveness levels of the other pool, i.e., the ratio of the pool's total mining reward to the total computational power of its miners. If a pool is infiltrated by miners of the other pool, the attractiveness level of the pool decreases. This decrease can be observed by the whole blockchain network, and thus the other pool can adjust its migration strategy based on the observations. In general, the pool's profit depends not only on the state, i.e., the allocation of miners for migration, but also on its chosen strategy. The experimental results show that if the miners in pool 1 stochastically migrate to pool 2 according to the pool 2's attractiveness level, then the mean-payoff objective, i.e., the average profit, of pool 2 can be guaranteed against any strategy of pool 1. However, the mean-payoff objective may not be guaranteed in multi-player scenarios. Such a scenario can be investigated in the future work.

The aforementioned approaches, i.e., [35], [50], [56], are constrained to the interaction among only two pools. Considering a multi-pool scenario, the authors in [55] adopt the Computational Power Splitting (CPS) game [70] to model the PBWH attack. To improve their expected payoffs, the players, i.e., the miners or the pools which own positive computational power, can choose to (i) attack other pools, i.e., to distribute their computational power to other pools and launch the BWH attack, and (ii) honestly follow or arbitrarily deviate from the pool's protocol. In the case that the player chooses to attack, the strategy of the player is to determine (i) the distribution of its computational power, and (ii) the portion of its mining power holding attack as presented in Fig. 5. The objective is to maximize the player's profit, which is defined as the sum of mining rewards received from all the pools. For any given strategies of the other miners, there always exists a computational power allocation for a miner to increase its profit and cause the other pool a loss. In other words, honestly mining is not the best response of the players and the game thus has no pure Nash Equilibrium strategy. Nonetheless, the game has a unique mixed strategy equilibrium at which each player has an incentive to launch the PBWH attack probabilistically rather than mining honestly. Simulation results show that the best strategy of the players is to comply with the following rules. First, the players launch the PBWH attack which improves their profits. Second, the attackers spend the computational power less than a specific fraction on the PBWH attack to gain more profit than mining honestly. Finally, the attackers should attack big pools rather than small pools. Both studies in [35], [55] arrive at some consistent findings from different perspective.

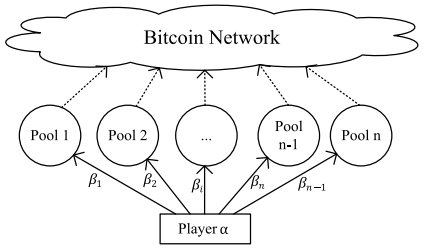


FIGURE 5. The player α distributes its computational power to several pools and launchs the BWH attack, where α is the computational power owned by the player, and β_i represents the fraction of mining power that the player allocates to the pool i [55].

The approaches discussed above, i.e., [35], [55], consider only the mining reward. In practice, the Bitcoin systems also provide the transaction fee [1]. When the block creation reward dominates the mining reward, the miners may not broadcast transactions to the others immediately so as to increase their expected profits [71]. This is called *selfish propagation attack*. To address the attack, the authors in [57] propose an incentive mechanism for the miners to propagate the transactions. The proposed mechanism is designed such that each miner receives a propagation reward from the blockchain system according to its behaviors in the propagation process (see Section II-B). To maximize the gained propagation reward, each miner strategically chooses to duplicate itself, i.e., to add fake identities before relaying the transaction, or to relay the transaction immediately, given the strategy profile of the other miners. The interaction among the miners can be modeled as a non-cooperative game as presented in [57]. In the game, the players are miners which are aware of the transaction. Each player not only strategically relays the transaction but also works on PoW. The authorizing player, i.e., the player which solves the PoW, and the players which are in the same relay chain with the authorizing player gain a certain reward. Other players gain nothing. This scenario is illustrated in Fig. 6. By using the iterative removal of dominated strategies [12], the game is proved to admit a unique Nash equilibrium. At the Nash equilibrium, only the transaction propagating strategy and the non-duplication strategy, i.e., the Nash equilibrium strategy, survive after dominated strategy removal. However, if there are not sufficient number of players which are connected with each other, the selfish propagation attack cannot be guaranteed to be prevented.

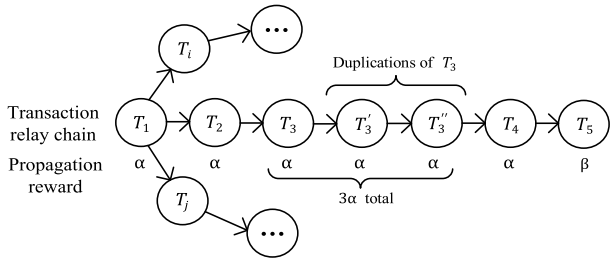


FIGURE 6. An example of the transaction relay process that the transaction flows from T_1 to T_5. T_1 to T_4 relay the transaction thus gain reward α. T_5 solves the PoW thus gains reward β. T_3 adds two fake identities, i.e., T_3' and T_3'', before relaying the transaction thereby gains 3α in total [57].

Other works on understanding the vulnerability of propagation mechanism without mining rewards can also be found in [28], [72], [73]. The authors in [33] demonstrate that with only block creation rewards, it is attractive enough for miners to extend the blocks that have the most available transaction fees rather than to follow the longest chain. Each miner intends to fork the head of the chain actively and leaves transactions unclaimed selectively to maximize its profit. Such an attack is called *undercutting attack*, and the miner

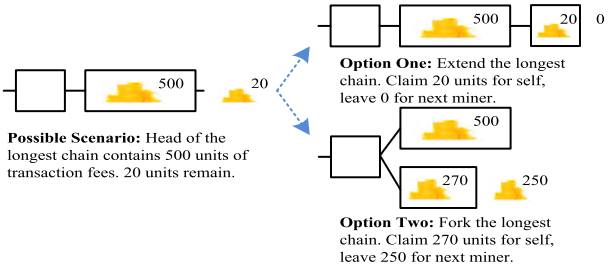


FIGURE 7. An example of undercutting attacks. Option one corresponds to honest mining that the miner mines on the longest chain. The miner in Option Two performs the undercutting attack that forks the longest chain and claims more reward compared with that of option one [33].

that performs the undercutting attack is called *undercutter*. The scenario is illustrated as in Fig. 7 where "Option Two" corresponds to the undercutting attack. If the miner performs the undercutting strategy, it may gain nothing if its block is not in the longest chain eventually. The undercutter strategically performs undercutting strategy so as to attract the other miners to mine on the forked chain. Meanwhile, the other miners consider whether to mine on the forked chain or not to maximize their profits. Thus, the interaction among the miners can be modeled as a repeated game that in every stage of mining, each miner chooses to perform honest mining or undercutting. The game theoretical analysis shows that if a miner's undercutting strategy follows a certain function to maximize the size of the block, then the strategy is also the best response for all miners. This is under the constraint that if the miners fork, they must perform undercutting. Thus, the Nash equilibrium exists as all miners adopt the same undercutting strategy. The simulation results show that when each miner applies a no-regret learning algorithm, even with 66% of miners mining honestly, undercutting is profitable than mining honestly. As a result, there could be many unclaimed transactions left, and it will be detrimental to the whole blockchain network. The same conclusion is reached in [74] through a non-game theoretical method. However, if the simulation takes network latency into account, the undercutters may have sufficient time to include all the transactions into the block, and thus the undercutters have no incentive to leave any transaction to the next miner.

Different from attacks among the pools, another variation of selfish mining attack inside the mining pool which operates on the protocol of Pay Per Last N Shares (PPLNS) [75] is introduced in [58]. PPLNS is a popular pool mining reward mechanism. Instead of distributing a block reward among miners in the pool in the current round, PPLNS distributes the reward among miners that have submitted shares[3] already in the latest PPLNS window. The PPLNS window includes the number of shares submitted continuously, and the latest share is the full solution of PoW. Specifically, shares in the PPLNS window are regarded as the effective shares. The miner that

[3] A share is a hash value which is easier to be found, compared with the valid hash puzzle solution of the block. Shares can be used to statistically measure the computational power that miner possesses.

submits effective shares obtains the reward according to its proportion of all effective shares. Under this mechanism, the miner may launch the delay attack. In the delay attack, the miner first delays submitting the shares, i.e., by holding the discovered shares, if the miner finds the solution of PoW, the miner releases all delayed shares and then submits the solution immediately. Thus, more reward can be obtained because of the higher fraction of shares in the latest PPLNS window. This scenario is illustrated in Fig. 8.

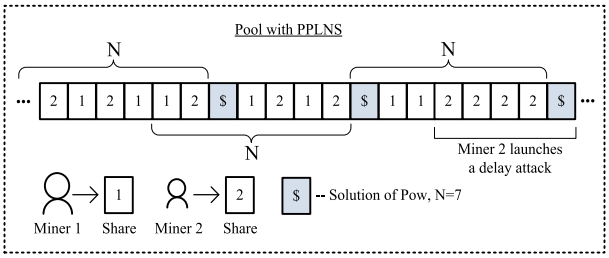


FIGURE 8. An example of delay attack in a pool with PPLNS. The pool includes two miners, i.e., miner 1 and miner 2. The size of PPLNS window in this case is 7. Miner 2 launches a delay attack [58].

For each miner in the same pool, there are two phases during mining. In the first phase, the miner only collects shares for delaying. In the second phase, the miner submits every share immediately, i.e., through honest mining. To maximize the expected profit of launching the delay attack, each miner needs to choose proper time to transit its phase according to the strategies of the other miner. Otherwise, the miner may lose the reward of all its delayed shares. Thus, the authors in [58] model the interaction between miners in the same pool as a non-cooperative game. It is proved that the Nash equilibrium exists if the computational power of the most powerful miner meets a certain condition. This condition is associated with the PPLNS window size, and complexity of finding the solution of PoW. At the Nash equilibrium, each miner of the pool is at the turning point between two phases. This means that the miner has no incentive to deviate from honest mining, and thus the miner would not delay its shares. Such a pool is called the *incentive compatible* pool. Simulation results show that if the pool is not incentive compatible, although the fraction of delaying miners decreases with a parameter related to the window size and the complexity of solving PoW, the game cannot reach the Nash equilibrium regardless of computational power distribution.

B. MAJORITY ATTACK

The security of blockchain is achieved through the distributed consensus of miners. This consensus is only reliable with the assumption that no single miner can hold more than 50% of the network's computational power [1]. Theoretically, to gain its profit, the miner invests more in the computational power, and it may possess more than 50% of the network's computational power [30]. In this case, the miner would be able to halt payments, reverse transactions, prevent new transactions from confirmation, and double-spend coins [2], [27], [76]–[81]. The attack is called 51% attack. As such, the assumption of the distributed consensus may not be valid any longer, and the security of blockchain is not guaranteed. More specifically, theoretical analyses [54], [59], [82] show that the miner which possesses only a relatively large part computational power can also achieve the similar goal. In general, we label this type of attack associated with a large group of miners as the majority attack.

When the majority attack is performed, mining on the fork chain may happen. The condition under which a miner has an incentive to mine on the fork is investigated in [28]. Although the miners follow the longest chain rule under the Nakamoto protocol, the chain can fork in some instance. It leads to a structure similar to a branching tree [83]. To maximize the profit, i.e., the reward of creation of a new block, each miner aims to extend selectively any of the existing branches or to create a new branch, given the strategy of the other miners. A non-cooperative game can thus be applied. If more than 50% of the network's total computational power are extending the longest chain, deviating from honest mining only leads to the waste of the miner's computational power of mining. The reason is that the mined block would not achieve the Nakamoto consensus with the majority of miners and thereby be orphaned. This lowers the miner's profit, and thus mining on the longest chain would be the best response of the other miners. Therefore, the game has a Nash equilibrium in which all miners extend the longest chain. If a cartel of miners which possesses more than 50% of the network's computational power forks a chain, following the rule of longest chain would not be the best response for the other non-cartel miners, and thus the Nash equilibrium will be shifted to another one that every miner mines on the fork. Similar conclusion is reached in [82]. If the fraction of computational power deviating from extending the longest chain is more than a value around $1/4$, each miner has an incentive to mine on the fork.

Compared with [28], a more general majority attack is investigated in [84], where the miner not only choose which branches to mine upon but also determine whether or not to release the mined block. The miner can probabilistically hide newly mined blocks and mine on the fork. Since this is similar to that the miners play a game with incomplete information of blockchain state among each other [85], a stochastic game can be applied as presented in [84]. The miner's expected utility is a function of the miner's action, i.e., the allocation of the miner's computational power, and the current state of the game, i.e., the structure of the block tree at present. In the case where the miner's computational power is equal to a profit threshold, the expected utility of mining on a fork is equal to that of mining on the longest chain regardless of the current state. Thereby, when the miner's computational power is less than the profit threshold, the miner has no incentive to deviate from mining on the longest chain which is the best response of the miner and the Nash equilibrium can be obtained. As shown in the simulation results, when the obtained profit threshold is approximately 0.42, the miner

with at most 36% of the total computational power cannot gain more than 36% of the total rewards. Meanwhile, the miner with computational power more than 46% always has an incentive to deviate from the longest chain rule. These results are more accurate than that obtained using the MDP-based scheme [54].

Furthermore, by using the smart contract [86], the authors in [59] illustrate that the miner or the pool which controls only 38.2% of the network's total computational power can gain more reward by deviating from the protocol. The attacking miner uses its full computational power to mine on its private chain while posting a smart contract transaction. This contract transaction includes a hashing puzzle, i.e., the solution of PoW, of its private chain. Any miner that solves the puzzle can receive the reward from the puzzle's creator, i.e., the attacker, in exchange for the solution. Thereby, the attacker may gain more profit when its private chain is longer than the public one. Every time the attacker posts a hashing puzzle through the smart contract, the other miners have two strategies: (i) work on the puzzle in the contract, and (ii) mine on the public chain. Each miner tries to maximize its expected utility, given the set of strategies of the other miners. The interaction among the miners except the attacker can thus be modeled as a non-cooperative game. When the attacker controls more than 38.2% of the network's total computational power, the miner's utility of working on the puzzle with probability α is greater than that of mining on the longest chain, and the attack is thus launched successfully. This means that each miner will work on the puzzle with probability α and mine on the public chain with probability $1-\alpha$. Thus, the game is proved to admit a mixed strategy Nash equilibrium. The game in [59] is formulated under the assumption that miners always mine on the longest chain. However, if some miners perform the selfish mining strategy, the reward of solving the hashing puzzle on a private chain provided by the attacker may not be attractive enough to the other miners. Thus, the attack may fail.

In addition to posting the smart contract as presented in [59], majority attack can also be launched by the attackers offering monetary bribes [87]. To extend the fork chain and thereby increase its probability of successful attack, the attacker can attract other rational miners to mine on the fork by issuing a *whale transaction*, i.e., a transaction with a high transaction fee. Since issuing the whale transaction is similar to bribing the other miners, such an attack is also called *bribery attack* [88]. The attacker's problem is to determine the cost of the attack, i.e., the transaction fee, to maximize its profit. Also, the other miners' problem is to trade off the profit of mining on the fork against the reward of mining on the public chain. A non-cooperative game can be thus used to model the interaction between the attacker and the other miners as presented in [60]. Both theoretical analysis and simulation results show that if the attacker's mining power is greater than a profit threshold, the cost of the attack decreases, i.e., the attacker's profit increases, as the attacker's mining power increases. Here, the profit threshold is a function of the computational power used to mine on the fork, and the number of blocks by which the fork chain is ahead of the public chain. Meanwhile, any miner that possesses as much mining power as the attacker's has an incentive to mine on the fork chain. However, the Nash equilibrium of the game is not discussed.

To avoid such majority attack, the existing miners can act as a defender actively adding honest nodes to the blockchain network. This case is investigated in [51]. The system model consists of one attacker, i.e., the miner which intends to fork a private chain, and one defender, i.e., the miner which honestly mines on the public chain. To obtain the mining rewards, the attacker and the defender compete to build the blocks for the private and public chains in a sequence of stages, respectively. The historical strategies and the probabilistic stage transitions can be observed by both the attacker and the defender. Thus, the interaction between the attacker and the defender can be modeled as a stochastic game. In the game, the strategies of the defender are (i) *defending*, i.e., actively adding the honest nodes to avoid the majority attack, and (ii) *doing nothing*, i.e., letting the blockchain network run as usual. If the winning probability of the attacker to fork successfully is greater than a certain value, the defender's utility of defending is greater than that of doing nothing. This means that the defending strategy is the best response of the defender and the game reaches the Nash equilibrium. Here, the value is determined based on the cost of adding honest nodes, the number of nodes added actively to the blockchain network, and the total mining power that the attacker has. Otherwise, the defender has no incentive to neutralize the attack. However, it is worth noting that the evaluation of the model is purely based on simulation results in [51]. No actual data gathered from real blockchain networks, e.g., Blockr.io [89] and Blockchain.info [90], is used to verify the practicability of the game model.

The aforementioned approaches, i.e., [51], [59], [60], [84], consider the motivation of the attack within the blockchain eco-system. However, the attacker's motivation can also be based on the incentive outside the system and this type of attack is called *Goldfinger attack* [91]. In this case, the attacker, i.e., miners, receive some payoff from devaluing the cryptocurrency (i.e., currency measured in digital tokens in the blockchain network), by forming a cartel to impair the consensus among miners and launching the majority attack. The defenders, i.e., the other miners, intend to preserve the value of the currency. To prevent the currency from being devalued, the defender makes a bid, i.e., similar to a tax to keep the currency alive, to the attacker. Meanwhile, the defender trades off the cost of making the bid and the profit of preserving the currency. Therefore, a non-cooperative game is used to model the interaction between the attacker and the defender in [28]. The utility of the miner is a function of the value of the currency, the bid, and the probability of the currency being attacked. The analysis shows that the defender can maximize its utility by using the first-order optimality condition in which the bid satisfies a

certain constraint associated with the computational power distribution. If such a bid exists, the game is at the Nash equilibrium point where the attacker has no incentive to attack. Otherwise, the currency will have a zero value. However, in a real case, the defender does not know the attacker's expected utility. If the attacker makes a strong claim about the imminent attack, the defender has no incentive to preserve the currency because of the possible high cost, and thus no equilibrium exists.

Apart from the PoW-based blockchains, the majority attack also happens in PoS-based systems [31]. In a PoS system, each agent, i.e., a stake-holder, can earn interest by holding crypto-currency (CC) units (see Section III). To improve the interest, the agent can make a price offer to buy CC units from other agents [92]. As an agent possesses more than 50% of CC units of the system, this agent can halt and reverse any payments or transactions. Thus, the consensus of the system is broken and CC loses its value. Only the agent that intends to devaluate the CC obtains the profit outside the system, e.g., payoff in terms of harsh social regulations on blockchains. The attack is typically launched in multiple stages [61]. Each agent, i.e., the attacker or an honest agent, can observe the historical strategies of each other and then optimize its own strategy. Therefore, a sequential game is proposed in [61] to model the interaction between the attacker and other agents. In the game, the players include one attacker and some other agents. The attacker trades off the profit of devaluating the CC against the cost of making offers and the loss of interest. In the case that the profit of devaluating the CC is greater than the interest of holding the CC, by using the backward induction method, the game is proved to admit a unique Nash equilibrium. At the equilibrium, the attacker has an incentive to buy more than 50% of CC units, and other agents are willing to sell the CC to the attacker since they know that the CC has no value. However, the attacker can succeed in its attack at no cost by announcing to other agents about launching the majority attack before making the price offer. The reason is that if the agents believe that the attack succeeds, they will sell the CC to the attacker regardless of the price that attacker offers. The Nash equilibrium may not exist in this case.

The majority attack also exists in the PoS-based consortium blockchain [93]. In the system, the blockchain user produces transactions for verification and pays the transaction fee. Due to the limited number of miners, some miners can launch the majority attack, i.e., halt or reverse transactions by forming a cartel. Thus, in addition to competing to solve the crypto-puzzle, the pre-selected miners recruit some other miners, i.e., verifiers, to verify the transaction. This results in recruitment cost and propagation delay that reduce the utility of the pre-selected miners [94]. In this case, the blockchain user acts as the leader to set the transaction fee for relative secure verification. The pre-selected miners act as the followers. Given the other miners' strategies, a miner tries to balance between the transaction propagation delay and recruitment cost against the transaction fee offered by the blockchain user. This scenario is illustrated in Fig. 9. The interaction between the blockchain user and the pre-selected miners can be modeled as a Stackelberg game as presented in [43]. By using the second-order derivation, the blockchain user and pre-selected miners' utility functions are proved to be concave. Thereby, they can jointly maximize their utility through backward induction. The simulation results show that the bigger variation range of propagation delay brings lower utility of the blockchain user. However, the game model is under the assumption of complete information of the all miners' strategy. The Bayesian game model [95] can be used to analyze the incomplete information case.

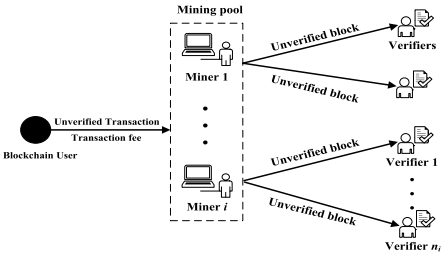


FIGURE 9. An example that demonstrates the relationship among blockchain user, miners and verifiers in the consortium blockchain. The miners recruit some other miners, i.e., verifiers, to verify the transaction [43].

C. DENIAL OF SERVICE (DOS) ATTACK

Due to the distributed structure of peer-to-peer (P2P) network in blockchain with the Nakamoto consensus protocol, each miner can observe the PoW done by their peer miners [1]. However, if the P2P network is interfered or disrupted by some attackers, the resources of the attacked miners for transaction propagation and verification may be exhausted. Thus, the attacked miners would not complete the mining process to gain the mining rewards and their expected profit. Such an attack is called Denial-of-Service (DoS) [96].

The mining pools can perform the DoS attack as presented in [62]. More specifically, to maximize the mining reward, the mining pools can choose (i) to trigger the Distributed DoS (DDoS) attack that lowers the other mining pools' expected payoffs, or (ii) to invest in additional computational power, e.g., by buying more mining machines, to increase its possibility of solving the next PoW. Each mining pool needs to consider the cost of the investment and attack associated with the other pools' strategies, as well as the uncertainty of launching the attack successfully. Therefore, a non-cooperative game can be adopted to analyze the interaction among the pools with different sizes. In the game, there are two players, i.e., a big pool and a small pool. The other pools own the rest of computational power. The payoff of different strategies of the two players can be expressed in a matrix in terms of the computational power distribution, the increasing rate of network's computational power over time, and the probability of launching the DDoS attack successfully.

This matrix is presented in Table 3 where P_s and P_b are the payoffs of the small pool and the big pool, respectively.

TABLE 3. Payoff matrix with launching DDoS attack.

	Investment(I)	Attack(A)
Investment(I)	$P_s(I,I)$,$P_b(I,I)$	$P_s(I,A)$,$P_b(I,A)$
Attack(A)	$P_s(A,I)$,$P_b(A,I)$	$P_s(A,A)$,$P_b(A,A)$

Investing in computational power is the only best response of both big and small pools when computational power distribution satisfies a certain inequality. The condition with a similar structure can also be derived for launching the DDoS attack. The unique Nash equilibrium can be obtained under different computational power distribution. Simulation results show that mining pools have different incentive to perform DDoS attack under different computational power distribution. Due to the higher expected payoff, each pool has a greater incentive to attack larger pools than smaller ones and the larger mining pools have a greater incentive to perform the DDoS attack than smaller ones. These results are consistent with the empirical evidence on the prevalence of DDoS attacks in the Bitcoin system as presented in [96]. The authors in [62] also consider the incentive of mining pools as a whole. However, in a real case, the individual miners have an incentive to hop among the pools and then the computational power distribution changes. Thus, the Nash equilibrium may be shifted.

Apart from only focusing on the short-term impact of DDoS attacks on mining pools as presented in [62], the authors in [63] study the long-term impact. An ongoing DDoS attack causes some long-term impacts that individual miners may migrate, i.e., leave the attacked pool and join other pools. The studied model consists of two pools. At every stage of mining competition, each pool chooses an attack level, i.e., the fraction of its computational power to launch the attack to the other pool. Choosing the attack level affects both the short-term utility consequences (as studied in [62]) and the long-term consequences. In particular, the long-term consequences affect the computational power distribution of mining pools in the next stage. Therefore, the interaction between the two pools can be modeled as a sequential game. By using the second-order derivative, the utility function of the mining pool is proved to be concave under the condition that the attack cost is greater than a certain value. This value is associated with the level of attracting miners to participate in the pool, and the migration rate of miners that are not affected by the attack. Thus, the game can reach a unique Nash equilibrium at which both the mining pools have no incentive to launch the DDoS attack. However, if the condition is not satisfied, the game reaches another Nash equilibrium at which one of the players attacks while the other remains not attacking. For the future work, a general case of multiple mining pools can be investigated.

To avoid DDoS attacks, the authors in [64] propose a reputation-based scheme in which each miner is assigned a reputation value that evaluates the miner's performance of mining honestly against launching DDoS attack. The pool managers send invitation probabilistically only to a subset of miners according to the miners' reputation values. Only miners that receive invitations from pool managers can mine for the pool. Otherwise, the miner has to mine for itself, and this is not preferable for the miner with small computational power. To maximize the profit, each miner chooses to attack or mine honestly while optimizing the profit of launching attack and minimizing the probability to be excluded from pool managers' invitation because of the decrease of its reputation value from the attack. Since the reputation value is updated periodically, and each miner determines its strategy based on the future utility associated with the other miners' reputation value and strategy, a repeated game is used to model the interaction among miners. By removing the strictly dominated strategies of the game according to the miner's utility function, the unique Nash equilibrium can be obtained such that the best response of each miner is not to launch the attack. Similar to the analysis presented in [63], the reason is that even the miner can gain some utilities in the current stage of mining competition by launching the attack, the miner will lose many future mining opportunities due to its low probability of being invited to join the pool. However, details of implementing this reputation-based scheme beyond numerical simulation is not discussed in the paper.

Similar to [64], a punishment scheme based on the action record in blockchain to suppress the attack motivation is proposed in [65]. Nevertheless, the scheme is applied to an edge network instead of the blockchain system. The network model consists of mobile devices and one server located in the edge network. The mobile devices can (i) send service requests to the server, or (ii) launch the DoS attacks to gain their illegal profits. The server can choose (i) to execute the service requests, or (ii) to launch the attack on the devices. Each device or the server can determine its strategy according to the other's historical strategy recorded in the blockchain. Therefore, the interaction between the mobile device and the server can be modeled as a non-cooperative game. The utility of both the players, i.e., the mobile device and the server, is a function of the cost and profit of launching the attack and executing the request, and a punishment factor related to their historical strategies. Since the players can maximize their utility by not attacking under a certain constraint associated with the punishment factor, not attacking is the best response of the players, and thus the game can reach the Nash equilibrium. Simulation results also show that both mobile device and edge server tend to not attack if the punishment factor is large and the attack rate of the server decreases compared with that of the non-punishment scheme. However, the existence of the Nash equilibrium may not be guaranteed in a multi-player scenario.

D. OTHER SECURITY ISSUES

The underlying blockchain technology of Bitcoin is now being applied to many new scenarios such as edge

networks, cloud computing, e-business and information sharing [13], [97], [98]. In particular, a series of security problems regarding false data sharing [40], [66], [67], distrustful goods trading [34], [41] and cyber-insurance [44], can be resolved by using a blockchain-based scheme.

1) FALSE DATA SHARING

The blockchain-based scheme is applied to the false data sharing scenarios. In most of the traditional data sharing application scenarios, the users transfer data either to other users or to a centralized authority for verification. However, the users are reluctant to share the cyber-security information due to the concern about the distrust, the possible false information, the privacy vulnerabilities, and the lack of incentive [99]. To address these problems, the authors in [66] propose a blockchain-based information sharing (iShare) framework. In the iShare framework, organizations, i.e., users participating in sharing cyber-attack information, receive a reward after the information transaction is proved authentic in the blockchain. The organizations can form a group to share information and gain the reward together similarly to forming the mining pool in Bitcoin systems [75]. However, some group members can form a sub-group and infiltrating in another group to gain more profit by not releasing the information in the infiltrated group. This is similar to launching the PBWH attack (see Section IV-A) as presented in [35]. In the two-group case, each group determines the number of organizations to infiltrate to the other group to maximize its profit. Thus, the non-cooperative game can be used to analyze the interaction between the two groups. Each group's utility is determined based on the size and number of infiltrating organizations of the two groups. Since the utility function of the group is concave, each group can maximize its profit when the number of infiltrating organizations satisfies the first-order optimality condition. The unique Nash equilibrium can be obtained when not launching the attack can be the best response for each group. The Nash equilibrium may shift when the number of infiltrating organizations satisfies different constraints. Then, it is possible that launching attack becomes the best response for the group. A general case of multi-groups can be investigated for the future work.

Risks of false information among the users and the lack of incentive can also be found in the traditional cloud computing scenario. The cloud users may not completely trust the computing results returned from the cloud provider. Thus, the verifiability becomes a critical requirement by the cloud users. The existing techniques, e.g., [100], for verifying correctness of the result cannot be done at a reasonable cost. In contrast, a blockchain-based scheme with smart contracts can be used to address the issue, as proposed in [40]. In the scheme, the cloud user pays two clouds, using smart contract, for computing the same task and then collects and crosschecks the results from the two clouds to verify the correctness. However, the two clouds can collude with each other, i.e., by outputting the same wrong result, to gain an extra profit. To maximize the utility, each cloud chooses to compute honestly or to collude to trade off the profit obtained from the cloud user's payment and the loss of the deposit, i.e., a sum of money that guarantees the security for the delivery of the correct result. The cloud's expected utility function is determined based on not only its present strategy but also the imperfect information of the other clouds' historical strategies over time. Thus, the extensive-form game can be used to analyze the interaction between the two clouds. By using the backward induction, each cloud is proved to obtain the strictly dominant strategy that maximizes its utility function at every information set in every sub-game, and thus the game can reach the unique sequential equilibrium. At the sequential equilibrium, both clouds have no incentive to deviate from computing honestly, i.e., not to collude. Simulation results show that the proposed scheme can achieve a low cost compared with the techniques from [100]. The reason is that the cloud users only need to pay the cost of employing two clouds for computing the same task.

Nevertheless, although the smart contract has the advantages as presented in [40], a major limitation exists regarding the data processed on the blockchain. More specifically, trusted entities are required to verify the correctness of the external data that will be brought into the blockchain. The trusted entities can launch an attack by manipulating the data to gain an extra profit [101]. The authors in [67] propose a decentralized entity scheme to prevent the attack. The model consists of the voters and the verifiers. A voter can vote by labeling the data as either true or false, once it submits a small deposit to the system. The verifier can vote about the chosen data after submitting a large deposit. Each participant, i.e., the voter or the verifier, can receive a reward if its statement about the data correctness is the same as that of the other participants. Thereby, a coordination game can be used to analyze the interaction between the voter and the verifier. According to the definition of the coordination game [12], it can be easily proved that the game has two Nash equilibria in which the participants state the same correctness. At the Nash equilibrium, rational participants have no incentive to deviate from voting honestly if the majority participants give the honest statement. The simulation results show that the proposed game can achieve a zero probability of data manipulation.

2) DISTRUSTFUL GOODS TRADING

The distrust of goods trading can also be mitigated by applying blockchain based smart contract as presented in [41]. The proposed smart contract involves two participants, i.e., one seller and one buyer. The participants are required to place a sufficiently large deposit for the reliable transaction which will be returned only after the transaction is completed. The participants can choose to cooperate, i.e., execute the transaction honestly, or to attack, i.e., cheat another participant, e.g., by double spending. To maximize the utility, each participant has to take into account the tradeoff between the cost, i.e., the loss of the deposit, and the profit of launching the attack given the other participant's strategy.

The seller takes its strategy before the buyer does, and thus an extensive-form game can be formulated. The utility of the player, i.e., the seller or the buyer, is determined based on the deposit, the value of the goods and the price set in the smart contract agreement. By using the backward induction, the game is proved to admit a unique subgame perfect Nash equilibrium at which both players perform the transaction honestly. However, how to implement the proposed smart contract is not discussed.

Using a deposit for buying and selling goods can also be found in [34]. The transaction is insured by the deposit of both participants, i.e., the buyer and the seller. The buyer's strategy profile includes (i) PC: pay and confirm the transaction, (ii) PD: pay and leave the system with denying the transaction, and (iii) L_b: leave the system without paying. The seller's strategy profile includes (i) SC: ship the goods and confirm the transaction, (ii) SD: ship the goods and leave the system with denying the transaction, and (iii) L_s: leave the system without shipping. Each participant's payoff is determined based on the value of the goods and its deposit given the other participant's strategy. The interaction between the two participants can be modeled as a normal-form game. By using the iterative removal of dominated strategies [12], the game is proved to have a unique Nash equilibrium if both the participants' deposits are greater than the goods' value. At the Nash equilibrium, the PC and SC strategies are the best response of the buyer and the seller, respectively. Simulation results show that if the deposits of both participants are greater than the value of the goods, the sum of buyer's money and the value of the seller's goods remain unchanged for the whole system. This means that the buyer's money is exchanged into the goods successfully, and the seller's goods is exchanged into the money with no loss. However, in practice, the participant may not be perfectly knowledgeable of the other participant's strategy. More sophisticated game models and tools can be considered.

3) CYBER-INSURANCE

Different from suppressing the attack motivation as presented in [34], [40], [41], [66], [67], the authors in [44] propose a cyber-insurance scheme [102] to compensate for the losses of the attacked blockchain participants. The model includes multiple blockchain users, one blockchain provider, and one cyber insurer. Each user needs to choose a service offered by the provider and maximize its utility given the other users' service demands. Given the users' demand, the provider's problem is to invest in the computing resource to increase its profit. To alleviate losses of being attacked, the blockchain provider also purchases insurance from the cyber-insurer. The cyber-insurer sets the price of the insurance based on the perceived risk level of the provider. Typically, the provider and the insurer offer the service first, and the user then chooses the service. Thus, the interaction among the users, the provider, and the insurer can be modeled as a Stackelberg game. By exploiting the characteristics of the Jacobian matrix [32] to analyze the utility functions of the players, the game is proved to admit a unique Stackelberg equilibrium. The simulation results show that the provider can maximize its utility at a unique point which is in accordance with the uniqueness analysis. In practice, the insurer cannot completely know the risk level of the provider, and thus the Bayesian game can be adopted for further problem investigation.

V. APPLICATIONS OF GAME THEORY FOR MINING MANAGEMENT

Under the Nakamoto protocol, anyone within the blockchain network is allowed to play the role of the mining competition, transaction dissemination and verification in order to obtain the profit [1]. Each miner or mining pool involved has full control of its strategy and attempts to maximize its payoff given the others' strategies. Thus, game theory can be effectively applied to model the interaction between these participants. In this section, we will survey the applications of game theory in the mining strategy management including computational power allocation, fork chain selection, block size setting, pool selection and reward allocation.

A. INDIVIDUAL MINING

1) COMPUTATIONAL POWER ALLOCATION

Bitcoin mining is a competition that miners contend with each other by investing in computational power to win mining rewards. To maximize the utility, each miner determines the allocation of its computational power, i.e., whether or not to invest in the computational power, given the other miners' strategies. Therefore, a non-cooperative game is applied to analyze the interaction among the miners in [29]. The miner's utility is a function of its computational power, the mining rewards and the marginal cost, i.e., the average cost for the miner to invest in a unit of computational power. By using the second-order derivative, the miner's utility function is proved to be concave. Thus, a unique Nash equilibrium exists at which investing is the best response of each miner as long as the miner's computational power satisfies a condition. Here, the condition is determined based on the computational power and the marginal cost of the miner and the entire Bitcoin network. At the equilibrium, it is found that the decision on the investment is not affected by the value of the mining rewards. Moreover, every miner can have a positive utility for any level of other miners' strategies which consequently can prevent a monopoly.

Different from [29] in which the miners choose whether or not to participate and then keep their chosen strategies, the authors in [48] consider a case in which the miners can choose ''arrival'', i.e., investing in the computational power, and ''departure'', i.e., leaving the mining, at any time. In general, the strategy of each miner depends on the state of the blockchain network, i.e., the number of miners participating in the mining, given other miners' strategies. A stochastic game can be applied to analyze the miners' strategies as presented in [48]. The miner's utility is a function of the number of the miners in the system, the arrival and departure

TABLE 4. A summary of game theoretical applications for mining management.

	Ref.	Game Model	Player	Action	Strategy	Payoff	Solution
Individual mining	[29]	Non-cooperative game	Miners	Computational power allocation	Selection of investment in computational power or not	Mining rewards minus cost	Nash equilibrium
	[48]	Stochastic game	Miners	Computational power allocation	Selection between investing and leaving	Mining rewards minus cost	Subgame perfect equilibrium
	[103]	Cournot game	Miners	Computational power allocation	Determination of the amount of investment in computational power	Mining rewards minus cost	Nash equilibrium
	[104]	Non-cooperative game	Miners	Computational power allocation	Selection of proper time to start using the mining machines	Mining rewards minus cost	Nash equilibrium
	[45]	Stackelberg game	Service provider and miners	Computational power allocation	Determination of service price and service demand	Profit minus cost	Stackelberg equilibrium
	[105]	Auction	Service provider and miners	Computational power allocation	Determination of the bid for service	Profit minus cost	Individual utility
	[106]	Auction	Service provider and miners	Computational power allocation	Determination of the bid for service	Profit minus cost	Social welfare
	[107]	Sequential game	Miners	Fork chain selection	Selection of reporting mined block and mining on the longest chain or not	Mining rewards	Sequential equilibrium
	[49]	Stochastic game	Miners	Fork chain selection	Selection of branch to mine	Mining rewards	Subgame perfect equilibrium
	[39]	Extensive-form game	Miners	Fork chain selection	Selection of mining on the fork or not	Mining rewards minus cost	Nash equilibrium
	[108]	Extensive-form game	Miners	Fork chain selection	Selection between strategically or stubbornly deviating the protocol and following the protocol	Mining rewards minus cost and punishment	ϵ-robust equilibrium
	[109]	Coordination game	Miners	Fork chain selection	Determination of updating blockchain version or not	Mining rewards	Nash equilibrium
	[110]	Coordination game	Blockchain users and miners	Fork chain selection	Chosen between two fork chains	Mining rewards	Nash equilibrium
	[111]	Repeated game	Miners	Fork chain selection	Selection of forming the coalition or not	Mining rewards minus cost	Social welfare
	[112]	Non-cooperative game	Miners	Fork chain selection	Selection of forming the coalition or not	Profit minus cost	ρ-coalition-safe 3δ Nash equilibrium
	[31]	Non-cooperative game	Miners	Fork chain selection	Selection of forming the coalition or not	Mining rewards	Nash equilibrium
	[113]	Non-cooperative game	Miners	Block size setting	Determination of the block size	Transaction fees and mining rewards	Nash equilibrium
	[72]	Non-cooperative game	Miners	Block size setting	Chosen transaction to be included in the block	Transaction fees and mining rewards	Nash equilibrium
	[114]	Non-cooperative game	Miners	Block size setting	Chosen of upper bound of block size	Transaction fees	Nash equilibrium
	[37]	Extensive-form game	Miners	Block size setting	Chosen transaction to be included in the block	Transaction fees	Sequential equilibrium
	[115]	Non-cooperative game	Blockchain users	Block size setting	Selection of paying the transaction fee or not	Profit minus transaction fee	Nash equilibrium
	[116]	Non-cooperative game	Miners	Block size setting	Selection to be included in the committee	Mining rewards	Nash equilibrium
Pool mining	[117]	Coalitional game	Miners and pools	Pool selection	Chosen of the pool to join	Mining rewards	Cooperative equilibrium
	[118]	Evolutionary game	Miners and pools	Pool selection	Chosen of the pool to switch	Mining rewards minus cost	Nash equilibrium
	[119]	Coalitional game	Miners and pools	Pool selection	Selection between forming the pool and joining the pool	Mining rewards	Non-myopic Nash equilibrium
	[30]	Non-cooperative game	Miners and pool manager	Reward allocation	Selection of reporting shares and allocating rewards	Mining rewards	Nash equilibrium
	[120]	Repeated game	Miners and pool manager	Reward allocation	Selection of reporting shares and allocating rewards	Mining rewards	Nash equilibrium
	[38]	Extensive-form game	Miners and pool manager	Reward allocation	Determination of the computational power allocation and optimizing the reward allocation	Mining rewards minus cost and charged fee	Subgame perfect equilibrium

rates of the miners, the rate of PoW getting solved, the cost and the reward of the mining. By transforming the utility function to the Bellman equation [121] and then calculating the first-order derivative, the utility function is proved to be monotonic increasing if the cost of mining is greater than a threshold. Thus, investing the maximum power is the dominant strategy of each miner regardless of the state of the blockchain network, and the game has a subgame perfect equilibrium. The simulation results show that the utilities of the miner under different arrival rates gradually converge to the same curve. Namely, the game reaches the equilibrium.

In addition to the case in [29], [48] that the miner can only choose to invest in the computational power or not, the authors in [103] investigate the amount of computational power that the miner determines to invest to win the mining rewards, given the other miners' strategies. The probability that the miner solves the PoW puzzle in a given time can be assumed to follow an exponential distribution [1]. As such, the Nakamoto protocol essentially formalizes an exponential race. A Cournot game [122] can be thus used to analyze the interaction among the miners as presented in [103]. The miner's utility is a function of the mining rewards, the computational power, and the marginal cost of the investment. The game is then proved to admit a symmetric Nash equilibrium by simply showing that the marginal revenue, i.e., the average revenue for the miner to invest in a unit of computational power, is equal to the marginal cost. At the equilibrium, each miner can optimize its investment and has no incentive to deviate from honest mining.

The aforementioned approaches, i.e., [29], [48] and [103], consider the case that the mining reward dominates the transaction fee. Nevertheless, when the transaction fee dominates the mining reward[4], the miner will adjust its allocation of computational power by choosing strategically the proper time to start using its mining machines, i.e., the machines used for mining process which require electricity for their operation, to mine given the other miners' strategies. The reason is that miners have no incentive to mine unless the accumulated transaction fees sufficiently exceed a certain threshold. Thus, the non-cooperative game can be used to analyze the interaction among the miners as presented in [104]. Each miner's utility is a function of the starting time, the operation time, the proportion of the miner's machines, and the probability distribution function of the block finding time. The numerical analysis is thus used to find the Nash equilibrium of the game. The simulation results show that the miners that own the same number of mining machines eventually converge to the same starting time, meaning that the game reaches the Nash equilibrium. However, how to prove the uniqueness of the Nash equilibrium is not discussed.

Although deploying blockchains have been widely considered in many scenarios as presented in [29], [48], [103], [104], deploying PoW blockchain-based applications in mobile environments is still challenging because the mining process consumes high computational power from mobile devices. An edge computing paradigm has been recently introduced in the mobile blockchain networks for offloading the mining tasks of mobile devices, i.e., the miners [42]. The system model is illustrated in Fig. 10. An important issue is how to allocate efficiently the limited edge computing resources of service providers to the miners. The authors in [45] model the interaction among the service provider and the miner as a two-stage Stackelberg game. The service provider acts as the leader setting the price of the service, and then the miner acts as the follower choosing its computational service demand, given the service price and the other miners' strategies. The utility of service provider is a function of the profit obtained from charging the miners, the miners' service demand, the time that the miner takes to mine a block, and the cost of electricity. The utility of the miner is a function of the computational service demand, the service price, the cost and the rewards of the mining. By using the backward induction, the game is proved to admit a unique Stackelberg equilibrium which is supported by the simulation results. However, in practice, the players cannot know the perfect information of each other, and the Bayesian game can be adopted.

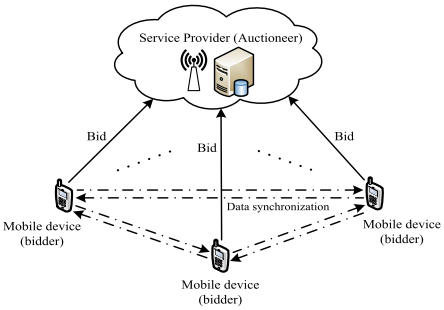


FIGURE 10. An example of the system model of edge computing in mobile blockchain network. The mobile devices compete for the computational power by submitting the bid, and the service provider determines the allocation rule of its service.

Traditional sealed-bid auctions, e.g., the Vickrey auction [123], can also be used to guarantee that the edge computing resources are allocated to the miners which value the resources most. However, designing the optimal auction is challenging. The authors in [105] propose to apply deep learning techniques to achieve the optimal auction for the computing resource allocation in the blockchain network. The model consists of one service provider, i.e., the seller or auctioneer, and multiple mobile users as miners, i.e., bidders. The miners compete for a computing resource unit of the service provider by submitting bids, i.e., the prices that the miners are willing to pay. Upon receiving the bids, the service provider determines the allocation rule, i.e., winning probabilities of the miners, and the conditional payment rule to the miners. The allocation and payment rules are implemented by using neural networks. The neural networks are

[4]Take Bitcoin as an example, the Bitcoin code includes a statement which declares that the mining reward will drop by half after about four years (210,000 blocks). Thereby, the mining reward will eventually be dominated by the transaction fee.

constructed based on an analytical solution of the optimal auction, i.e., the Myerson theory [124]. As such, the auction mechanism learned by the neural networks is optimal in terms of maximizing the revenue of the service provider while ensuring the economic properties, i.e., incentive compatibility and individual rationality. The simulation results show that the proposed scheme outperforms the traditional sealed-bid auction [123] in terms of revenue. However, the proposed scheme is constrained to a single computing resource unit that may not meet the needs of the miners.

Different from the auction in [105] that the service provider, i.e., the auctioneer, maximizes its individual utility, the authors in [106] investigate the case of maximizing the social welfare of the entire blockchain network. Under the same model as that in [105], the utility of the mobile user and service provider is a function of the mining rewards, the computational power, the service price, the demand of the miner, and the robustness of the network associated with the distribution of the computational power. By transforming the social welfare maximization auction problem to a problem of non-monotone submodular maximization with knapsack constraints [125], the algorithm of achieving the social optimum can be developed. The simulation results show that the algorithm not only achieves the good performance in maximizing the social welfare, but also guarantees the truthfulness, individual rationality and computational efficiency. However, the algorithm is designed for the offline auction which is not applicable for real-time trading scenarios.

2) FORK CHAIN SELECTION

Under the Nakamoto protocol, there are sequential PoW puzzles that the next puzzle depends on the solution of the previous one. Each miner needs to choose to (i) report its puzzle solution found based on the longest chain, or (ii) not to report the most recent puzzle solution and to mine on the next puzzle secretly, given the publicity of previous puzzles. As a result, fork chain may appear. To maximize the utility, the miner trades off between reporting the puzzle solution to gain the mining rewards and not reporting the solution and mine on fork. Meanwhile, the miner is uncertain about whether it is the first one to find the solution of the puzzle. Thus, a sequential game with imperfect information can be applied to model the interaction among the miners as presented in [107]. The miner's utility is a function of the distribution of the computational power, the probability of winning to solve the PoW, and the other miners' belief of the upcoming publicity of the puzzles. By using the backward induction, the game is proved to admit a multiplicity of sequential equilibrium. This means that both reporting and not reporting can be the best response of each miner depending on the computational power that the miner uses to solve the puzzle. However, the authors only consider a three-miner case, and a general case with any number of miners can be further investigated.

After finding the solution of the PoW as discussed in [107], the miner probabilistically chooses which branch to mine, i.e., to choose a certain chain to attach its block to, among the tree-like branches of the blockchain network structure. If the miner chooses the branch which will not be the longest chain, the miner's effort to solve PoW is wasted. A stochastic game can be used to analyze the strategies of the miners as presented in [49]. The miner's utility is determined based on the miner's computational power, the number of blocks solved by the miner, the mining rewards, and the difficulty of solving the PoW. By using the backward induction, it is proved that mining on the longest chain is a subgame perfect equilibrium. However, the current longest chain may not be the longest one after several rounds of mining competition. Portions of the historical transactions may be abandoned.

Similar to [49], the authors in [39] demonstrate that following the Nakamoto protocol, i.e., mining on the longest chain, is the Nash equilibrium. However, the model in [39] is based on the PoS system in which the fork chain randomly selects the coin from the set of coins owned by miners at each time step (see Section III). Thus, an extensive-form game can be applied. The miner chooses whether or not to mine on the fork, given the other miners' strategies. The miner's utility is a function of the stake, the mining rewards, the coins of miners selected by the fork, and a discounted factor. Since the cost of mining on the fork increases with the miner's stake, for a sufficiently large stake of the miner, the cost overweighs the profit gained from the mining rewards. By restricting access to the miners with the large stake, the rest of miners have no incentive to deviate from mining on the longest chain, and the game thus reaches the Nash equilibrium. Empirical data obtained from Blockchain.info [90] supports the theoretical analysis.

Extended from [39], the authors in [108] investigate the case of miners choosing the fork chain in an upgraded PoS system. In the upgraded system, the latest block is called the parent block, and concurrent blocks attached to the parent block are called the leaf blocks. Instead of following the longest chain protocol, miners can choose the leaf blocks to be attached to the parent block. To model the interaction among the miners in the tree-like structure of the system, an extensive-form game can be applied. The miners' strategies include deviating from the protocol stubbornly, following the protocol, and strategically choosing whether or not to deviate from the protocol to maximize their utility. Since there is only one leaf block that can reach the consensus to win the reward, the utility of the miner is a function of the reward, the cost of losing the block, and the punishment of deviating from the protocol, given the other miners' strategies. The punishment is implemented by taking away the deposit of the miner that is deposited in advance. When the fraction of the stubborn miners is less than $1/3$, each miner cannot increase its utility more than ϵ or decrease its utility more than $1/\epsilon$ by deviating from the protocol. Thus, the game has a unique ϵ-robust equilibrium [116]. The simulation results show that only when the fraction of the deviated miners is greater than a quarter, the utilities of the miners that follow the protocol decrease, as the number

of the deviated miners increases. This is consistent with the theoretical analysis.

Furthermore, when the fork chain appears, the miners need to decide whether to update the blockchain version, i.e., to acknowledge the fork as a hard fork or not. The hard fork is a permanent divergence from the previous version of the blockchain which requires the miners to upgrade the blockchain software. Since having more miners participating in a particular chain version increases the value of the version, the miner's strategy depends on not only its individual profit, but also the other miners' profits. Thus, a coordination game can be used as presented in [109]. In the game, the miner gains a zero-profit if the miner's strategy is not consistent with those of the majority of miners, and thus the game admits a unique Nash equilibrium. At the equilibrium, every miner chooses to stay on the current version or to upgrade the version. However, voting organization for upgrading the blockchain version remains a topic for further research.

Similar to [109], the authors in [110] propose to use the coordination game approach for choosing the fork chain. The players in the game in [110] are the blockchain users and miners. To maximize the utility, both types of players need to choose between two fork chains to participate. Here, the utility of a blockchain user is a function of the users' distribution of choosing certain chain, the transaction fees, and the strategies of the miners. The miner's utility is a function of the distribution of the users between two fork chains, the computational power, the mining rewards, and the other miners' choice of the chain. If the number of the blockchain users choosing a certain chain is greater than a threshold, the utility of the players can be proved to be monotonous. Thus, the game has a unique Nash equilibrium that all of the players choose the same chain. Otherwise, a mixed strategy Nash equilibrium exists such that players choose the chain randomly. The simulation results show that the user will choose to remain on a certain chain when the number of the users on this chain is greater than a certain value which is in accordance with the theoretical analysis. However, the case which involves multiple fork chains can also be investigated.

The aforementioned approaches, i.e., [109], [110], show that the miners can coordinate, i.e., through forming a coalition, to increase their utilities by deviating from the honest mining. To address this issue, the authors in [111] propose an upgrade scheme for the blockchain protocol. In the upgrade scheme, the mining reward is delayed to be allocated to the miner that finds the solution of the PoW puzzle. Also, the miner can receive variable discounted rewards during several rounds of mining after the miner finds the solution. Extended from the coordination game model in [110] to its infinite form, a repeated game is then adopted in [111] where each miner chooses whether to form the coalition or not in every round of mining. The utility of each miner is a function of its computational power, the mining rewards, the difficulty of solving the PoW, the cost of mining, the number of rounds for allocating the discounted rewards, and the discounted factor of the rewards. It is proved in [111] that if the discounted factor meets a certain inequality, the miner's utility of honest mining is greater than that of forming the coalition. This means that the game has a unique subgame perfect equilibrium at which the inequality is satisfied, and all the miners perform honest mining.

Similar to [111], the authors in [112] propose a scheme to prevent the miners from forming the coalition. In the scheme, the transactions are first included in a buffer block, and the miner mines on the buffer block by solving the PoW. Only after the buffer block is broadcast and verified, this buffer block becomes the real block and will be attached to the blockchain. The miner can choose whether or not to form the coalition, i.e., deviating from the honest mining, given the other miners' strategies. Thus, the interaction among the miners can be modeled as a non-cooperative game. The miner's utility is a function of the computational power, the number of the blocks in a round of mining, the difficulty of solving the PoW, the distance between the buffer block and the blockchain, the cost and the rewards of mining, and the transaction fees. By calculating the ratio of the upper bound to the lower bound of the coalition's profit, the multiplicative increase in utility is proved to be less than $(1 + 3\delta)$. Here, the coalition controls $\rho < 1/2$ fraction of the computational power, and the constant satisfies $\delta < 0.3$. This means that no coalition that controls less than a fraction ρ of the computational power can gain more than a factor $(1 + 3\delta)$ of the mining rewards and transaction fees by deviating from the protocol. Therefore, the game has a ρ-coalition-safe 3δ Nash equilibrium.

Different from the PoW based coalition as discussed in [109]–[111], the coalition in the PoS based system is investigated in [31]. In PoS, the miner's stake, i.e., a parameter associated with the amount of the miner's cryptocurrency and the time that miner has been holding the cryptocurrency, is updated at the end of each round of mining and the stake will be reset to zero after the miner discovers the block (see Section III). The higher stake means less difficulty in mining the block. Thereby, the miner chooses whether or not to form the coalition for holding more stakes to lower the mining difficulty, given the other miners' strategy. Thus, a non-cooperative game can be applied. The miner's utility is a function of the stake, the mining rewards, the number of times that the miner discovers the block and the number of transactions to be included in the block. Even when deviating from the protocol, the coalition miners cannot obtain a higher utility than that of non-coalition. Thus, the game is proved to have a unique Nash equilibrium at which every miner follows the protocol. However, forming the coalition is not the only way to increase the miner's stake. To increase the holding time and thereby increase the stake, the miner has an incentive to hold its tokens without mining. It may leads to a situation where no miner consumes its stake-time to mine, and the entire blockchain network crashes.

3) BLOCK SIZE SETTING

When mining in the Bitcoin network, the miner can earn more transaction fees by including more transactions in its block. However, it also decreases the miner's probability of gaining the mining reward [73] for a number of reasons, e.g., resulting in a longer propagation time for reaching a consensus. Each miner needs to determine strategically the block size, i.e., the number of transactions to be included in a block, to maximize its utility, given the other miners' strategies. Thus, the authors in [113] model a two-miner case as a non-cooperative game. The miner's utility is a function of its computational power, block size, and the time to reach the consensus. Since the first-order derivative of the miner's utility function with respect to the block size is always less than zero when the unit transaction fee and the mining reward meet a certain condition, the strategy that all of the miners include no transaction in their block is a unique Nash equilibrium. However, if the transaction fee or the mining reward change, the Nash equilibrium shifts to the strategy that all of the miners include more than one transaction in their block.

To avoid the case in [113] that all miners include no transaction in their block, the authors in [72] demonstrate the necessity of setting the maximum block size. As with the game approach presented in [113], the miner chooses the transactions to be included in a block at every round of the mining competition. The miner's utility is a function of its computational power and the transaction fees associated with the block size and the Bitcoin mining reward. The transactions that one miner does not include in its block will be included by another miner before the next round of the mining competition. Thus, when the block size is unlimited, the strategy of including all transactions by all the miners regardless of the fee is the unique Nash equilibrium. It is also found that unbounded transaction fee leads to the same Nash equilibrium. However, inflations of the computational power distribution may have an impact on the existence of the Nash equilibrium of the game.

The analysis of setting a proper block size can also be found in [114]. The authors propose a Bitcoin-unlimited scheme to increase the throughput of the Bitcoin system. In the scheme, each miner chooses its own upper bound of the block size, and invalidates and discards the excessive block, i.e., the block with the size larger than its upper bound. To maximize the utility, the miner trades off the transaction fees and the probability of its block being orphaned based on its mining power, given the other miners' strategies. Thus, a non-cooperative game can be used to model the interaction among the miners. Since any miner that chooses different upper bound gains zero utility, the game is proved to admit a unique Nash equilibrium at which all miners choose the same upper bound. Since only the blocks with appropriate sizes would be added to the blockchain, the block size under the proposed scheme gradually increases to the maximum limit associated with the network capacity. This means that the divergence on the block size is always bounded and the throughput of the system increases. The simulation results show that if all miners have different bounds, the miners that possess large computational power intend to form a coalition to gain extra profit. However, this is harmful to maintaining the decentralized structure of Bitcoin.

However, the unlimited block size [114] may not lead to a higher throughput of the Bitcoin system. The reason is that any two blocks may have collisions, i.e., the miners simultaneously choose the same subset of transactions to be included in the blocks. This situation wastes the computational power for verification and lowers the throughput of the system. To address this issue, the authors in [37] propose an improved Bitcoin protocol. In the protocol, the system selectively incorporates transactions of off-chain blocks into the main chain and awards creators, i.e., miners, of the accepted transactions even if the creators' blocks are not part of the main chain. Each miner chooses the transactions to be included in its block and trades off the transaction fees and probability of the collision. The miners are partially aware of other miners' strategies and take their strategies sequentially. Thus, an extensive-form game can be used to model the interaction among the miners. The utility of the miner is a function of the position of its block in the main chain, the discount factor, and the fees of the chosen transactions. By using the backward induction, the game is proved to admit a sequential equilibrium at which the miners probabilistically choose the transaction to minimize the collision. As a result, the proposed protocol achieves a higher throughput which is consistent with the simulation analysis. However, the game has several other Nash equilibria at which the miners' utilities are much less than that of the sequential equilibrium.

Moreover, even with the unlimited block size as presented in [114], there is still a limitation on transactions to be included in the block. The limitation is imposed by the waiting time, i.e., the time that a transaction of the blockchain user waits in a queue to be included in the block. The blockchain user can choose (i) to pay a transaction fee to the miner to reduce the waiting time, or (ii) not to pay any fee and may experience a longer waiting time. The miner can decide to stay in or to leave the mining competition according to the expected profit of the transaction fees and the cost. Thus, the interaction between the miners and the users can be modeled as a non-cooperative game as presented in [115]. The miner's utility is a function of the number of miners in the network, the rate of solving the PoW, the exchange rate between the Bitcoin value and the dollar, the transaction fees, the rewards and the cost of the mining. The user's utility is a function of the exchange rate, the transaction fee, the waiting time, the profit of the included transaction, and the fraction of users that pay the fee. The constraint on the number of miners and the rate of solving the PoW can be obtained, when the miner's and the user's utilities are both greater than zero. This means that if the constraint is satisfied, the game has a unique Nash equilibrium. At the equilibrium, the miner chooses to keep mining and the user chooses to pay the transaction fee. Empirical evidence from blockchain.info [90] is used

to validate the theoretical analysis. However, multiple Nash equilibria can exist if the constraint is not satisfied.

As presented in [115] that the waiting time limits the throughput of the blockchain network, the authors in [116] propose a novel protocol that greatly reduces the waiting time for the transaction to reach the Nakamoto consensus. In the protocol, there is a committee comprised by a certain number of members, i.e., miners. The block found by any miner is verified only when the majority of members reach the consensus. This miner is then selected as a member in the committee and ranked based on its computational power. The utility of the member is a function of the computational power, the mining rewards and the other members' strategy. Thus, a non-cooperative game can be applied. Since the member gains the positive profit only when the member follows the protocol, i.e., chooses the block with higher rank, the game is proved to admit a unique Nash equilibrium. At the equilibrium, the chain is never forked and the confirmation time for preventing from the double spending is unnecessary. As a result, the throughput of entire the blockchain network increases.

B. POOL MINING

1) POOL SELECTION

To reduce the volatility of the mining rewards and to maximize the utility, miners can form a coalition, i.e., mining pool [75], and cooperate with the members, i.e., miners in the pool, by following the reward allocation of the pool. Thus, a coalitional game [11] can be used to analyze the interaction among the miners and the pools as presented in [117]. Since the communication delay of the Bitcoin network leads to the non-linearity of the pool's mining rewards, the rewards cannot be distributed stably among the members. This means that there always exist some miners that have an incentive to leave their pools and join other pools to increase their utility. As a result, no cooperative equilibrium exists in the game. Additionally, as more transactions are processed in the Bitcoin system, the non-linearity effect on the mining rewards increases, and thus miners are more likely to switch to other pools. In other words, they prefer to join the pool which benefits them most.

During pool selection, each miner first randomly selects a mining pool to start mining with and then switches to another pool after a time period according to its expected utility. The distribution of the miners in mining pools of the whole blockchain network evolves over time based on the miners' strategies. Thus, the framework of evolutionary game [126] can be used to analyze the dynamic process of the miners' pool selection as proposed in [118]. According to the rules of the replicator dynamics [127], if the growth rate of the pool size becomes zero and small perturbation to the pool size does not cause deviation, the distribution of the miners reaches evolutionary stability [128]. Here, the utility of the miner is a function of its computational power, propagation delay, the mining reward and the mining cost. By exploiting the characteristics of the Jacobian matrix of the replicator dynamics in a two-mining-pool network, the game is proved to admit conditionally a unique evolutionary stable equilibrium.

The miners in a PoS system can also form coalitions, i.e., pools, to increase their utilities. The miners need to trade off the cost and the expected profit of forming the pool. For this, each miner chooses (i) to form a pool as a leader, or (ii) to allocate its stake to pools that are already created by the other miners given the reward scheme of the system. In particular, the miner first determines the amount of stake to be allocated to become the leader and then calculates the best possible allocation of mining rewards. Thus, a coalitional game can be applied to analyze the respective aspect of interactions among the miners and the pools as presented in [119]. The results of backward induction illustrate that both the games have a unique non-myopic Nash equilibrium [129]. At the equilibrium, the certain number of pools are formed with the same size. The rewards are distributed evenly among all miners, except for pool leaders that get an additional gain. The simulation results show that starting from no pool, the game quickly converges to multiple pools of an equal size which is consistent with the theoretical analysis.

2) REWARD ALLOCATION

Admittedly, the mining pool's reward allocation, i.e., the algorithm used to share mining rewards among miners, has a significant impact on the utilities of the miners [75]. The miner can choose to immediately report shares, i.e., preimage solutions for a block that meets the requirement set by the pool manager [25], or to delay the reporting given the reward allocation of the pool. The pool manager needs to select the reward allocation algorithm according to the miners' expected utility. Thus, a non-cooperative game can be used to analyze the interactions between the miners and the pool manager as presented in [30]. If a certain condition is satisfied, the strategy that each miner reports the shares immediately is the Nash equilibrium. Here, the condition is associated with the miner's computational power, the probability of finding the full solution of the PoW, the number of reported shares, and the number of the completed rounds of the mining competition.

However, the approach proposed in [30] considers only the single share. Namely, each miner reports the share only one time during mining. In practice, the miners can report the shares repeatedly, and the pool manager can optimize its reward allocation to maximize its utility. Thus, a repeated game can be applied as presented in [120]. It is proved that in the game the pool manager can use the geometric-pay, i.e., a certain reward function, to achieve the social optimum. The simulation results show that the expected utility of the geometric-pay pool, i.e., the pool that allocates its mining rewards following geometric distribution, is greater than those of both the proportional pay pool, i.e., the pool that shares mining rewards evenly among the shares, and the PPLNS pool which is in accordance with the theoretical analysis.

As the miners participate in mining pools to reduce the volatility of the mining rewards, a large pool may become even larger. It may lead to a centralized topology, which is against the fundamental concept of decentralization in the blockchain. However, the authors in [38] demonstrate that this situation will not happen. During each round of mining, the miner chooses to allocate its computational power to a certain pool according to the state of the blockchain, i.e., the distribution of computational power among the pools. The pool manager adjusts the fees charged to the participated miners to maximize its profit, given the state of the blockchain. Thus, an extensive-form game can be applied to analyze the interaction between the miners and the pool managers as presented in [38]. The miner's utility is a function of the computational power, fee charged by the pool, the distribution of miners among the pools, the cost and the rewards of mining. If the fee charged by the pool manager satisfies a condition, the game reaches a subgame perfect equilibrium. Here, the condition is associated with the number of the remaining miners in the same pool. At the equilibrium, the large pools charge a higher fee than the small pools. The miners thus choose the small pools to participate to maximize their utility. As a result, the centralization will not happen. Empirical evidence from Bitcoinity and Bitcoin Wiki supports the theoretical analysis.

VI. APPLICATIONS OF GAME THEORY ATOP BLOCKCHAIN PLATFORM

A. CRYPTO-CURRENCY ECONOMIC

1) TRANSACTION TRANSPARENCY

Under the Nakamoto protocol, the entire history records of transactions are transparent to all the blockchain miners and users. This may cause a series of problems. For example, blockchain miners intend to include the transaction of high quality (i.e., the transactions that are legalized and reliable) into the block rather than the transaction of low quality. The reason is that the transactions that can be traced back to the darknet markets or ransomware payment may be added to the blacklist of the government. The large transaction of low quality may thus be orphaned by the miners regarding the possible huge loss. To mitigate the risk of orphaning transactions of low quality, the user mixes strategically its payment, i.e., by splitting its payment of transaction into several small ones in different qualities. This scenario is illustrated as in Fig. 11. Since the miner's possible loss decreases due to the smaller size of the transaction, the transaction that is not of high quality has a better chance of getting included into the block. The user checks the quality of the other user's transaction sequentially, and a sequential game can thus be used to analyze the interaction among the users [130]. The user's utility is a function of the quality of the transaction, the value of the post-transaction and the cost of mixing the payment. With backward induction, the game is proved to admit multiple subgame perfect Nash equilibria. At an equilibrium, each user mixes their payment in a single transaction instead of sending multiple individual transactions. For future study,

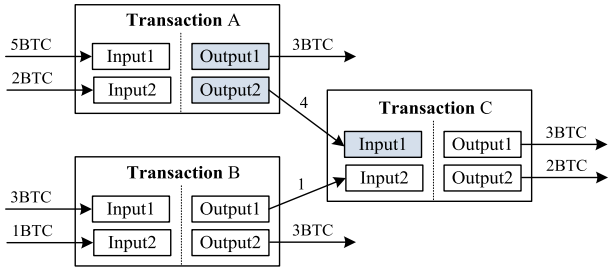


FIGURE 11. An example of the mixing payment: transaction A is identified to be a ransom payment and all of its outputs are added to the blacklist. Transaction B is of high quality. To avoid getting transaction C orphaned by the miners, the user mixes the payment of the transaction C with the payment of transaction A and transaction B.

the transaction size, the cost and the rewards of mining can be taken into account in a more general case.

Under the scenario in [130], the user that mixes the payment of transaction makes money flows more difficult to trace. This is harmful for the entire blockchain system. To address this issue, the authors in [131] investigate the optimal level of transaction transparency and propose a reliable trading system. Since each blockchain user has a unique public key, the user can use the crypto-currency to trade goods with another user directly. To avoid the transaction information, e.g., the ownership of a certain sum of money, being exploited for crime, the proposed system restricts the user's ability to view the complete transaction information attached to the public keys. Thereby, before delivering the goods for trading to other users, the user trades off the expected profit and possible loss in terms of the incomplete transaction information to choose whether or not to perform the trading. The trading can thus be organized as an infinitely repeated game in discrete time as presented in [131]. The user's utility is a function of the trading quantity, trading price, the probability of the trade being performed, the allocation of the goods for trading, and the cost of trading. By defining the inequality that the user's utility of offering a positive trading price is greater than that of the offering a zero trading price, i.e., the transaction failure, the constraint between the trading price and the allocation can be obtained. This means that if the constraint is satisfied, the game has multiple Nash equilibria. In any equilibrium of the game, the user has an incentive to split large transaction into small ones and trades with several other users.

Although the transparency of transaction information causes a series of problems, e.g., malicious uses of information, as presented in [130], [131], it enables the entrant, i.e., the new blockchain user, to possess an endogenous high reputation, i.e., the ability of performing the reliable trading. Thereby, potential users have more incentive to enter the trading system compared with the traditional real-world trading system where only the user that has high reputation can attract customers to trade with. Although the blockchain-based trading system facilitates the entry for potential entrant, the trading competition in the system increases, and the collusion

among the users arises due to the information transparency. Thus, each potential entrant chooses whether or not to enter the system regarding the trade-off between the expected utility after the entry and the severed competition and collusion. Since the potential entrant makes its choice repeatedly in discrete time period, a repeated game can be applied as presented in [132]. The entrant's utility is a function of the probability that one customer joins the trading in a time period, the probabilistic distribution of the reputation, the profit that can be obtained by the trading and the cost of entry. Since both the utility of the entrant and the social welfare of the system are higher than those of the traditional trading system, each potential entrant entering the system is proved to be the Nash equilibrium. However, the balance between transparency and privacy of the blockchain trading system still remains a topic for further research.

2) CRYPTO-CURRENCY VALUE

In the last decade, hundreds of crypto-currencies are adopted in the worldwide financial market. Each crypto-currency has its value which depends on its transaction rate, transaction fees, mining rewards and its fiat exchange rate. The miners need to choose a certain currency to mine according to the value of the crypto-currency and the competition from the other miners. Given the other miners' strategies, the miner can choose to keep mining on the same crypto-currency or change its strategy to mine on another one. Since the incentive of all miners, i.e., players, to change their strategy can be expressed using a single global function, i.e., the potential function [135], the potential game can be applied as presented in [133]. The potential function is determined by the distribution of the miners on mining different crypto-currencies, the computational power, the value and the reward allocation of the crypto-currencies. By using the induction of the better-response learning algorithm [135], the game is proved to admit more than one Nash equilibrium. However, how to achieve a desired equilibrium is not discussed. Similar conclusion is reached in [136]. By leveraging a congestion game model [137], the authors prove the existence of pure Nash equilibria at which users decide whether to mine or not join the blockchain system.

The authors in [36] further investigate the relationship between the value of the crypto-currencies and the population size of the users. Given a certain blockchain-based crypto-currency, the user can choose whether or not to participate in the blockchain platform with a cost and to hold a certain amount of the crypto-currency, given the other users' strategies. Since the user selects its strategy based on the productivity of the blockchain platform, i.e., the state which represents the quality or the usefulness of the blockchain platform, an extensive-form game can be adopted to analyze the interaction among the users as presented in [36]. The user's utility is a function of the transaction supply and demand, the size of the blockchain users, the participation cost and the profit of holding the crypto-currency. By exploiting the characteristics of the Hamilton-Jacobi-Bellman (HJB) equation [138] transformed from the user's utility, the game is proved to admit a unique Markov equilibrium. At the equilibrium, the high crypto-currency value attracts more potential users to participate. This reflects the future growth of the user population size, and the expectation of future growth leads reciprocally to a higher crypto-currency value.

Similar to [36], the authors in [134] demonstrate that the value of the crypto-currency is derived by the computational power of the blockchain network and the population size of the users. The user determines the amount of real money to be allocated in the transaction in the blockchain, and the miner determines the investment in the computational power in exchange for the mining profit according to the strategies of both the other users and miners. A non-cooperative game can thus be applied as presented in [134]. The larger number of users attract more investment in computational power, and more computational power means the stronger consensus within the blockchain network and the higher crypto-currency value. Thereby, it leads to more users participating in the blockchain network. Thus, the reciprocal interaction between the computational power and the user population size captures the equilibrium value of the crypto-currency. This equilibrium value of crypto-currency depends on the users' preferences, e.g., the risk aversion and the censorship aversion, and the usefulness of the network. The empirical data from Blockchain.info [90] supports the theoretical analysis in [134].

B. ENERGY TRADING

Increasing distributed renewable energy users, e.g., solar rooftops and energy storage units, gradually changes the centralized structure of conventional power system. The reason is that the distributed energy users produce the energy and thereby users can trade their energy with each other directly. Therefore, by utilizing the decentralized structure of the blockchain network for trading information exchange, the blockchain-based energy trading systems are proposed. Each energy user in the system can decide the amount of energy to (i) buy from the conventional power system, (ii) buy renewable energy from other users, (iii) store its harvest energy, and (iv) sell its energy to the other users.

When the energy exchange price is set by the users, the interactions among the users can be modeled as games. For example, in [139], a potential game [135] is applied to achieve the social optimum. Considering the energy demand variation, a non-cooperative game is adopted in [140]. The authors in [94] propose a credit-based energy trading system and model the interaction between the users and the credit bank as a Stackelberg game. Otherwise, when the energy exchange price is set by the system where the users bid for the exchange price, the auction models can be applied to achieve the social optimum as presented in [141], [142].

VII. CHALLENGES AND FUTURE DIRECTIONS

In Sections IV, V, and VI, we provide an in-depth survey on applications of game theory to address a wide range

TABLE 5. A summary of game theoretical applications for crypto-currency economic.

	Ref.	Game Model	Player	Action	Strategy	Payoff	Solution
Crypto-currency Economic	[130]	Sequencial game	Blockchain users	Setting transaction transparency	Selection of mixing payments	Profits minus cost	Subgame perfect Nash equilibrium
	[131]	Repeated game	Blockchain users	Setting transaction transparency	Selection of performing trading or not	Function of expected profits and possible loss	Nash equilibrium
	[132]	Repeated game	Blockchain users	Setting transaction transparency	Chosen of entering the system or not	Profits minus cost	Nash equilibrium
	[133]	Potential game	Miners	Determination of the crypto-currency value	Selection between keeping mining and switching to mine on another coin	Crypto-currency value and mining rewards	Nash equilibrium
	[36]	Extensive-form game	Blockchain users	Determination of the crypto-currency value	Chosen of entering the system or not	Profits minus cost	Markov equilibrium
	[134]	Non-cooperative game	Blockchain users	Determination of the crypto-currency value	Determination of the allocation of real money and investment in computational power	Function of computational power and population size of users	Nash equilibrium

of issues in the blockchain networks and related systems. However, with the fast evolution of the blockchain technologies and their applications, a plethora of emerging problems remain open for further studies, many of which can be solved using game theory. In this section, we expand our discussion to some challenges as well as research directions with blockchain, where the mathematical tools of game theory may exert further potential for system analysis and mechanism design.

A. CHALLENGES FROM GAME THEORY PERSPECTIVE

1) EXISTENCE OF NASH EQUILIBRIA

Most references reviewed in this survey discuss the existence of the unique Nash equilibrium. At the Nash equilibrium, the players, e.g., the miners or the pools, have no incentive to deviate from their current strategies. However, in practice, multiple Nash equilibra can exist, and thus it is challenging for the players to choose the optimal strategy or solution. For example, for the mining management [115], with the existence of Nash equilibra, the miners can choose between staying and leaving, and the blockchain users choose between paying or not paying the transaction fee. In this case, finding the solution among the Nash equilibria to achieve a social optimum for the whole network is a challenge. Similarly, for the crypto-currency economic [133], how to achieve a social optimal equilibrium in the crypto-currency market is very challenging.

2) IMPLEMENTATION OF GAME MODELS

The applied game models proposed in aforementioned reviews have its limitation. For example, due to the first-mover advantage, the Stackelberg game is widely used to solve many issues in blockchain network. However, the blockchain network is a type of decentralized system with a number of distributed nodes, i.e., players. Therefore, how leader nodes observe the strategy of each follower node, make optimal decisions, and find the equilibrium is one big challenge. To address the challenge, the meanfield games [143] can be applied for analyzing the performance of the whole blockchain network with large number of miners where individual miners have relatively negligible impact upon the network. In addition, evolutionary games can be adopted for analyzing mining pools' formation and evolution. Stochastic games can be used for analyzing more complex scenarios, such as miners' probabilistic selection of transactions to be included, blocks to be verified and broadcast, and chains to be attached and mine.

B. OPEN ISSUES AND RESEARCH DIRECTIONS FOR APPLICATIONS OF GAME THEORY IN BLOCKCHAIN

1) THROUGHPUT IMPROVEMENT

Blockchain technologies have been adopted in a huge number of scenarios. However, the throughput, i.e., capacity of processing requested transactions, of blockchain networks limits the scope of blockchain applications. The major reasons for this issue are the long block creation time and limited block size [113]. However, block creation time and the block size cannot be easily changed for improving the throughput. The analyses in [114] show that miners intend to form a coalition if the block size is unlimited. This is harmful to maintaining the decentralized structure of the blockchain network. Also, the authors in [115] demonstrate that even with the unlimited block size, there is still a limitation on throughput imposed by the waiting time for transactions to be included in blocks. Thus, to improve the throughput, blockchain protocols in terms of the efficient block creation and the proper block size need to be further developed, and game theory can be a useful tool for improving the consensus protocols.

2) ALTERNATIVE CONSENSUS MECHANISMS

In blockchain networks, e.g., PoW networks, every node performs several certain tasks to maintain the consensus across the blockchain. However, reaching the consensus needs nodes to repeat tasks and may consume a large amount

of electricity [29]. Thus, an alternative consensus mechanism to PoW such as Proof of Useful Work or Resources (PoUWR) [144] may be used. For example, computing hash value in PoW network can be replaced with performing stochastic gradient descent for neural network training [144]. Due to the difference between the tasks in terms of data volume, expected accuracy and variable dimension, the strategies of nodes to obtain a puzzle solution are different from those in the PoW network. Therefore, it is necessary to apply game approaches to analyze the interaction among nodes in the process of PoUWR competition, e.g., the computational power allocation between PoUWR and PoW, the tradeoff between the payoff and the cost, and security issues regarding the deviation from the PoUWR protocol.

3) PERMISSIONED LEDGERS

Public blockchain has been adopted in many applications. Public blockchain allows anyone to participate as a consensus node, and it is not controlled by regulatory agencies, industries or governments. As an alternative to the public blockchain, permissioned blockchain ledgers such as consortium blockchains, become another interesting approach to implement the applications based on Nakamoto-based blockchains. Consortium blockchains can be considered to be semi-decentralization. The reason is that not everyone can participate in the network. The consortium blockchain is maintained by a group of pre-selected nodes, thus allowing for a greater degree of control over the network by regulators. As such, the consortium blockchains involve multiple entities and stake-holders, i.e., the pre-selected nodes, the verification nodes, and the blockchain users. To model and analyze complex interactions among the entities and stake-holders, game theory can be adopted as a useful tool. For example, the non-cooperative games can be used to analyze the node selection, Stakeleberg games can be applied to analyze the interaction between the pre-selected nodes, i.e., the leaders, and the verification nodes, i.e., the followers. Also, evolutionary games can be used to analyze the formation of BFT committees in permissioned blockchain networks.

4) INCORPORATING BLOCKCHAIN TECHNOLOGIES INTO OTHER SCENARIOS

As a versatile technology, it is also possible to incorporate blockchain into other emerging networking and application scenarios. For example, the authors in [45] introduce a blockchain-based edge computing paradigm in which mobile users offload their computing tasks to computing service providers and pay the corresponding fees. This paradigm addresses the implementation issue of blockchain applications on resource-limited mobile services. However, the blockchain-based edge computing paradigm raises resource management issues. For example, how to motivate the service providers to contribute their computing resources. Game theory can be efficiently used to design incentive mechanisms. For example, auction schemes can be adopted to improve the utility or revenue of the service providers. Also, the Stackelberg game can be applied to improve both the utility of the computing service providers and the mobile users. Predictably, by taking advantage of game theory to analyze and design incentive mechanisms, blockchain technologies can be widely incorporated into multi-agent scenarios beyond the crypto-currencies, e.g., mobile blockchain networks, information sharing scenarios, and energy trading markets.

VIII. CONCLUSIONS

This paper has presented a comprehensive survey of the applications of game theory in blockchain. Firstly, we have given an overview of blockchain with its structure, workflow, and incentive compatibility. Then, we have introduced the basic knowledge of game theory and several game models with the objective to understand the motivations of using game theory to analyze interactions among different components in blockchain. Afterwards, we have provided reviews and analyses using game theory in detail to deal with a variety of problems regarding security, mining management and blockchain applications. Finally, we have outlined existing challenges as well as several directions for future research.

REFERENCES

[1] S. Nakamoto. (2017). *Bitcoin: A peer-to-peer electronic cash system*. [Online]. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[2] Z. Zheng, S. Xie, H.-N. Dai, and H. Wang, "Blockchain challenges and opportunities: A survey," *Int. J. Web Grid Services*, vol. 14, no. 4, pp. 352–375, 2016.
[3] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," *Ethereum Project Yellow Paper*, vol. 151, pp. 1–32, Apr. 2014.
[4] D. Schwartz *et al.*, "The ripple protocol consensus algorithm," Ripple Labs, San Francisco, CA, USA, White Paper. 5, 2014.
[5] T. Cox, "Eos. io technical white paper," *GitHub repository*, 2017.
[6] S. Popov. (2018). *The Tangle*. [Online]. Available: http://iotatoken.com/IOTA Whitepaper.pdf
[7] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control," *J. Med. Syst.*, vol. 40, no. 10, p. 218, 2016.
[8] M. Raikwar, S. Mazumdar, S. Ruj, S. S. Gupta, A. Chattopadhyay, and K.-Y. Lam, "A blockchain framework for insurance processes," in *Proc. 9th IFIP Int. Conf. New Technol., Mobility Secur. (NTMS)*, Feb. 2018, pp. 1–4.
[9] M. Castro and B. Liskov, "Practical byzantine fault tolerance and proactive recovery," *ACM Trans. Comput. Syst.*, vol. 20, no. 4, pp. 398–461, 2002.
[10] E. Altman, *Constrained Markov Decision Processes*, vol. 7. Boca Raton, FL, USA: CRC Press, 1999.
[11] R. B. Myerson, *Game Theory*. Cambridge, MA, USA: Harvard Univ. Press, 2013.
[12] Z. Han, D. Niyato, W. Saad, T. Başar, and A. Hjørungnes, *Game Theory Wireless Communication Networks: Theory, Models, Application*. Cambridge, U.K.: Cambridge Univ. Press, 2012.
[13] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical survey on decentralized digital currencies," *IEEE Commun. Surveys Tuts.*, vol. 18, no. 3, pp. 2084–2123, 3rd Quart., 2016.
[14] M. Conti, S. Kumar, C. Lal, and S. Ruj, "A survey on security and privacy issues of bitcoin," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 4, pp. 3416–3452, Apr. 2018.
[15] M. C. K. Khalilov and A. Levi, "A survey on anonymity and privacy in bitcoin-like digital cash systems," *IEEE Commun. Surveys Tuts.*, vol. 20, no. 3, pp. 2543–2585, Mar. 2018.
[16] T. Salman, M. Zolanvari, A. Erbad, R. Jain, and M. Samaka, "Security services using blockchains: A state of the art survey," *IEEE Commun. Surveys Tuts.*, vol. 21, no. 1 pp. 858–880, Jan. 2018.

[17] M. S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, and M. H. Rehmani, "Applications of blockchains in the Internet of Things: A comprehensive survey," *IEEE Commun. Surveys Tuts.*, to be published.
[18] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, "Integrated blockchain and edge computing systems: A survey, some research issues and challenges," *IEEE Commun. Surveys Tuts.*, to be published.
[19] R. C. Merkle, "A digital signature based on a conventional encryption function," in *Advances in Cryptology—CRYPTO*. New York, NY, USA: Springer, 1987, pp. 369–378.
[20] V. Buterin, "On public and private blockchains," *Ethereum blog*, vol. 7, pp. 1–25, May 2015.
[21] C. Cachin, "Architecture of the hyperledger blockchain fabric," in *Proc. Workshop Distrib. Cryptocurrencies Consensus Ledgers*, 2016, p. 310.
[22] C. Christian, "Yet another visit to Paxos," IBM Res., Zurich, Switzerland, Tech. Rep. RZ3754, 2009.
[23] D. Mazieres, "The stellar consensus protocol: A federated model for internet-level consensus," *Stellar Develop. Found.*, to be published.
[24] J. Mogan. (2018). *Quorum. Advancing Blockchain Technology*. [Online]. Available: https://www. jpmorgan. com/country/US/EN/Quorum
[25] W. Wang *et al.*, "A survey on consensus mechanisms and mining strategy management in blockchain networks," *IEEE Access*, vol. 7, pp. 22328–22370, 2018. doi: 10.1109/ACCESS.2019.2896108.
[26] J. Katz, A. J. Menezes, P. C. Van Oorschot, and S. A. Vanstone, *Handbook Application Cryptography*. Boca Raton, FL, USA: CRC Press, 1996.
[27] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Gener. Comput. Syst.*, to be published.
[28] J. A. Kroll, I. C. Davey, and E. W. Felten, "The economics of bitcoin mining, or bitcoin in the presence of adversaries," in *Proc. WEIS*, Jun. 2013, p. 11.
[29] N. Dimitri, "Bitcoin mining as a contest," *Ledger J.*, vol. 2, pp. 31–37, Apr. 2017.
[30] O. Schrijvers, J. Bonneau, D. Boneh, and T. Roughgarden, "Incentive compatibility of bitcoin mining pool reward functions," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, 2016, pp. 477–498.
[31] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A provably secure proof-of-stake blockchain protocol," in *Proc. Annu. Int. Cryptol. Conf.*. New York, NY, USA, 2017, pp. 357–388.
[32] J. B. Rosen, "Existence and uniqueness of equilibrium points for concave n-person games," *Econometrica J. Econ. Soc.*, vol. 5, pp. 520–534, Jun. 1965.
[33] M. Carlsten, H. Kalodner, S. M. Weinberg, and A. Narayanan, "On the instability of bitcoin without the block reward," in *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2016, pp. 154–167.
[34] G. Bigi, A. Bracciali, G. Meacci, and E. Tuosto, "Validation of decentralised smart contracts through game theory and formal methods," in *Programming Languages with Applications to Biology and Security*. Cham, Switzerland: Springer, 2015, pp. 142–161.
[35] I. Eyal, "The miner's dilemma," in *Proc. IEEE Symp. Secur. Privacy*, May 2015, pp. 89–103.
[36] L. W. Cong, Y. Li, and N. Wang, "Tokenomics: Dynamic adoption and valuation," in *Proc. 2nd Emerg. Trends Entrepreneurial Finance Conf.*, Hoboken, NJ, USA, May 2018, pp. 18–46.
[37] Y. Lewenberg, Y. Sompolinsky, and A. Zohar, "Inclusive block chain protocols," in *Financial Cryptography and Data Security*. New York, NY, USA: Springer, 2015, pp. 528–547.
[38] L. W. Cong, Z. He, and J. Li, "Decentralized mining in centralized pools," NBER, New Yrok, NY, USA: Tech. Rep. w25592 2018.
[39] F. Saleh, "Blockchain without waste: Proof-of-stake," Desautels Fac. Manage., McGill Univ., Montreal, QC, Canada, Tech. Rep., 2018.
[40] 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 *Proc. ACM SIGSAC Conf. Comput. Commun. Secur.*, Oct. 2017, pp. 211–227.
[41] A. Asgaonkar and B. Krishnamachari. (2018). "Solving the buyer and seller's dilemma: A dual-deposit escrow smart contract for provably cheat-proof delivery and payment for a digital good without a trusted mediator." [Online]. Available: https://arxiv.org/abs/1806.08379
[42] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When mobile blockchain meets edge computing," *IEEE Commun. Mag.*, vol. 56, no. 8, pp. 33–39, Aug. 2018.
[43] J. Kang, Z. Xiong, D. Niyato, P. Wang, D. Ye, and D. I. Kim, "Incentivizing consensus propagation in proof-of-stake based consortium blockchain networks," *IEEE Wireless Commun. Lett.*, vol. 8, no. 1, pp. 157–160, Feb. 2019. [Online]. Available: https://ieeexplore.ieee.org/document/8432083/
[44] S. Feng, W. Wang, Z. Xiong, D. Niyato, P. Wang, and S. S. Wang. (2018). "On cyber risk management of blockchain networks: A game theoretic approach." [Online]. Available: https://arxiv.org/abs/1804.10412
[45] Z. Xiong, S. Feng, D. Niyato, P. Wang, and Z. Han, "Optimal pricing-based edge computing resource management in mobile blockchain," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–6.
[46] L. S. Shapley, "Stochastic games," *Proc. Nat. Acad. Sci.*, vol. 39, no. 10, pp. 1095–1100, Oct. 1953.
[47] E. Maskin and J. Tirole, "Markov perfect equilibrium: I. Observable actions," *J. Econ. Theory*, vol. 100, no. 2, pp. 191–219, Oct. 2001.
[48] S. Dhamal, T. Chahed, W. Ben-Ameur, E. Altman, A. Sunny, and S. Poojary. (2018). "A stochastic game framework for analyzing computational investment strategies in distributed computing with application to blockchain mining," [Onlne]. Available: https://arxiv.org/abs/1809.03143
[49] B. Biais, C. Bisière, M. Bouvard, and C. Casamatta, "The blockchain folk theorem," *Rev. Financial Stud.*, vol. 32, no. 5, pp. 1662–1715, Apr. 2019. doi: 10.1093/rfs/hhy095.
[50] Y. Zhen, M. Yue, C. Zhong-Yu, T. Chang-Bing, and C. Xin, "Zero-determinant strategy for the algorithm optimize of blockchain PoW consensus," in *Proc. 36th Chin. Control Conf. (CCC)*, Jul. 2017, pp. 1441–1446.
[51] S.-K. Kim. (2018). "The trailer of blockchain governance game." [Online]. Available: https://arxiv.org/abs/1807.05581
[52] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," *Commun. ACM*, vol. 61, no. 7, pp. 95–102, 2018.
[53] N. T. Courtois and L. Bahack. (2014). "On subversive miner strategies and block withholding attack in bitcoin digital currency." [Online]. Available: https://arxiv.org/abs/1402.1718
[54] A. Sapirshtein, Y. Sompolinsky, and A. Zohar, "Optimal selfish mining strategies in bitcoin," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, 2016, pp. 515–532.
[55] L. Luu, R. Saha, I. Parameshwaran, P. Saxena, and A. Hobor, "On power splitting games in distributed computation: The case of bitcoin pooled mining," in *Proc. IEEE 28th Comput. Secur. Found. Symp.*, Jul. 2015, pp. 397–411.
[56] K. Chatterjee, A. K. Goharshady, R. Ibsen-Jensen, and Y. Velner. (2018). "Ergodic mean-payoff games for the analysis of attacks in crypto-currencies." [Online]. Available: https://arxiv.org/abs/1806.03108
[57] M. Babaioff, S. Dobzinski, S. Oren, and A. Zohar, "On bitcoin and red balloons," in *Proc. 13th ACM Conf. Electron. Commerce*, Feb. 2012, pp. 56–73.
[58] Y. Zolotavkin, J. García, and C. Rudolph, "Incentive compatibility of pay per last N shares in bitcoin mining pools," in *Proc. Int. Conf. Decision Game Theory Secur.*, Oct. 2017, pp. 21–39.
[59] J. Teutsch, S. Jain, and P. Saxena, "When cryptocurrencies mine their own business," in *Financial Cryptography and Data Securit*. New York, NY, USA: Springer, 2016, pp. 499–514.
[60] K. Liao and J. Katz, "Incentivizing blockchain forks via whale transactions," in *Financial Cryptography and Data Security*. New York, NY, USA: Springer, 2017, pp. 264–279.
[61] N. Houy, "It will cost you nothing to'kill'a proof-of-stake crypto-currency," SSRN, New York, NY, USA, Tech. Rep.2393940, 2014.
[62] B. Johnson, A. Laszka, J. Grossklags, M. Vasek, and T. Moore, "Game-theoretic analysis of DDoS attacks against bitcoin mining pools," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, Mar. 2014, pp. 72–86.
[63] A. Laszka, B. Johnson, and J. Grossklags, "When bitcoin mining pools run dry," in *Int. Conf. Financial Cryptogr. Data Secur.*, May 2015, pp. 63–77.
[64] M. Nojoumian, A. Golchubian, L. Njilla, K. Kwiat, and C. Kamhoua, "Incentivizing blockchain miners to avoid dishonest mining strategies by a reputation-based paradigm," in *Proc. IEEE Computing Conf. (CC)*. London, U.K., Jul. 2018, pp. 1118–1134.
[65] D. Xu, L. Xiao, L. Sun, and M. Lei, "Game theoretic study on blockchain based secure edge networks," in *Proc. IEEE/CIC Int. Conf. Commun. China (ICCC)*, Oct. 2017, pp. 1–9
[66] D. B. Rawat, L. Njilla, K. Kwiat, and C. Kamhoua, "ishare: Blockchain-based privacy-aware multi-agent information sharing games for cybersecurity," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Mar. 2018, pp. 425–431.

[67] J. Adler, R. Berryhill, A. Veneris, Z. Poulos, N. Veira, and A. Kastania. (2018). "Astraea: A decentralized blockchain oracle." [Online]. Available:https://arxiv.org/abs/1808.00528
[68] X. He, H. Dai, P. Ning, and R. Dutta, "Zero-determinant strategies for multi-player multi-action iterated games," *IEEE Signal Process. Lett.*, vol. 23, no. 3, pp. 311–315, Mar. 2016.
[69] H. Zhang, D. Niyato, L. Song, T. Jiang, and Z. Han, "Zero-determinant strategy for resource sharing in wireless cooperations," *IEEE Trans. Wireless Commun.*, vol. 15, no. 3, pp. 2179–2192, Mar. 2016.
[70] R. Laraki, "The splitting game and applications," *Int. J. Game Theory*, vol. 30, no. 3, pp. 359–376, Mar. 2002.
[71] C. Decker and R. Wattenhofer, "Information propagation in the Bitcoin network," in *Proc. P2P*, Sep. 2013, pp. 1–10.
[72] N. Houy, "The economics of Bitcoin transaction fees," Groupe d'Analyse et de Théorie Economique, Univ. Lyon 2, Lyon, France, Tech. Rep. GATE WP 1407, Feb. 2014.
[73] P. R. Rizun, "A transaction fee market exists without a block size limit," *Block Size Limit Debate Work. Paper*, to be pblished.
[74] M. Möser and R. Böhme, "Trends, tips, tolls: A longitudinal study of bitcoin transaction fees," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, 2015, pp. 19–33.
[75] M. Rosenfeld. (2011). "Analysis of bitcoin pooled mining reward systems." [Online]. Available: https://arxiv.org/abs/1112.4980?context=cs.DC
[76] D. Bradbury, "The problem with bitcoin," *Comput. Fraud Secur.*, vol. 2013, no. 11, pp. 5–8, Feb. 2013.
[77] S. Barber, X. Boyen, E. Shi, and E. Uzun, "Bitter to better—How to make bitcoin a better currency," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, 2012, pp. 399–414.
[78] C. G. Akcora, Y. R. Gel, and M. Kantarcioglu. (2017). "Blockchain: A graph primer." [Onlne]. Available: https://arxiv.org/abs/1708.08749
[79] I. Bentov, A. Gabizon, and A. Mizrahi, "Cryptocurrencies without proof of work," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, 2016, pp. 142–157.
[80] M. Rosenfeld. (2014). "Analysis of hashrate-based double spending." [Online]. Available: https://arxiv.org/abs/1402.2009
[81] A. Shomer, "On the phase space of block-hiding strategies," Cryptol. ePrint Arch., Tech. Rep. 2014/139, 2014. [Online]. Available: https://eprint.iacr.org/2014/139
[82] L. Bahack. (2013). "Theoretical bitcoin attacks with less than half of the computational power (draft)." [Online]. Available: https://arxiv.org/abs/1312.7013
[83] N. T. Courtois. (2014). "On the longest chain rule and programmed self-destruction of crypto currencies." [Online]. Available: https://arxiv.org/abs/1405.0534
[84] A. Kiayias, E. Koutsoupias, M. Kyropoulou, and Y. Tselekounis, "Blockchain mining games," in *Proc. ACM Conf. Econ. Comput.*, Jul. 2016, pp. 365–382.
[85] E. Anceaume, R. Ludinard, M. Potop-Butucaru, and F. Tronel, "Bitcoin a distributed shared register," in *Proc. Int. Symp. Stabilization, Saf., Secur. Distrib. Syst.*, 2017, pp. 456–468.
[86] V. Buterin *et al.*. (2014). *A Next-Generation Smart Contract and Decentralized Application Platform*. [Online]. Available: https://github.com/ethereum/wiki/wiki/White-Paper
[87] J. Bonneau, E. W. Felten, S. Goldfeder, J. A. Kroll, and A. Narayanan, "Why buy when you can rent? Bribery attacks on bitcoin-style consensus," in *Financial Cryptography and Data Security*, J. Clark, S. Meiklejohn, P. Y. A. Ryan, D. Wallach, M. Brenner, and K. Rohloff, Eds. Berlin, Germany: Springer, 2016, pp. 19–26.
[88] J. Becker, D. Breuker, T. Heide, J. Holler, H. P. Rauer, and R. Böhme, "Can we afford integrity by proof-of-work? Scenarios inspired by the bitcoin currency," in *The Economics of Information Security and Privacy*. New York, NY, USA: Springer, 2013, pp. 135–156.
[89] (2018). *Blockr.io*. [Online]. Available: https://www.coinbase.com//
[90] (2018). *Blockchain.info*. [Online]. Available: https://www.blockchain.com/explorer/
[91] P. McCorry, A. Hicks, and S. Meiklejohn, "Smart contracts for bribing miners," IACR Tech. Rep. 2018, 581, 2018.
[92] S. King and S. Nadal. (2018). *Ppcoin: Peer-to-Peer Crypto-Currency With Proof-of-Stake*. [Online]. Available: https://peercoin.net/assets/paper/peercoin-paper. pdf
[93] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *Proc. IEEE Int. Congr. Big Data (BigData Congr.)*, Jun. 2017, pp. 557–564.
[94] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in industrial Internet of Things," *IEEE Trans. Ind. Inform.*, vol. 14, no. 8, pp. 3690–3700, Aug. 2017.
[95] W. Armbruster and W. Böge, "Bayesian game theory," *Game theory Rel. Topics*, vol. 17, p. 28, Feb. 1979.
[96] M. Vasek, M. Thornton, and T. Moore, "Empirical analysis of denial-of-service attacks in the bitcoin ecosystem," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, 2014, pp. 57–71.
[97] S. Underwood, "Blockchain beyond Bitcoin," *Commun. ACM*, vol. 59, no. 11, pp. 15–17, 2016.
[98] M. Crosby, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," *Appl. Innov.*, vol. 2, pp. 6–10, Jun. 2016.
[99] A. Rutkowski *et al.*, "Cybex: The cybersecurity information exchange framework (x. 1500)," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 40, no. 5, pp. 59–64, 2010.
[100] M. Walfish and A. J. Blumberg, "Verifying computations without reexecuting them," *Commun. ACM*, vol. 58, no. 2, pp. 74–84, 2015.
[101] J. Peterson, J. Krug, M. Zoltu, A. K. Williams, and S. Alexander. (Feb. 2018). "Augur: A decentralized oracle and prediction market platform." [Online]. Available: https://arxiv.org/abs/1501.01042
[102] R. Pal, L. Golubchik, K. Psounis, and P. Hui, "Will cyber-insurance improve network security? a market analysis," in *Proc. INFOCOM*, Feb. 2014, pp. 235–243.
[103] J. Chiu *et al.*, "Incentive compatibility on the blockchain," Bank of Canada, Ottawa, Canada, Tech. Rep. 1456, 2018.
[104] I. Tsabary and I. Eyal. (2018). "The gap game." [Online]. Available: https://arxiv.org/abs/1805.05288
[105] N. C. Luong, Z. Xiong, P. Wang, and D. Niyato, "Optimal auction for edge computing resource management in mobile blockchain networks: A deep learning approach," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–6.
[106] Y. Jiao, P. Wang, D. Niyato, and K. Suankaewmanee. (2018). "Auction mechanisms in cloud/fog computing resource allocation for public blockchain networks." [Online]. Available: https://arxiv.org/abs/1804.09961
[107] J. Beccuti and C. Jaag, "The bitcoin mining game: On the optimality of honesty in proof-of-work consensus mechanism," Swiss Econ., Working Paper 0060, 2017.
[108] S. Azouvi, P. McCorry, and S. Meiklejohn. (2018). "Betting on blockchain consensus with fantomette." [Online[. Available: https://arxiv.org/abs/1805.06786
[109] C. Barrera and S. Hurder, "Blockchain upgrade as a coordination game," Prysm Group, Bristol, U.K., Tech. Rep. SSRN 3192208, 2018.
[110] J. Abadi and M. Brunnermeier, "Blockchain economics," MIMEO, New York, NY, USA, Tech. Rep.1254, 2018.
[111] D. Stone. (2018). "Delayed blockchain protocols." [Online]. Available: https://arxiv.org/abs/1804.06836
[112] R. Pass and E. Shi, "Fruitchains: A fair blockchain," in *Proc. ACM Symp. Principles Distrib. Comput.*, Jul. 2017, pp. 315–324.
[113] N. Houy, "The bitcoin mining game," SSRN, New York, NY, USA, Tech. Rep. 2407834, 2014.
[114] R. Zhang and B. Preneel, "On the necessity of a prescribed block validity consensus: Analyzing bitcoin unlimited mining protocol," in *Proc. 13th Int. Conf. Emerg. Netw. EXperiments Technol.*, Aug. 2017, pp. 108–119.
[115] D. Easley, M. O'Hara, and S. Basu, "From mining to markets: The evolution of bitcoin transaction fees," *J. Financial Econ.*, to be published.
[116] I. Abraham, D. Malkhi, K. Nayak, L. Ren, and A. Spiegelman, "Solidus: An incentive-compatible cryptocurrency based on permissionless byzantine consensus," Tech. Rep., Feb. 2016.
[117] Y. Lewenberg, Y. Bachrach, Y. Sompolinsky, A. Zohar, and J. S. Rosenschein, "Bitcoin mining pools: A cooperative game theoretic analysis," in *Proc. Int. Conf. Auto. Agents Multiagent Syst.*, May 2015, pp. 919–927.
[118] X. Liu, W. Wang, D. Niyato, N. Zhao, and P. Wang, "Evolutionary game for mining pool selection in blockchain networks," *IEEE Wireless Commun. Lett.*, vol. 7, no. 5, pp. 760–763, Oct. 2018.
[119] L. Brünjes, A. Kiayias, E. Koutsoupias, and A.-P. Stouka. (2018). "Reward sharing schemes for stake pools." [Online]. Available: https://arxiv.org/abs/1807.11218
[120] B. Fisch, R. Pass, and A. Shelat, "Socially optimal mining pools," in *Proc. Int. Conf. Web Internet Econ.*, Sep. 2017, pp. 205–218.
[121] R. Bellman, "On the theory of dynamic programming," *Proc. Nat. Acad. Sci. USA*, vol. 38, no. 8, pp. 716–719, 1952.
[122] B. Allaz and J.-L. Vila, "Cournot competition, forward markets and efficiency," *J. Econ. theory*, vol. 59, no. 1, pp. 1–16, Feb. 1993.

[123] W. Vickrey, "Counterspeculation, auctions, and competitive sealed tenders," *J. Finance*, vol. 16, no. 1, pp. 8–37, 1961.
[124] R. Myerson, "Optimal auction design," *Math. Oper. Res.*, vol. 6, no. 1, pp. 58–73, 1981.
[125] J. Lee, V. S. Mirrokni, V. Nagarajan, and M. Sviridenko, "Non-monotone submodular maximization under matroid and knapsack constraints," in *Proc. 41st Annu. ACM Symp. Theory Comput.*, Sep. 2009, pp. 323–332.
[126] J. W. Weibull, *Evolutionary Game Theory*. Cambridge, MA, USA: MIT Press, 1997.
[127] J. Hofbauer and K. Sigmund, "Evolutionary game dynamics," *Bull. Amer. Math. Soc.*, vol. 40, no. 4, pp. 479–519, 2003.
[128] J. Hofbauer *et al.*, "Stable games and their dynamics," *J. Econ. theory*, vol. 144, no. 4, p. 1665, May 2009.
[129] S. J. Brams and D. Wittman, "Nonmyopic equilibria in 2× 2 games," *Conflict Manage. Peace Sci.*, vol. 6, no. 1, pp. 39–62, 1981.
[130] S. Abramova, P. Schöttle, and R. Böhme, "Mixing coins of different quality: A game-theoretic approach," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.*, 2017, pp. 280–297.
[131] K. Malinova and A. Park, "Market design with blockchain technology," SSRN, New York, NY, USA, Tech. Rep. 2785626, 2017.
[132] L. W. Cong and Z. He, "Blockchain disruption and smart contracts," NBER, Cambridge, MA, USA, Tech. Rep.14569, 2018.
[133] A. Spiegelman, I. Keidar, and M. Tennenholtz. (2018). "Game of coins." [Online]. Available: https://arxiv.org/abs/1805.08979
[134] E. Pagnotta and A. Buraschi, "An equilibrium valuation of bitcoin and decentralized network assets," Imperial College London, London, U.K., Tech. Rep. SSRN 3142022, Mar. 2018.
[135] D. Monderer and L. S. Shapley, "Potential games," *Games Econ. Behavior*, vol. 14, no. 1, pp. 124–143, 1996.
[136] E. Altman, F. A. Reiffers, D. S. Menaschë, M. Matar, S. Dhamal, and C. Touati, "Mining competition in a multi-cryptocurrency ecosystem at the network edge: A congestion game approach," in *Proc. 1st Symp. Cryptocurrency Anal.*, Aug. 2018, pp. 12–25.
[137] R. W. Rosenthal, "A class of games possessing pure-strategy Nash equilibria," *Int. J. Game Theory*, vol. 2, no. 1, pp. 65–67, 1973.
[138] M. Bardi and I. Capuzzo-Dolcetta, *Optimazation Control Viscosity Solutions Hamilton-Jacobi-Bellman Equation*. New York, NY, USA: Springer, 2008.
[139] A. Ghosh, V. Aggarwal, and H. Wan. (2018). "Exchange of renewable energy among prosumers using blockchain with dynamic pricing." [Online]. Available: https://arxiv.org/abs/1804.08184
[140] S. Noor, W. Yang, M. Guo, K. H. van Dam, and X. Wang, "Energy demand side management within micro-grid networks enhanced by blockchain," *Appl. Energy*, vol. 228, pp. 1385–1398, Aug. 2018.
[141] E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer, and C. Weinhardt, "A blockchain-based smart grid: Towards sustainable local energy markets," *Comput. Sci.-Res. Develop.*, vol. 33, nos. 1–2, pp. 207–214, 2018.
[142] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3154–3164, Dec. 2017.
[143] J.-M. Lasry and P.-L. Lions, "Mean field games," *Jpn. J. Math.*, vol. 2, no. 1, pp. 229–260, 2007.
[144] L. Bottou, "Stochastic gradient learning in neural networks," *Proc. Neuro-Nımes*, vol. 91, no. 8, p. 12, 1991.

ZIYAO LIU received the B.E. degree from the School of Electronics Information Engineering, Zhengzhou University, Zhengzhou, China, in 2015, and the M.S. degree from the Beijing Institute of Technology, Beijing, China, in 2018. He is currently pursuing the Ph.D. degree with the School of Computer Science and Engineering, Nanyang Technological University, Singapore. His research interests include game theory, distributed systems, and cybersecurity.

NGUYEN CONG LUONG received the B.E. degree in electronic and telecommunication engineering from the Hanoi University of Science and Technology (HUST). His research interest includes the Internet of Things (IoT).

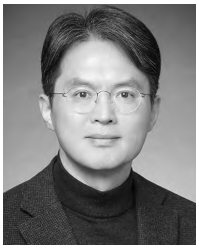
WENBO WANG (S'13–M'17) received the B.S. and M.S. degrees from the School of Automation, Beijing Institute of Technology, Beijing, China, and the Ph.D. degree in computing and information sciences from the Rochester Institute of Technology, Rochester, NY, USA, in 2016. He is currently a Research Fellow with the School of Computer Science and Engineering, Nanyang Technological University, Singapore. His research interests include cross-layer optimization and mechanism design in multimedia wireless networks, cognitive radio networks, green wireless networks, and the Internet of Things (IoT).

DUSIT NIYATO (M'09–SM'15–F'17) received the B.Eng. degree from the King Mongkut's Institute of Technology Ladkrabang (KMITL), Thailand, in 1999, and the Ph.D. degree in electrical and computer engineering from the University of Manitoba, Canada, in 2008. He is currently a Professor with the School of Computer Science and Engineering, Nanyang Technological University, Singapore. His research interests include energy harvesting for wireless communication, the Internet of Things (IoT), and sensor networks.

PING WANG (M'08–SM'15) received the Ph.D. degree in electrical engineering from the University of Waterloo, Canada, in 2008. She is currently an Associate Professor with the Department of Electrical Engineering and Computer Science, York University, Canada. Before that, she was with Nanyang Technological University, Singapore. Her current research interests include resource allocation in multimedia wireless networks, cloud computing, and smart grids. She was a co-recipient of the Best Paper Awards from the IEEE International Conference on Communications, in 2007, the IEEE Wireless Communications and Networking Conference, in 2012, and the Technical Committee on Green Communications and Computing (TCGCC) of the IEEE Communications Society (ComSoc), in 2018. She has been serving as an Associate Editor for several journals, including the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the *EURASIP Journal on Wireless Communications and Networking*, and the *International Journal of Ultra Wideband Communications and Systems*.

YING-CHANG LIANG (F'11) was a Professor with The University of Sydney, Australia, a Principal Scientist and Technical Advisor with the Institute for Infocomm Research, Singapore, and a Visiting Scholar with Stanford University, USA. He is currently a Professor with the University of Electronic Science and Technology of China, China, where he leads the Center for Intelligent Networking and Communications and serves as the Deputy Director of the Artificial Intelligence Research Institute. His research interests include wireless networking and communications, cognitive radio, dynamic spectrum access, the Internet-of-Things, artificial intelligence, and machine learning techniques.

Dr. Liang is a Fellow of the IEEE for contributions to cognitive radio communications and has also been recognized by Thomson Reuters (now Clarivate Analytics) as a Highly Cited Researcher, since 2014. He received the Prestigious Engineering Achievement Award from the Institution of Engineers, Singapore, in 2007, the Outstanding Contribution Appreciation Award from the IEEE Standards Association, in 2011, and the Recognition Award from the IEEE Communications Society Technical Committee on Cognitive Networks, in 2018. He has also received numerous paper awards, including the IEEE ICC Best Paper Award, in 2017, the IEEE ComSoc's TAOS Best Paper Award, in 2016, and the IEEE Jack Neubauer Memorial Award, in 2014. He was the Chair of the IEEE Communications Society Technical Committee on Cognitive Networks. He served as the TPC Chair and Executive Co-Chair of the IEEE Globecom'17. He is the Founding Editor-in-Chief of the IEEE JOURNAL ON SELECTED AREAS IN COMMUNICATIONS: COGNITIVE RADIO SERIES, and the Key Founder and Editor-in-Chief of the IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS and NETWORKING. He is also serving as an Associate Editor-in-Chief for *China Communications*. He served as a Guest/Associate Editor for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, the IEEE JOURNAL OF SELECTED AREAS IN COMMUNICATIONS, the *IEEE Signal Processing Magazine*, the IEEE TRANSACTIONS ON VEHICULAR TECHNOLOGY, and the IEEE TRANSACTIONS ON SIGNAL AND INFORMATION PROCESSING OVER NETWORK. He was also an Associate Editor-in-Chief of the *World Scientific Journal on Random Matrices: Theory and Applications*. He was a Distinguished Lecturer of the IEEE Communications Society and the IEEE Vehicular Technology Society.



DONG IN KIM (S'89–M'91–SM'02–F'19) received the Ph.D. degree in electrical engineering from the University of Southern California, Los Angeles, CA, USA, in 1990. He was a tenured Professor with the School of Engineering Science, Simon Fraser University, Burnaby, BC, Canada. Since 2007, he has been with Sungkyunkwan University (SKKU), Suwon, South Korea, where he is currently a Professor with the College of Information and Communication Engineering. He has been a Fellow of the IEEE for contributions to cross-layer design of wireless communications systems. He is also a Fellow of the Korean Academy of Science and Technology (KAST) and a member of the National Academy of Engineering of Korea (NAEK). He was a first recipient of the NRF of the Korea Engineering Research Center (ERC) in Wireless Communications for RF Energy Harvesting, from 2014 to 2021. From 2001 to 2019, he served as an Editor of Spread Spectrum Transmission and Access and an Editor-at-Large of Wireless Communication I for the IEEE TRANSACTIONS ON COMMUNICATIONS. From 2002 to 2011, he also served as an Editor and a Founding Area Editor of Cross-Layer Design and Optimization for the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS. From 2008 to 2011, he served as the Co-Editor-in-Chief for the IEEE/KICS JOURNAL OF COMMUNICATIONS AND NETWORKS. He served as the Founding Editor-in-Chief for the IEEE WIRELESS COMMUNICATIONS LETTERS, from 2012 to 2015.