2022 IEEE International Conference on Decentralized Applications and Infrastructures (DAPPS) | 978-1-6654-9172-3/22/$31.00 ©2022 IEEE | DOI: 10.1109/DAPPS55202.2022.00012

Game-theoretic Designs for Blockchain-based IoT: Taxonomy and Research Directions

Fatemeh Erfan[1], Martine Bellaiche[1], and Talal Halabi[2]

[1]Polytechnique Montréal, Montréal, QC, Canada
[2]Université Laval, Québec, QC, Canada
Corresponding Author: [1]*fatemeh.erfan@polymtl.ca*

***Abstract*—In the last few years, the combination of the Internet of Things (IoT) and blockchain technologies has widely attracted significant research attention from academia and the industry due to the salient characteristics of blockchain and its natural compatibility with the functional requirements of IoT architectures. Despite the advantages of utilizing the blockchain in IoT systems, several issues have been raised regarding the mitigation of security attacks on blockchain-based IoT systems, management of blockchain operations, node communications, energy consumption, efficient consensus algorithm design, data sharing, and edge/fog computing. Many of the solutions proposed in the literature tried to address these issues using game-theoretic models. This paper surveys and investigates state-of-the-art blockchain-based IoT solutions leveraging game theory to address common issues in blockchain design. The developed taxonomy enabled us to highlight existing challenges to the integration of game theory models into the design of blockchain-driven IoT and bring forward some critical research questions.**

***Index Terms*—Internet of Things, blockchain design, game theory, security, consensus algorithms.**

I. Introduction

The security and privacy of Internet of Things (IoT) have attracted tremendous research efforts. IoT devices generate and process data that may contain sensitive information, creating vulnerabilities that can be exploited by confidentiality and integrity threats. To address these, traditional cryptographic techniques such as attribute-based encryption, identity-based encryption, and public-key systems have been applied. However, they tend to be expensive in terms of energy consumption, processing, and storage. In addition, they require highly centralized architectures, which raise several deployment and scalability challenges and exacerbate single points of failure. Blockchain technology provides a platform to tackle IoT security concerns and alleviate the inherent bottleneck of fast-growing IoT networks that rely on centralized servers [1].

Despite the significant benefits of integrating the blockchain within IoT, it entails several challenges that can be broken down into seven major areas: security, blockchain operations, communication, edge/fog computing, energy consumption, consensus algorithm, and data sharing in scenarios involving devices with constrained capabilities. Furthermore, emerging blockchain-based IoT systems should be analyzed and compared against state-of-the-art architectures in terms of security, privacy, communication, and storage overheads. Moreover, despite the benefits of blockchain in mitigating some security attacks against IoT including single point of failure, Sybil, flooding, and jamming [2], there exist other security attacks driven by the blockchain itself that could be launched against the IoT platform. These include selfish, withholding, majority, and Distributed Denial of Service (DDoS) attacks [3].

To avoid these threats, some researchers usually investigate and analyze the strategies executed by the IoT nodes using game theory models that can be effectively applied to predict the behavior of participating nodes and their defense strategies. Also, during the consensus algorithm, semi-honest or malicious entities participating in the system intend to maximize their benefits by deviating from the protocol. Hence, these nodes will not broadcast their mined blocks; instead, they will hold on to them to maximize their revenue. In such scenarios, game-theoretic approaches can be applied to enable the system to strategically analyze the communications among participants to predict malicious behaviors and adopt optimized punishment strategies toward selfish nodes.

In general, game theory can be leveraged in blockchain-based IoT systems to address existing challenges. For instance, by adopting the blockchain, the design must determine how to manage computational resources, maximize rewards, and choose the nonce selection strategy. In particular, in a blockchain like Bitcoin, participants exploit their computational resources to solve the difficult cryptographic puzzle and gain a reward. In blockchain-based IoT, devices joining the system normally have limited computational resources and must compete with each other to gain access to limited energy resources to support computing. Hence, game theory models can be used to solve such non-cooperative optimization problems. Last, but not least, game theory can be used in designing the consensus algorithm. As the miners in the blockchain are IoT devices with limited computational resources, performing Proof of Work (PoW) or other consensus algorithms may not be suitable. Therefore, Proof of Game (PoG) has been proposed to improve the efficiency of IoT systems [4]–[7].

The goal of this paper is to attract the attention of the research community toward the potential applications of game theory in blockchain-based IoT systems. To the best of our knowledge, this is the first work focusing on the applications and benefits of game theory in blockchain-based IoT systems. The contributions of this paper are summarized as follows:

DOI 10.1109/DAPPS55202.2022.00012

- We overview the various game theory models that have been integrated into the design of blockchain-based IoT.
- We survey, analyze, and classify existing work presenting game-theoretic approaches to tackle security, performance, and management issues in blockchain-based IoT systems into a comprehensive and timely taxonomy.
- We provide an insightful discussion and highlight the research questions and open challenges related to exploiting game theory for blockchain designs in future IoT.

The remainder of the paper is organized as follows. Section II presents background information and concepts. Section III proposes a taxonomy of game theory applied to blockchain-based IoT. Section IV discusses the research gaps and future research areas. Finally, Section V concludes the paper.

II. Background Concepts

Blockchain-based IoT systems normally contain the blockchain as a component within their global architecture [8]. This section provides background knowledge of IoT and blockchain as well as game-theoretic concepts to allow the reader to acquire a comprehensive understanding of Blockchain-based IoT and better grasp its design challenges. Blockchain is one of the disruptive technologies of the last decade. It provides a distributed platform to run decentralized service architectures such as IoT and edge computing [2], and can be effectively used to respond to the security and privacy requirements of most IoT domains by enabling a secure and transparent ledger system [9]. The literature provides several surveys on security issues and blockchain solutions in IoT systems [1], [10], [11]. Nonetheless, the application of game theory to address blockchain design challenges in various scenarios has also been gaining significant traction [3].

A. IoT Systems

IoT has brought new service paradigms across different sectors such as health, autonomous transportation, and various industries. It plays a crucial role in turning homes into smart homes and cities into smart cities [9]. IoT involves smart devices that can upload data to the Internet and control the decisions of cyber-physical processes. They can be monitored and controlled remotely using mobile applications such as in smart hospitals and factories. IoT consists of four main layers: the perception layer consisting of sensors and actuators; the network layer (edge-fog-cloud communications) responsible for transferring the data from devices for processing in upper layers; the processing layer leveraging the cloud environment to perform some computational tasks; and the application layer delivered via end-user devices. In all layers, data confidentiality, integrity, and privacy need to be maintained.

IoT raises many vulnerabilities that can lead to security threats. Attacks at the perception layer include side channel, device tampering, and fake node injection [10]. Attacks at the networking layer include Sybil and man-in-the-middle. At the processing layer, data corruption and DDoS attacks could affect the cloud server and delivered services. Finally, attacks carried out against the application layer are mainly driven by malware such as viruses, worms, rootkits, and ransomware.

Several security attacks and privacy issues in IoT can be addressed using the blockchain [2]. These include the lack of trusted communication channels (intra-system and inter-system), threats brought by single points of failure, and data integrity (e.g., can be addressed using consensus algorithms). Blockchain provides an infrastructure to implement secure and efficient IoT systems by effectively integrating its secure and decentralized platform, and can be applied in most IoT domains such as the Internet of Vehicles (IoV), autonomous drones, smart grids, healthcare IoT, and supply chains.

B. Blockchain Technology

The blockchain is a decentralized system that allows transactions to be verified by a group of unreliable entities [12]. For instance, Bitcoin is a Blockchain concept and one of the virtual cryptocurrencies that has revolutionized the mechanisms in money transfer. To best understand emerging blockchain-based IoT systems, it is important to acquire basic knowledge of the components, types, and significant features of blockchain.

Block: Each transaction transmitted through the blockchain is stored in a block. A sequential chain of blocks created by miners is called a blockchain. Each block includes two parts, the header and body. Data as a transaction is stored in the body part of a data structure called the Merkle tree. It keeps hashing transactions in pairs until a single hash called the Merkle Root is obtained [9]. The block header consists of the identity of the current block, the previous block, a timestamp, and a nonce.

Miner: Once a new block is created by a miner, it is added to the blockchain through the following steps. Miners perform a consensus algorithm to solve a cryptographic puzzle. Then, members in the blockchain validate the created block. To verify a transaction, a local copy of all transactions is not required, and the verification phase can be done by using the Merkle tree stored in the block. Finally, a reward is given to the miner and verified transactions are stored in the blockchain.

Consensus algorithm: In general, it is used to validate the blockchain and add new blocks. This is an approach to mining a block through the blockchain. As part of all consensus algorithms, participants should verify the transaction stored in a new block. Every transaction has a unique ID which is the cryptographic hash of the corresponding transaction's information stored in the block. Table I compares the consensus protocols used in different blockchain platforms [6], [13]–[15].

- *Proof of Work (PoW)* is the first consensus algorithm used in blockchain such as the Bitcoin network. It requires the participants to use their capacities for solving the hard cryptographic puzzle. Publishing new blocks under the PoW protocol is called "mining". Miners try to find a nonce and should have powerful computational resources to perform the proof of work.
- *Proof of Stake (PoS)* is used in blockchains such as Ethereum, where the term "miner" is replaced with "validator". Here, there is no race among participants to find the nonce value and solve the puzzle. One validator is selected for mining based on its proportional stake

including its economic share in the network. This is done in a pseudorandom way with the probability of selection proportional to the validators' share [1], [13], [16]. Delegated Proof of Stake (DPoS) is a variant of PoS where all peers vote to select a node as a witness or delegate [13]. Witnesses are rewarded for generating new blocks and delegates oversee retaining the blockchain and offering some changes including transaction fees and block size. DPoS is more efficient than PoS thanks to its different voting and delegation mechanism.

- *Proof of Game (PoG)* is one of the consensus protocols leveraging game-theoretic models. PoG is proposed for resource-dependent and computational independent consensus algorithms. It restricts the block creator in creating the number of blocks based on the level of the game it can play and the score it can earn [5].
- *Practical Byzantine Fault Tolerance (PBFT)* is a popular consensus algorithm used in permissioned blockchain, where the system combines a group of active and passive replicas [17]. The pre-preparation phase is the first stage of the process of deploying PBFT, followed by the preparation, commit, and reply stages.
- *Proof of Activity (PoA)* combines the features of PoW and PoS. It tends to maintain the best aspects of both algorithms and avoid their worst features. The process of mining is similar to that of PoW. In the first stage, miners make efforts to solve the hash function and win the race based on PoS. Next, transactions are added to the block. Then, several validators are selected to verify the new block according to the PoS consensus algorithm.

Table I categorizes different consensus algorithms which are suitable for IoT networks based on accessibility, scalability, computing, network and storage overhead, throughput, and latency. PBFT has low computing overhead while PoW, PoG, and PoA have high computing overhead.

Based on how it is used and deployed in various systems, blockchain can be categorized into the following types:

- *Public blockchain*, where everyone can participate in the mining, publishing, and verification of the new block as well as accessing the data gathered in the blockchain. This blockchain is also known as permissionless, i.e., everyone can join the blockchain without any permission.
- *Private blockchain*, where only known participants can join the blockchain and access the data shared in the ledger. This type is also named permissioned blockchain.
- *Consortium*, also known as a federated blockchain, this type of ledger is similar to a private blockchain as it includes clusters of private participants managed by different organizations. Hence, multiple organizations having private participants usually join a consortium blockchain.

Blockchain technology also enjoys several features that make it attractive for IoT research including decentralization, immutability, auditability, and fault tolerance [1]. Decentralization is one of the most salient characteristics of blockchain. Turning from a centralized towards decentralized architecture will protect the IoT network against single points of failure and bottlenecks [18] and enable every device to participate in the consensus protocol. Each transaction in the blockchain should be verified by the majority of participants and no central entity monitors the information generated through the network.

TABLE I: Comparison of consensus algorithms.

Consensus algorithm	Accessibility	Scalability	Computing overhead	Network overhead	Storage overhead	Throughput	Latency
PoW	Public	High	High	Low	High	Low	High
PoS	Public	High	Medium	Low	High	Low	Medium
DPoS	Public	High	Medium	N/A	High	High	Medium
PBFT	Private	Low	Low	High	High	High	Low
PoG	N/A	Low	High	Medium	Low	N/A	N/A
PoA	Public	High	High	Low	High	Low	Medium

C. Game Theory

Game theory can play a key role in addressing strategic situations in IoT networks such as competition over resources and decentralized decision making. Also, researchers can take advantage of the powerful game-theoretic models to formally assess the security issues in blockchain-based IoT and develop strategic defense against attacks [9]. In peer-to-peer systems, game theory provides a set of mathematical tools to model the communications between peers, predict their behaviors, and optimize their actions. Generally, each player participating in the game aims to choose a strategy that maximizes its reward. This section overviews the game-theoretical models which have been incorporated into blockchain-based IoT systems.

To better grasp the power and advantages of game theory, some basic terms are first explained as follows.

- *Player:* Each entity (e.g., individual or organization) participating in the game and affecting it by their moves.
- *Action:* In every game, there is a finite set of actions that players can take as part of their strategies.
- *Payoff:* Players take actions to maximize the revenue or payoff they receive. The payoff is defined based on players' selected strategies and is computed using problem-specific parameters.
- *Strategy:* Players' reward or payoff is computed according to the strategies played by all players. Players can choose between a pure or mixed (probabilistic) strategy over their set of actions.
- *Solution concept*: It is a set of rules used to predict how a game will be played. The predictions derived by solving the game indicate the strategies that players will select.
- *Nash equilibrium:* It is a solution concept. If each player has chosen a strategy and no player has an incentive to maximize their own expected payoff by deviating from their strategy while the other players keep theirs unchanged, the game is in Nash equilibrium state. When Nash equilibrium is achieved, each player has chosen their optimal strategy that maximizes their reward.

Many game-theoretical models have been proposed to design blockchain networks, especially in IoT systems. These are divided between non-cooperative and cooperative (i.e., coalitional) games. Due to their inherent nature, non-cooperative games are the most used in blockchain network design, normally to optimize the defensive strategy (e.g., honest mining) against the adversary's actions. On the other hand, cooperative

games are used to effectively coordinate the collaborative behavior of nodes in peer-to-peer networks. As shown in Fig. 1, non-cooperative games can either be static or dynamic, and can be further categorized according to the information available about players' types and their action history [19]. For instance, acquiring the full information in the decentralized blockchain network in a timely fashion can be challenging, hence Bayesian games can be adopted in the design of distributed blockchain-enabled IoT systems with incomplete information sharing [20].

Various game models that exist under this classification have been leveraged for blockchain-based IoT design. These are described as follows:

- *Stackelberg game:* An asymmetric, sequential game where players are divided into two types: the leader who makes a move first, and the followers who select their strategies after observing the leader's actions. Every player tries to maximize their payoff by selecting the best strategy. The leader derives the optimal strategy through backward-inductive reasoning about the follower's anticipated actions. Many of the approaches discussed in this paper used the Stackelberg game model [21]–[24].
- *Repeated game:* When players dynamically play a game multiple times (e.g., super game), the previous strategies may be observed by each player so that they can optimize their future strategies accordingly. Hence, dynamic games can be based on complete or incomplete information.
- *Stochastic game:* It involves repeating distinct games every time the game is executed, i.e., the game is played in different states. Players are allowed to rearrange their strategies depending on the decisions made by other players [25]. For instance, miners can leverage this game to find the best chain to join and the best block to be mined and verified. A stochastic game has also been used to mitigate the majority attack, as described later [26].
- *Differential game*: Here, each player solves an optimal control problem. For instance, Wang et al. [27] used differential games to model the blockchain on top of fog computing to solve the resource contribution problem.
- *Coalitional game:* An important approach to studying the interactions of cooperative players. Each formed coalition has a payoff that may be distributed among its members (e.g., transferable utility). For instance, this approach has been used to investigate the feasibility of integrating blockchain into the design of autonomous systems [28].

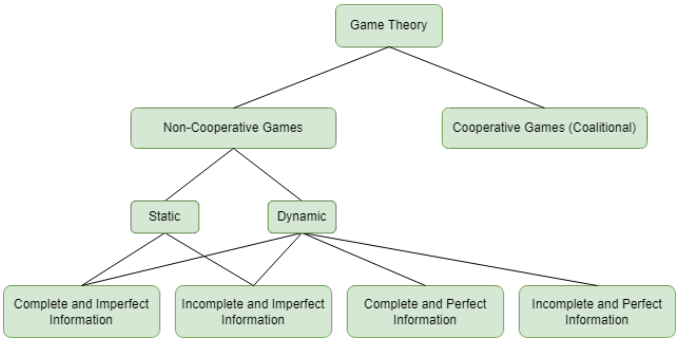

Fig. 1: Categorization of game theory models.

For distributed (and mostly non-collaborative) decision making in IoT networks, game theory can be a valuable tool to predict and regulate nodes' behaviors in the blockchain. Also, it can be used for detecting and mitigating security attacks.

III. Taxonomy of Game-theoretic Design in Blockchain-based IoT

Blockchain is a potential solution to tackle security issues in emerging IoT ecosystems. Nonetheless, it entails challenges in terms of performance, management, and energy consumption, most of which have been recently addressed by integrating game-theoretic models. This section builds a comprehensive taxonomy of the integration of game-theoretic models into various design areas in blockchain-based IoT including security, communication, blockchain operations, energy consumption, consensus protocols, and data sharing as illustrated in Fig. 2. This taxonomy is a valuable roadmap for conducting future research in the field of blockchain design for IoT.

A. Game Theory for Security

When deploying blockchain-based IoT systems, there exist serious security threats that should not be overlooked [29], especially zero-day attacks. For instance, Dongjin Xu et. al. [30] proposed a game-theoretic punishment approach based on action records in the blockchain platform to decrease the probability of occurrence of cyber attacks by mobile users and edge servers and improve the security of the edge network. This section describes several important attacks along with the game-theoretic approaches proposed to address them.

1) Selfish mining attack: A subversive strategy in PoW-driven blockchain where malicious miners or mining pools do not broadcast the newly mined block but instead select to withhold or hold on to it then release it later [31]. In this case, honest miners waste their computational power, creating a block race between honest and selfish miners. Selfish mining attacks can invalidate the blocks mined by honest miners. Thus, all transactions in the honest miners' blocks get rejected. One of the common selfish mining attacks is the pool block withholding (PBWH) attack, where a malicious pool launches a Block WithHolding (BWH) attack against another pool. To prevent this, it is important to assess the strategies taken by miners during communication. Several game-theoretic approaches have been proposed to optimally solve the decision-making problem of resource mining in blockchain [32], [33].

For instance, Singh et al. [33] proposed a non-cooperative differential game to maximize the profit of miners, where each miner behaves selfishly and individually wants to maximize the profit gained. On the other hand, Toda et al. [32] modeled the decision-making problem of miners as a non-cooperative game, where the utility function is defined in terms of energy consumption and the mean mining reward.

For example, Eyal [34] proposed a non-cooperative game among the pools to analyze the node communication through

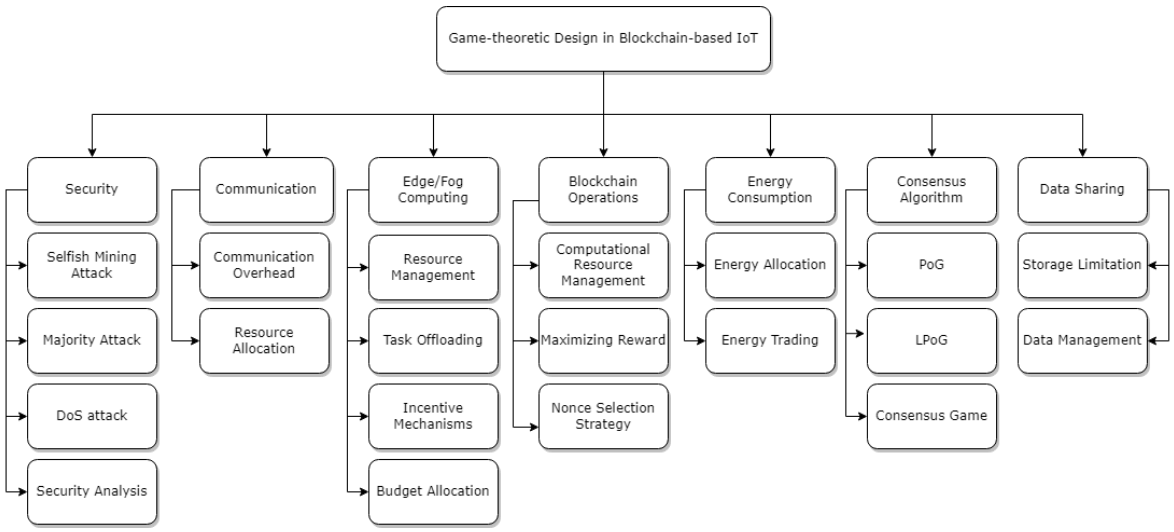

Fig. 2: A timely and comprehensive taxonomy of game-theoretic design in blockchain-based IoT systems.

the blockchain. Particularly, the miners are willing to join those private pools that are not under the PWH attack. Thus, large mining pools could be shrunken down into several smaller ones. The proposed miner's dilemma is similar to the classical prisoner's dilemma: If a miner controls the majority of the mining power, both miners will achieve a lesser reward than when both miners behave honestly. Hence, each miner can choose to attack or behave honestly. If miner 2 (miner 1) chooses to behave maliciously or honestly, the payoff of miner 1 (miner 2) is larger when behaving maliciously than when behaving honestly, respectively. At the equilibrium state, if both miners behave maliciously, the payoff of each miner is smaller than its payoff if neither miner behaves maliciously. The game is played dynamically. The miners can cooperate to behave honestly, and in each round, a miner can detect whether another miner is behaving maliciously and deviating from the agreement. TABLE II depicts this interaction.

2) Majority attack: When a single miner, group of Sybil nodes, or a mining pool control more than 50% of the computational power of a network, a majority or 51% attack [35] is yielded. Attackers can prevent blocks from being verified and reverse transactions during the time they are in control to allow double-spending. Moreover, malicious nodes can split the blockchain and fork the main network. They can also prevent honest miners from finding and verifying new blocks [17]. To avoid this, benign miners can defend against attacker nodes by adding honest nodes to the blockchain network [26]. The communication between these nodes can also be formulated as a stochastic game in which the states reflect the blockchain portions controlled by malicious and benign nodes.

TABLE II: The miner's Dilemma (simplified), where p_1 and p_2 represent the payoffs of miners 1 and 2, respectively.

Miner 1 / Miner 2	Honest	Malicious
Honest	$(p_1 = 1,\ p_2 = 1)$	$(p_1 > 1,\ p_2 < 1)$
Malicious	$(p_1 < 1,\ p_2 > 1)$	$(p_1 < 1,\ p_2 < 1)$

3) DoS attack: Mining pools can potentially carry out DoS attacks to maximize their reward. Some may launch DDoS attacks to decrease the other mining pools' rewards or to access additional computation resources and improve the likelihood of solving the next proof of work. Non-cooperative games can be used to prevent DoS attacks. Particularly, Johnson et al. [36] addressed the trade-off between two different strategies when performing the consensus protocol including construction and destruction by deploying a series of game-theoretic models. Under the construction strategy, a mining pool uses additional computing resources to increase the probability of winning the next race. Under the destruction strategy, it launches a computationally intensive DDoS attack to mitigate the likelihood of winning for the other pools. The authors also studied the incentives of Bitcoin mining pool operators to launch DDoS attacks. Furthermore, machine learning for anomaly detection combined with game theory can be helpful in identifying various attacks including majority and DDoS [37].

4) Security and performance analysis: Game theory is one of the tools used to analyze and compare the security of blockchain-based IoT systems and evaluate their performance. For instance, Tan and Chung [38] made use of game theory to evaluate the security of their proposed blockchain-enabled VANETs system against not only unauthorized tracking of specified vehicles but also adaptive chosen message and replay attacks. Cheng et al. [39] utilized a game theory-based method to analyze time cost consideration in the traffic signal control mode in blockchain-based IoV.

On the other hand, mean-field game is a popular game-theoretic model dealing with large-scale settings and was used by Taghizadeh et al. [40] for equilibrium analysis of mining computational power in blockchain-based IoT. Since dealing with a large group of peers in the blockchain is one of the major challenges that conventional analytical tools normally face, leveraging mean-field game theory allows to analyze the behavior of a large number of players in the network by enabling macroscopic security studies of mining groups.

B. Game Theory for Communications

Communication problems in Blockchain-enabled IoT networks involve the minimization of communication overhead (i.e., transmitted packets) and the management of communication resources (e.g., how to allocate radio channels). Game theory has been applied to solve these problems. For instance, Qiu et al. [21] used a Stackelberg game to perform spectrum trading operations among the buyer and seller. The game involves a leader (mobile network operator) and multiple trackers (unmanned aerial vehicles) competing over resources.

One of the most crucial challenges that have emerged in electric vehicles (EV) is to ascertain the best strategy for each decision-maker to optimize the interests of any participant in the grid with a lower communication overhead. Generally, game theory can be utilized when multiple parties are willing to maximize their own revenue based on their abilities and interests. Xia et al. [20] proposed an approach using a Bayesian game to achieve optimal pricing in the distributed blockchain-based IoV while decreasing the communication load. More specifically, an electricity buyer buys electricity from an electricity seller which is a vehicle that wants to sell its electricity in a trustful way by using a blockchain platform. The Bayesian game-based pricing scheme is written by the smart contract, which plays the role of a virtual agency and achieves optimal trading with lower communication costs.

Chen et al. [41] proposed a secure electricity trading and incentive contract model using blockchain and game theory to encourage vehicles to trade and participate in the game, which is based on income and reward. They showed that communication overhead could be reduced by 64.55%. Hassija et al. [42] proposed an IoV framework using game theory to manage the communication among vehicles. They used the blockchain to address the security and tracking challenges via game-theoretic modeling of the interactions between the vehicles providing and consuming offloading services. Furthermore, to maximize miners' utility, Cong et al. [43] enabled the miners to form a coalition (e.g., mining pool) and cooperate by following the reward allocation mechanism. Therefore, a coalitional game can be effectively designed to manage the communications through the blockchain and predict miners' strategies.

C. Game Theory for Edge/Fog Computing

Incorporating mobile edge computing (MEC) technologies into blockchain-enabled IoT may potentially overcome resource constraints of smart end devices. Edge servers may store the whole blockchain and participate in most of heavy operations such as initiating and validating transactions while IoT devices may serve as lightweight nodes that only store partial blockchain data and undertake less computational-intensive tasks [44]. From a design perspective, game theory can assist in managing the interactions between MEC servers and client devices. For instance, Liu et al. [23] formulated the video transcoding and delivery problem as a three-stage Stackelberg game. The architecture consists of users, base stations, and video providers that all use their computational and communication resources to provide video streaming in a distributed and secure manner. Hence, by using the blockchain, the transcoding service could run without a central server.

Zuo et al. [45] formulated the interaction between the MEC server and users as a two-stage Stackelberg game in mobile blockchain networks. Hence, the achieved Stackelberg equilibrium enables the server to maximize its reward as well as the profit of mobile users. On the other hand, Xiong et al. [46] proposed a game-theoretic approach to analyze the interaction between miners and cloud/fog providers (CFP) in blockchain-based IoT. They presented a lightweight PoW-based blockchain so that the computation overhead is delegated to the cloud/fog. In addition, the management of computational resources in the blockchain consensus process is formulated as a Stackelberg game, through which the revenue earned by CFPs and the miners can be effectively optimized.

Guo et al. [47] proposed a mining task offloading approach using the Stackelberg game and double auction to exploit idle network resources and reduce communication overhead and delay. Ding et al. [48] proposed a model allowing the blockchain to encourage IoT nodes to participate in the mining process by purchasing more computational resources from edge servers. The interaction between IoT nodes and the blockchain is formulated as a Stackelberg game, where the blockchain platform is the leader and the nodes are followers intending to maximize their profit. Xiong et al. [49] proposed a framework to maximize the gains of devices and the MEC server performing heavy tasks in blockchain-based IoT using the Stackelberg game. Miners must decide on a trade-off between the reward from mining and the price to purchase resources. Liu et al. [50] also proposed an architecture based on the Stackelberg game by formulating the interaction between blockchain users and miners. Here, IoT devices want to store their information in the blockchain as transactions.

Wenlong Guo et al. [51] proposed an optimal incentive scheme also based on the Stackelberg game to manage computational resources. This approach formulates the interaction between the edge service providers (ESP) as the leader and mining devices as followers. The ESP provides its computational resources to miners during mining. The game enables the miners and ESP to choose optimal strategies for allocating computational resources and maximizing their profits. This approach assumes three types of rewards: fixed reward, performance reward, and participant reward. The fixed reward is the constant reward for generating a new block. The performance reward is considered as a reward related to the size of the block and the volume of the transaction, while a participant reward depends on the level of participation of miners.

When miners try to mine new blocks, the reward is sometimes not adequate to encourage miners to keep mining. The blockchain with miners who are not incentivized to mine due to low rewards is called a gap chain, and the blockchain with miners who are encouraged to mine due to sufficient profits is called the normal chain. For the first time, Yuan et al. [52] proposed the normal gap game for managing edge resource allocation in the blockchain where the gap and normal chain coexist. Here, miners compete with each other to maximize

their profits. This approach allows the miners to follow the best strategy to manage their computational resources.

Ding et al. [53] proposed a framework for budget allocation in blockchain-based IoT systems with edge computing. The scenario considered consists of IoT resource-constrained devices that require edge servers to perform computational tasks including data analysis or storage. The interaction between buyers and sellers, IoT devices, and edge servers, is formulated using a Stackelberg game model. To the best of our knowledge, there has been little investigation of using game-theoretic models to manage budget allocation in blockchain-based IoT systems, which creates a potential research direction.

D. Game Theory for Blockchain Operations

Anyone in the blockchain network can mine and verify the transactions to obtain profits. In order to gain the maximum rewards, each miner should analyze what strategy to adopt. Game theory can be leveraged to fulfill this goal. Some of the applications of game theory to the blockchain operational phases are normally in computational resource management, achieving maximum reward, and nonce selection strategies.

1) Computational resource management: Each miner decides whether or not to allocate a share of its computational power based on the strategies taken by the other miners. Yang et al. [54] proposed to use non-cooperative game theory to achieve decentralized scheduling of multiple reusable energy sources in the energy local network (ELN) system. Each player in the game needs to make a decision to achieve the optimal objective under limited resources while considering players' interaction and the iterative strategy updates. This is done by formulating its own collaboration strategy to achieve the overall game goal. To deploy the decentralized automated demand response framework for energy storage in the ELN system, each decision maker should select an optimal consumption plan from its strategy set based on the available information.

Wang et al. [27] proposed a scheme based on blockchain in fog computing to optimize resource management using differential game theory. Fog nodes have limited computational resources, hence they need to deploy the optimal management strategy and achieve maximum benefits. This game is an effective solution to represent the dynamic process of fog nodes' strategy generation. Yao et al. [55] formulate the problem of pricing and resource management between industrial IoT miners and cloud providers using a Stackelberg game, where the provider is the leader who sets the price first, then the miners act as followers and pick their strategies.

2) Maximizing reward: Bataineh et al. [56] presented a game-theoretic model exhibiting a mix of cooperative and competitive strategies between the miners and data providers to help them both determine the monetary reward and allocate computational resources. Chen et al. [57] designed a blockchain-based resource auction mechanism in a distributed edge storage scenario, where an auction model based on Bayesian Nash equilibrium is used to maximize profit. Furthermore, efficient pricing-based resource management for mobile mining in edge computing is presented by Xiong et al. [24] to encourage offloading operations in the blockchain platform. In particular, a Stackelberg game is proposed to maximize the utilities of miners as well as the edge computing provider.

Gao et al. [58] presented an approach to establish Nash equilibrium for all parties in the supply chain using game-theoretic models. A bidding session is created and the game is played between a set of suppliers and retailers. Also, Zhang et al. [59] proposed an approach where the electricity consumer creates a contract including its trading strategies, whose goal is to attract small-scale electricity suppliers (SESs) to sell electricity and maximize their revenue. In addition, SESs get maximal rewards if they select the right contract of their own types. Finally, Jiang and Wu [4] used a game-theoretic model to study the effect of block size on miners' payoff. They defined a strategy for varying block sizes due to earning profits (e.g., determining the optimal default size). This approach can be effectively implemented in blockchain-based IoT systems.

3) Nonce selection strategy: Zuo et al. [45] formulated the user's nonce selection strategy as a non-cooperative game, where the utilities of the individual users are maximized in the untrusted MEC-aided mobile blockchain networks. This approach proves the existence of Nash equilibrium and argues that the cooperation behavior is unsuitable for blockchain-enabled IoT devices by using the repeated game concept.

E. Game Theory for Energy Consumption

Throughout the mining process, IoT devices having limited computational resources cannot satisfy the requirements of on-demand energy consumption. To tackle this issue, Li et al. [60] designed a decentralized, on-demand energy supply framework based on microgrids to satisfy the different energy demands of miners in response to consensus protocols. The Stackelberg game is used to formulate the energy allocation among microgrids and miners and achieve optimal profits for both. The microgrid is considered the game leader offering a nonuniform pricing strategy for miners, and a game is launched among the IoT devices that purchase energy from the microgrids. These perform real-time scheduling and decision making to enable the system to maximize the smoothness of operations, while every device intends to maximize its benefits.

Li et al. [61] designed a secure energy trading system in industrial IoT using the consortium blockchain. They proposed a credit-based payment approach to minimize transaction delay and support fast payment along with frequent energy trading. The approach also uses the Stackelberg game to achieve an optimal strategy for credit loans that maximizes the utility of credit banks. For energy trading in the internet of electric vehicles (IoEV), Ali et al. [62] proposed a framework based on the Stackelberg game and the IoTA blockchain to enable EVs to provide energy to vehicles and grids. The game allows the buyer to select the best seller to negotiate the energy price.

F. Game Theory for Consensus Algorithms

Many efficient consensus algorithms for blockchain networks have been presented. Many surveys exist on analyzing consensus algorithms in terms of scalability, how to reward

validators, and security risks [63]. Game theory is also applied in the design of consensus mechanisms. For instance, Kumar and Jain [5] presented the consensus algorithm PoG that can be applied in IoT systems having limited-resource devices. PoG can manage the miners so that they can be restricted in creating the number of blocks based on their levels in the game and their reward. This algorithm can be used for a single miner (i.e., one player) or a pool of miners (i.e., multi-player), and can be applied for resourceful and restricted-resource environments so that the number of game levels and their difficulty are based on resource availability in the network.

A game-theoretic model is also integrated into the fully decentralized consensus protocol to reward honest validators and punish dishonest or lazy ones that do not adhere to the protocol as a way of deterring attacks on the blockchain [64]. Also, a game-theoretic consensus protocol for resource-constrained devices (artificial medical body parts) was proposed in the field of healthcare, namely LPoG, to enable a secure and faster data-centric network [6]. Yaxing Wei et al. [65] proposed a new delegated proof of stake (DPoS) consensus algorithm and a game-theoretic reward and punishment incentive mechanism to improve the voting enthusiasm of blockchain entities and decrease the probability of occurrence of attacks.

Di et al. [66] used a Consensus Game (CG) in blockchain-based IoT to manage the data trading process. They formulated the interactions between IoT sensors as a game combining cooperative and non-cooperative models named "Consensus Game of IoT". The results demonstrate that such hybrid solutions can have an important role in blockchain over IoT. Finally, Alhasnawi et al. [67] presented an advanced demand management scheme based on coalitional game theory as a consensus algorithm to minimize the power mismatch, energy bill, and load energy waste. The communication packet loss can be reduced by using the consensus protocol

G. Game Theory for Data Sharing

IoT devices face the challenge of storage limitation and resource management as they create and collect large amounts of data. Jiang et al. [68] designed a blockchain-based data sharing framework for industrial IoT using game theory, where the relations between data owners and edge devices such as service interactions and data storage are formulated as a Stackelberg game. Zhang et al. [69] also proposed to solve the problem of data sharing and facilitate quality evaluation of the data created by IoT devices using a two-phase Stackelberg game that attempts to maximize the profits of participants.

Bai et al. [70] enabled efficient cross-chain edge data sharing in blockchain-based Industrial Internet of Energy (IIoE). They used a two-step Stackelberg game to achieve the gains from resource scheduling while considering the preferences and risk factors of edge users. Si et al. [71] designed a lightweight blockchain-based information sharing system for IoT devices via a dynamic cooperative game to encourage nodes to behave honestly and mitigate malicious behavior.

Raifa Akkaoui et al. [72] designed a blockchain-based personal health data trading trust model and verification mechanism by leveraging an evolutionary game with two types of players: a data generator who is a patient wanting to share their data and be part of the Medical IoT (MIoT), and a data requester who is accountable for rewarding data generators to motivate them to share their data. There are four different strategy profiles: trustworthy patient, trustworthy requester, untrustworthy patient, and untrustworthy requester. Finally, Jiang and Wu [73] proposed to solve shortage limitations for mining devices in mobile environments using non-cooperative games. The interactions among miners are formulated to explore the impact of delegating mining mechanisms on miners' utilities. Overall, game theory has helped mobile miners to find optimal strategies to tackle storage limitation problems.

IV. Discussion and Insights

This section investigates open challenges related to implementing the blockchain in IoT systems using game-theoretic designs and explores potential research directions in which game theory can play an important role. Some challenges mainly relate to IoT functional and architectural requirements in terms of performance and security. On the other hand, several open problems and limitations still exist when it comes to effectively and efficiently managing blockchain operations in IoT and practically implementing game-theoretic models.

A. Impact on IoT Performance and Security

Most of the existing consensus protocols such as PoW require intensive computations, where IoT nodes must execute computational tasks frequently, thereby leading to energy wastage. In addition, IoT nodes participating in the blockchain system should communicate and cooperate with other nodes, and each block added to the blockchain needs to be broadcast to all nodes, which results in communication overhead. However, most IoT devices have limitations in computation and communication capacity. Although game-theoretic models can be applied to allow IoT nodes to manage their computational and communication resources when the consensus algorithm is executed, finding an efficient game theory-based consensus algorithm for IoT devices by saving on energy consumption and reducing computation overhead remains a challenge.

On the other hand, IoT devices using blockchain can become vulnerable to security threats including selfish, majority, and DDoS attacks. Although these can be mitigated via game-theoretic approaches, various attacks such as eclipse [74] still need to be addressed, potentially using game-theoretical formulations. In IoT, the open nature of mining pools can attract a large number of miners for solving difficult problems together to improve efficiency. However, this increases the attack surface. Recent studies investigated the strategic trade-off that must be established between network openness and vulnerability in PoW-based blockchain [75]. Furthermore, ensuring data privacy when deploying the IoT over the blockchain is a critical challenge. Hence, more research is needed to investigate privacy-preserving ways when deciding on which transactions should be offloaded to the blockchain and how differential privacy can be combined with blockchain.

B. Open Challenges to Blockchain Operations

There exist several challenges related to blockchain design and they can be categorized as follows.

1) Security: Although the blockchain can mitigate security attacks against IoT, it introduces new security threats. For instance, malicious nodes participating in the blockchain may try to maximize their profits by deviating from the protocol. Also, blockchain systems may introduce new program vulnerabilities related to smart contracts. Game theory can be applied to mitigate the likelihood of attacks such as selfish mining by predicting anomalous behavior and adapting the defense strategies of the other miners in the pool. Such defense approaches should be extrapolated to address other attack types such as Sybil and device spoofing. Although risk assessment has already been conducted for generic cyber applications of blockchain technology [76], a more tailored security risk assessment must be performed in the context of IoT taking into consideration the confluence of its multiple dynamic characteristics such as pervasiveness and cyber-physical operations. Stochastic games for risk modeling under uncertainty can serve as a breeding ground for developing more sophisticated approaches that emphasize the nonlinear, erratic, and unpredictable nature of vulnerability exploitation in networked dynamical systems driven by blockchain.

2) Blockchain architecture: The three types of blockchain including public, private, and consortium can be utilized in blockchain-based IoT systems. However, selecting an appropriate blockchain based on its features, advantages, and drawbacks is challenging. Tran et al. [8] surveyed several positions of blockchain in IoT systems. However, analyzing existing blockchain architectures in terms of performance and security should be considered. In addition, the number of blockchain networks used in the blockchain-based IoT architecture can have a significant impact on the performance of the whole system. Adopting a game-theoretic perspective to perform such an analysis can be a promising direction.

3) Consensus algorithms and energy consumption: Developing optimized consensus algorithms that fit the IoT architecture is another significant issue. For energy-constrained devices, improving consensus algorithms by using practical game-theoretic models can reduce energy consumption. To the best of our knowledge, there is no comprehensive work that compares and analyzes existing consensus algorithms with game theory-based designs in terms of energy consumption, computation, communication, and storage overhead.

C. Limitations of Game-theoretical Design

Incorporating game-theoretic models in blockchain-based IoT may also raise some challenges explained as follows.

1) Implementation: The deployment of game-theoretic models have not yet received its share of attention. In practice, implementing gamified approaches may entail some challenges. For instance, reaching an optimal decision by the IoT nodes may not be straightforward. Since the blockchain is decentralized, there is a large number of distributed nodes that participate in the blockchain network. Therefore, it is challenging to make optimal decisions under incomplete information where leader nodes cannot observe the strategy of the follower nodes. Games that are based on partially-observable environments or the mean-field theory may be explored to cope with large-scale systems. In addition, due to the high computation overhead of game theory-based consensus algorithms, their practicality should be investigated in future research to ensure that deployment challenges can be addressed in practice. Finally, realism can be further improved by reducing the number of abstract game-theoretic parameters and evaluating the game theory-enabled blockchain networks using real measured data and testbeds.

2) Nash equilibrium: Finding Nash equilibrium can be hard in a decentralized system like blockchain, which can have a large number of miners participating in the consensus protocol. IoT nodes have two choices when Nash equilibrium exists, residing in the pool or leaving it. Similarly, the transaction fee may be paid by blockchain users when they choose to withdraw [25]. In Nash equilibrium, players are not willing to deviate from the chosen strategies. However, more than one Nash equilibrium could be reached as the process of finding the best strategy is largely demanding for players [3].

3) Types of game models: This survey discussed several types of game-theoretic models used in blockchain-based IoT. However, selecting an adequate game model that fits the IoT architecture and the various design aspects of the blockchain constitutes a potential research direction. For instance, based on the target application area, designers can choose between simultaneous vs sequential play, as well as cooperative vs non-cooperative games. Nonetheless, we find that dynamic games are well suited to solve many of the challenges discussed in this survey compared to one-shot games. Finally, most existing work has considered security games among mining pools, which might not be fully realistic in pervasive computing systems since the optimal strategy of the individual miner is not necessarily the optimal strategy for the overall pool. Designing a dynamic mean-field game to enable an individual node to make strategic decisions in an iterative fashion as part of the mining pool can be a potential solution. Mean-field game theory provides a powerful mathematical tool for problems with a large number of non-cooperative players. Since the subtle changes among nodes can be negligible if the number of players is sufficiently large, we usually research the epsilon Nash to analyze game stability [77].

V. Conclusion

This timely survey covered the recent research contributions made toward blockchain-based IoT systems using game-theoretical models. While the blockchain has significant advantages in establishing a secure platform for IoT applications, it entails some limitations that need to be emphasized during the design phase. The proposed taxonomy of game theory approaches will allow future researchers to address existing challenges in integrating the blockchain within IoT systems and achieve smarter designs. Moreover, new design problems and solutions will likely emerge and contribute to this roadmap. In

the future, we plan to explore other methodological avenues that will enable system designers to improve the security, efficiency, and management of blockchain platforms.

ACKNOWLEDGEMENT

This research is partially supported by the Natural Sciences & Engineering Research Council of Canada (NSERC).

REFERENCES

[1] 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 Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1676–1717, 2018.

[2] 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 Communications Surveys & Tutorials*, vol. 21, no. 2, pp. 1508–1532, 2019.

[3] Z. Liu, N. C. Luong, W. Wang, D. Niyato, P. Wang, Y.-C. Liang, and D. I. Kim, "A survey on applications of game theory in blockchain," *arXiv preprint arXiv:1902.10865*, 2019.

[4] S. Jiang and J. Wu, "Bitcoin mining with transaction fees: a game on the block size," in *2019 IEEE International Conference on Blockchain (Blockchain)*, pp. 107–115, IEEE, 2019.

[5] A. Kumar and S. Jain, "Proof of game (pog): A game theory based consensus model," in *International Conference on Sustainable Communication Networks and Application*, pp. 755–764, Springer, 2019.

[6] A. Kumar, D. Kumar Sharma, A. Nayyar, S. Singh, and B. Yoon, "Lightweight proof of game (lpog): a proof of work (pow)'s extended lightweight consensus algorithm for wearable kidneys," *Sensors*, vol. 20, no. 10, p. 2868, 2020.

[7] A. Kumar and S. Jain, "Proof of game (PoG): a proof of work (pow)'s extended consensus algorithm for healthcare application," in *International Conference on Innovative Computing and Communications*, pp. 23–36, Springer, 2021.

[8] N. K. Tran, M. A. Babar, and J. Boan, "Integrating blockchain and internet of things systems: A systematic review on objectives and designs," *Journal of Network and Computer Applications*, vol. 173, p. 102844, 2021.

[9] M. A. Ferrag and L. Shu, "The performance evaluation of blockchain-based security and privacy systems for the internet of things: A tutorial," *IEEE Internet of Things Journal*, 2021.

[10] J. Sengupta, S. Ruj, and S. D. Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *Journal of Network and Computer Applications*, vol. 149, p. 102481, 2020.

[11] X. Wang, X. Zha, W. Ni, R. P. Liu, Y. J. Guo, X. Niu, and K. Zheng, "Survey on blockchain for internet of things," *Computer Communications*, vol. 136, pp. 10–29, 2019.

[12] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, p. 21260, 2008.

[13] M. Salimitari and M. Chatterjee, "A survey on consensus protocols in blockchain for iot networks," *arXiv preprint arXiv:1809.05613*, 2018.

[14] L. M. Bach, B. Mihaljevic, and M. Zagar, "Comparative analysis of blockchain consensus algorithms," in *2018 41st International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO)*, pp. 1545–1550, Ieee, 2018.

[15] Z. Zheng, S. Xie, H. Dai, X. Chen, and H. Wang, "An overview of blockchain technology: Architecture, consensus, and future trends," in *2017 IEEE international congress on big data (BigData congress)*, pp. 557–564, Ieee, 2017.

[16] G.-T. Nguyen and K. Kim, "A survey about consensus algorithms used in blockchain," *Journal of Information processing systems*, vol. 14, no. 1, pp. 101–128, 2018.

[17] M. Saad, J. Spaulding, L. Njilla, C. Kamhoua, S. Shetty, D. Nyang, and D. Mohaisen, "Exploring the attack surface of blockchain: A comprehensive survey," *IEEE Communications Surveys & Tutorials*, vol. 22, no. 3, pp. 1977–2008, 2020.

[18] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, "On blockchain and its integration with IoT. challenges and opportunities," *Future generation computer systems*, vol. 88, pp. 173–190, 2018.

[19] S. Roy, C. Ellis, S. Shiva, D. Dasgupta, V. Shandilya, and Q. Wu, "A survey of game theory as applied to network security," in *2010 43rd Hawaii International Conference on System Sciences*, pp. 1–10, IEEE, 2010.

[20] S. Xia, F. Lin, Z. Chen, C. Tang, Y. Ma, and X. Yu, "A bayesian game based vehicle-to-vehicle electricity trading scheme for blockchain-enabled internet of vehicles," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 7, pp. 6856–6868, 2020.

[21] J. Qiu, D. Grace, G. Ding, J. Yao, and Q. Wu, "Blockchain-based secure spectrum trading for unmanned-aerial-vehicle-assisted cellular networks: An operator's perspective," *IEEE Internet of Things Journal*, vol. 7, no. 1, pp. 451–466, 2019.

[22] A. Wilczyński and J. Kołodziej, "Modelling and simulation of security-aware task scheduling in cloud computing based on blockchain technology," *Simulation Modelling Practice and Theory*, vol. 99, p. 102038, 2020.

[23] Y. Liu, F. R. Yu, X. Li, H. Ji, and V. C. Leung, "Decentralized resource allocation for video transcoding and delivery in blockchain-based system with mobile edge computing," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 11, pp. 11169–11185, 2019.

[24] Z. Xiong, S. Feng, D. Niyato, P. Wang, and Z. Han, "Optimal pricing-based edge computing resource management in mobile blockchain," in *2018 IEEE International Conference on Communications (ICC)*, pp. 1–6, IEEE, 2018.

[25] Z. Liu, N. C. Luong, W. Wang, D. Niyato, P. Wang, Y.-C. Liang, and D. I. Kim, "A survey on blockchain: A game theoretical perspective," *IEEE Access*, vol. 7, pp. 47615–47643, 2019.

[26] S.-K. Kim, "Blockchain governance game," *Computers & Industrial Engineering*, vol. 136, pp. 373–380, 2019.

[27] H. Wang, L. Wang, Z. Zhou, X. Tao, G. Pau, and F. Arena, "Blockchain-based resource allocation model in fog computing," *Applied Sciences*, vol. 9, no. 24, p. 5538, 2019.

[28] R. Kovacs, B. Iancu, V. Dadarlat, S. Buzura, A. Peculea, and E. Cebuc, "A collaborative game theory approach for determining the feasibility of a shared as blockchain infrastructure," in *2021 20th RoEduNet Conference: Networking in Education and Research (RoEduNet)*, pp. 1–6, IEEE, 2021.

[29] J. Cheng, L. Xie, X. Tang, N. Xiong, and B. Liu, "A survey of security threats and defense on blockchain," *Multimedia Tools and Applications*, vol. 80, no. 20, pp. 30623–30652, 2021.

[30] D. Xu, L. Xiao, L. Sun, and M. Lei, "Game theoretic study on blockchain based secure edge networks," in *2017 IEEE/CIC International Conference on Communications in China (ICCC)*, pp. 1–5, IEEE, 2017.

[31] I. Eyal and E. G. Sirer, "Majority is not enough: Bitcoin mining is vulnerable," in *International conference on financial cryptography and data security*, pp. 436–454, Springer, 2014.

[32] K. Toda, N. Kuze, and T. Ushio, "Game-theoretic approach to a decision-making problem for blockchain mining," *IEEE Control Systems Letters*, vol. 5, no. 5, pp. 1783–1788, 2020.

[33] R. Singh, A. D. Dwivedi, G. Srivastava, A. Wiszniewska-Matyszkiel, and X. Cheng, "A game theoretic analysis of resource mining in blockchain," *Cluster Computing*, vol. 23, no. 3, pp. 2035–2046, 2020.

[34] I. Eyal, "The miner's dilemma," in *2015 IEEE Symposium on Security and Privacy*, pp. 89–103, IEEE, 2015.

[35] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, p. 21260, 2008.

[36] B. Johnson, A. Laszka, J. Grossklags, M. Vasek, and T. Moore, "Game-theoretic analysis of DDoS attacks against bitcoin mining pools," in *International Conference on Financial Cryptography and Data Security*, pp. 72–86, Springer, 2014.

[37] S. Dey, "Securing majority-attack in blockchain using machine learning and algorithmic game theory: A proof of work," in *2018 10th computer science and electronic engineering (CEEC)*, pp. 7–10, IEEE, 2018.

[38] H. Tan and I. Chung, "Secure authentication and key management with blockchain in vanets," *IEEE access*, vol. 8, pp. 2482–2498, 2019.

[39] L. Cheng, J. Liu, G. Xu, Z. Zhang, H. Wang, H.-N. Dai, Y. Wu, and W. Wang, "SCTSC: A semicentralized traffic signal control mode with attribute-based blockchain in iovs," *IEEE Transactions on Computational Social Systems*, vol. 6, no. 6, pp. 1373–1385, 2019.

[40] A. Taghizadeh, H. Kebriaei, and D. Niyato, "Mean field game for equilibrium analysis of mining computational power in blockchains," *IEEE Internet of Things Journal*, vol. 7, no. 8, pp. 7625–7635, 2020.

[41] X. Chen and X. Zhang, "Secure electricity trading and incentive contract model for electric vehicle based on energy blockchain," *IEEE access*, vol. 7, pp. 178763–178778, 2019.

[42] V. Hassija, V. Chamola, G. Han, J. J. Rodrigues, and M. Guizani, "Dagiov: A framework for vehicle to vehicle communication using directed acyclic graph and game theory," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 4, pp. 4182–4191, 2020.

[43] L. W. Cong, Z. He, and J. Li, "Decentralized mining in centralized pools," *The Review of Financial Studies*, vol. 34, no. 3, pp. 1191–1235, 2021.

[44] H.-N. Dai, Z. Zheng, and Y. Zhang, "Blockchain for internet of things: A survey," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8076–8094, 2019.

[45] Y. Zuo, S. Jin, and S. Zhang, "Computation offloading in untrusted MEC-aided mobile blockchain IoT systems," *IEEE Transactions on Wireless Communications*, 2021.

[46] Z. Xiong, S. Feng, W. Wang, D. Niyato, P. Wang, and Z. Han, "Cloud/fog computing resource management and pricing for blockchain networks," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4585–4600, 2018.

[47] S. Guo, Y. Dai, S. Guo, X. Qiu, and F. Qi, "Blockchain meets edge computing: Stackelberg game and double auction based task offloading for mobile blockchain," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 5, pp. 5549–5561, 2020.

[48] X. Ding, J. Guo, D. Li, and W. Wu, "An incentive mechanism for building a secure blockchain-based internet of things," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 1, pp. 477–487, 2020.

[49] Z. Xiong, Y. Zhang, D. Niyato, P. Wang, and Z. Han, "When mobile blockchain meets edge computing," *IEEE Communications Magazine*, vol. 56, no. 8, pp. 33–39, 2018.

[50] W. Liu, B. Cao, L. Zhang, M. Peng, and M. Daneshmand, "A distributed game theoretic approach for blockchain-based offloading strategy," in *ICC 2020-2020 IEEE International Conference on Communications (ICC)*, pp. 1–6, IEEE, 2020.

[51] W. Guo, Z. Chang, X. Guo, D. N. K. Jayakody, and T. Ristaniemi, "Resource allocation for edge computing-based blockchain: A game theoretic approach," in *2020 IEEE international conference on communications workshops (ICC workshops)*, pp. 1–6, IEEE, 2020.

[52] J. Yuan, Q. Zhao, J. Li, J. Li, Z. Cai, and Y.-T. Chang, "Edge mining resources allocation among normal and gap blockchains using game theory," *The Journal of Supercomputing*, pp. 1–18, 2022.

[53] X. Ding, J. Guo, D. Li, and W. Wu, "Pricing and budget allocation for IoT blockchain with edge computing," *IEEE Transactions on Cloud Computing*, 2022.

[54] X. Yang, G. Wang, H. He, J. Lu, and Y. Zhang, "Automated demand response framework in elns: Decentralized scheduling and smart contract," *IEEE transactions on systems, man, and cybernetics: systems*, vol. 50, no. 1, pp. 58–72, 2019.

[55] H. Yao, T. Mai, J. Wang, Z. Ji, C. Jiang, and Y. Qian, "Resource trading in blockchain-based industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3602–3609, 2019.

[56] A. S. Bataineh, J. Bentahar, O. A. Wahab, R. Mizouni, and G. Rjoub, "A game-based secure trading of big data and iot services: Blockchain as a two-sided market," in *International Conference on Service-Oriented Computing*, pp. 85–100, Springer, 2020.

[57] H. Chen, J. Yu, H. Zhou, T. Zhou, F. Liu, and Z. Cai, "Smartstore: A blockchain and clustering based intelligent edge storage system with fairness and resilience," *International Journal of Intelligent Systems*, vol. 36, no. 9, pp. 5184–5209, 2021.

[58] J. Gao, B. Adjei-Arthur, E. B. Sifah, H. Xia, and Q. Xia, "Supply chain equilibrium on a game theory-incentivized blockchain network," *Journal of Industrial Information Integration*, p. 100288, 2021.

[59] B. Zhang, C. Jiang, J.-L. Yu, and Z. Han, "A contract game for direct energy trading in smart grid," *IEEE Transactions on Smart Grid*, vol. 9, no. 4, pp. 2873–2884, 2016.

[60] J. Li, Z. Zhou, J. Wu, J. Li, S. Mumtaz, X. Lin, H. Gacanin, and S. Alotaibi, "Decentralized on-demand energy supply for blockchain in internet of things: A microgrids approach," *IEEE transactions on computational social systems*, vol. 6, no. 6, pp. 1395–1406, 2019.

[61] 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 transactions on industrial informatics*, vol. 14, no. 8, pp. 3690–3700, 2017.

[62] M. Ali, A. Anjum, A. Anjum, and M. A. Khan, "Efficient and secure energy trading in internet of electric vehicles using IOTA blockchain," in *2020 IEEE 17th International Conference on Smart Communities: Improving Quality of Life Using ICT, IoT and AI (HONET)*, pp. 87–91, IEEE, 2020.

[63] X. Fu, H. Wang, and P. Shi, "A survey of blockchain consensus algorithms: mechanism, design and applications," *Science China Information Sciences*, vol. 64, no. 2, pp. 1–15, 2021.

[64] N. Alzahrani and N. Bulusu, "Towards true decentralization: A blockchain consensus protocol based on game theory and randomness," in *International conference on decision and game theory for security*, pp. 465–485, Springer, 2018.

[65] Y. Wei, L. Liang, B. Zhou, and X. Feng, "A modified blockchain dpos consensus algorithm based on anomaly detection and reward-punishment," in *2021 13th International Conference on Communication Software and Networks (ICCSN)*, pp. 283–288, IEEE, 2021.

[66] L. Di, G. X. Yuan, T. Zeng, Q. Zhang, and X. Zhang, "The existence of consensus equilibria for data trading under the framework of internet of things (IoT) with blockchain ecosystems," *Procedia Computer Science*, vol. 174, pp. 55–65, 2020.

[67] B. N. Alhasnawi, B. H. Jasim, B. E. Sedhom, and J. M. Guerrero, "Consensus algorithm-based coalition game theory for demand management scheme in smart microgrid," *Sustainable Cities and Society*, vol. 74, p. 103248, 2021.

[68] Y. Jiang, Y. Zhong, and X. Ge, "IIoT data sharing based on blockchain: a multi-leader multi-follower stackelberg game approach," *IEEE Internet of Things Journal*, 2021.

[69] C. Zhang, T. Shen, and F. Bai, "Toward secure data sharing for the iot devices with limited resources: A smart contract–based quality-driven incentive mechanism," *IEEE Internet of Things Journal*, 2022.

[70] F. Bai, T. Shen, Z. Yu, K. Zeng, and B. Gong, "Trustworthy blockchain-empowered collaborative edge computing-as-a-service scheduling and data sharing in the IIoE," *IEEE Internet of Things Journal*, 2021.

[71] H. Si, C. Sun, Y. Li, H. Qiao, and L. Shi, "Iot information sharing security mechanism based on blockchain technology," *Future generation computer systems*, vol. 101, pp. 1028–1040, 2019.

[72] R. Akkaoui, X. Hei, and W. Cheng, "An evolutionary game-theoretic trust study of a blockchain-based personal health data sharing framework," in *2020 Information Communication Technologies Conference (ICTC)*, pp. 277–281, IEEE, 2020.

[73] S. Jiang and J. Wu, "Game theoretic storage outsourcing in the mobile blockchain mining network," in *2020 IEEE 17th International Conference on Mobile Ad Hoc and Sensor Systems (MASS)*, pp. 300–308, IEEE, 2020.

[74] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, "Eclipse attacks on bitcoin's peer-to-peer network," in *24th {USENIX} Security Symposium ({USENIX} Security 15)*, pp. 129–144, 2015.

[75] Y. Wang, C. Tang, F. Lin, Z. Zheng, and Z. Chen, "Pool strategies selection in pow-based blockchain networks: Game-theoretic analysis," *IEEE Access*, vol. 7, pp. 8427–8436, 2019.

[76] S. Feng, W. Wang, Z. Xiong, D. Niyato, P. Wang, and S. S. Wang, "On cyber risk management of blockchain networks: A game theoretic approach," *IEEE Transactions on Services Computing*, vol. 14, no. 5, pp. 1492–1504, 2018.

[77] J.-M. Lasry and P.-L. Lions, "Mean field games," *Japanese journal of mathematics*, vol. 2, no. 1, pp. 229–260, 2007.