IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received May 30, 2019, accepted June 17, 2019, date of publication June 26, 2019, date of current version July 16, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2925010

Proof-of-Stake Consensus Mechanisms for Future Blockchain Networks: Fundamentals, Applications and Opportunities

CONG T. NGUYEN[1], DINH THAI HOANG[2], (Member, IEEE), DIEP N. NGUYEN[2], (Senior Member, IEEE), DUSIT NIYATO[3], (Fellow, IEEE), HUYNH TUONG NGUYEN[1], AND ERYK DUTKIEWICZ[2], (Senior Member, IEEE)

[1]Ho Chi Minh City University of Technology, VNU-HCM, Ho Chi Minh City 70000, Vietnam
[2]University of Technology Sydney, Sydney, NSW 2007, Australia
[3]Nanyang Technological University, Singapore 639798

Corresponding author: Dinh Thai Hoang (hoang.dinh@uts.edu.au)

This work was supported in part by the Joint Technology and Innovation Research Centre—a partnership between the University of Technology Sydney and the VNU Ho Chi Minh City University of Technology (VNU HCMUT).

ABSTRACT The rapid development of blockchain technology and their numerous emerging applications has received huge attention in recent years. The distributed consensus mechanism is the backbone of a blockchain network. It plays a key role in ensuring the network's security, integrity, and performance. Most current blockchain networks have been deploying the proof-of-work consensus mechanisms, in which the consensus is reached through intensive mining processes. However, this mechanism has several limitations, e.g., energy inefficiency, delay, and vulnerable to security threats. To overcome these problems, a new consensus mechanism has been developed recently, namely proof of stake, which enables to achieve the consensus via proving the stake ownership. This mechanism is expected to become a cutting-edge technology for future blockchain networks. This paper is dedicated to investigating proof-of-stake mechanisms, from fundamental knowledge to advanced proof-of-stake-based protocols along with performance analysis, e.g., energy consumption, delay, and security, as well as their promising applications, particularly in the field of Internet of Vehicles. The formation of stake pools and their effects on the network stake distribution are also analyzed and simulated. The results show that the ratio between the block reward and the total network stake has a significant impact on the decentralization of the network. Technical challenges and potential solutions are also discussed.

INDEX TERMS Blockchain, consensus mechanisms, energy, game theory, proof-of-stake, proof-of-work, security, and mining process.

I. INTRODUCTION

Over the last few years, blockchain technology has been proclaimed by many as the most significant technological breakthrough since the invention of the Internet. A blockchain is a distributed database of records shared among network participants. With the help of cryptographic hash functions, digital signatures, and distributed consensus mechanisms, once a record enters the database, it cannot be altered without the consensus of the other network participants [1]. As a result, data stored in a blockchain can be conventionally verified even in a decentralized environment, which leads to numerous blockchain applications. Cryptocurrencies, the most famous blockchain applications, have the total market capitalization of more than $200 billion by the time this article is written, with more than 2000 cryptocurrencies networks [2]. Beyond cryptocurrencies, blockchain applications have also been emerging in various areas, such as finance, healthcare, military, and Internet-of-Things (IoT) networks [4].

In this paper, we first provide an overview of blockchain technology including basic concepts, operations, benefits, and applications. We then briefly present the consensus mechanisms and discuss the Proof-of-Work (PoW) mechanism together with its existing issues. After that, we introduce the key emerging Proof-of-Stake (PoS) consensus

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

mechanisms, such as Ouroboros, Chains-of-Activity, Casper, Algorand, and Tendermint. For each mechanism, we present the operation, analyze security and energy efficiency, and evaluate performance through comparisons with other protocols. We also present several notable blockchain-based Internet-of-Vehicles networks, where the PoS mechanisms are being used as the backbone of their operations. Then, we discuss and analyze stake pools in a PoS-based network as well as impacts of factors to the decentralized strategies of stakeholders through using a non-cooperative game model. In particular, we first formulate the stake competition problem among the stakeholders in the PoS-based blockchain network as a non-cooperative game. In this game, each player (i.e., a stakeholder, e.g., RSU, in the IoV networks) acts independently to maximize the profit which is affected by the actions of all players. We then prove that this game has a unique Nash equilibrium and the convergence to the Nash equilibrium is guaranteed. We also prove that the Nash equilibrium of this game is Pareto optimal. They are very important features of this game which are crucial to help the PoS-blockchain network provider as well as stake pools to design suitable parameters (e.g., total network stakes, rewards, and so on). These features are also very important to encourage stakeholders to participate in and contribute to the PoS-based blockchain network. Finally, we present some challenges for the development of future PoS-based blockchain networks and propose several potential solutions.

The rest of this paper is organized as follows. We first provide a brief overview of blockchain technology and consensus mechanisms in Section II. We then focus on emerging PoS-based protocols in Section III and introduce some applications of PoS in Internet-of-Vehicles networks in Section IV. After that, Section V introduces the case study to examine the interrelations and impacts of network parameters to the PoS-based blockchain networks. Finally, challenges and potential solutions are discussed in Section VI, and conclusions are given in Section VII.

II. OVERVIEW OF BLOCKCHAIN NETWORKS AND CONSENSUS MECHANISMS

A. FUNDAMENTAL BACKGROUND AND APPLICATIONS OF BLOCKCHAIN NETWORKS

1) BLOCKCHAIN NETWORKS

As illustrated in Fig. 1, in the blockchain, transactions (data) are stored in blocks which form an ever-growing sequence (chain) shared among participants in the network. Transactions are the fundamental units of a blockchain. For example, when Alice wants to send money to Bob, she creates a transaction which consists of her address as the input, her digital signature to verify that this transaction is made by her, the amount of money to be sent, and Bob's address as the output. Alice then broadcasts this transaction to the network. A miner, i.e., a consensus participant, after receiving the transaction will validate and include Alice's transaction, along with other transactions received from other users, into a block. If the block is mined successfully, the miner will broadcast the block to the network for other nodes to verify the mined block. If this block is verified successfully and identified to be the first block mined after the last block in the chain, it will be integrated into the chain and marked as the latest block in the chain. Besides the transactions, a block also contains a hash pointer created by hash functions to map all the block contents to the hash pointer. The main feature of the hash functions is to ensure that the chain is tamper-evident. It means that any change in the previous data will result in a different hash value in the next block, and it can be traced back to the genesis block, i.e., the first block of the chain. A block can also contain additional data depending on requirements of different consensus mechanisms. To reduce storage space, the transactions in a block can be stored in the form of a Merkle tree [1].

2) BENEFITS AND APPLICATIONS

Although blockchain technology attracts a lot of attention due to the successful implementation of cryptocurrencies, its benefits extend far beyond. The key benefits of blockchain technology are as follow:

- *Decentralization:* Blockchain networks are not controlled by a central controller. Thus, they do not have any single point of failure. Instead, all the nodes reach the agreement on the state of the network by participating in the distributed consensus mechanisms.
- *Transparency:* Data stored in a blockchain is visible to all network participants.
- *Immutability:* Once the data are stored in the blockchain, it is extremely difficult to be altered. Moreover, thanks to the distributed consensus mechanisms, the network can achieve consensus on the data even in a trustless environment.
- *Security and Privacy:* Using cryptographically secure mechanisms, the privacy and security of the network participants can be significantly enhanced. Users in the network use a pair of public and private keys for identification and verification. When a user makes a transaction, a digital signature is used, which can be easily verified but impossible to forge.

Given the aforementioned outstanding benefits, blockchain technology has many applications in a number of areas. Some major applications of blockchain technology are as follow:

- *Cryptocurrencies:* Cryptocurrencies, e.g., Bitcoin [39], Ethereum [40], Cardano [22], are the most famous applications of blockchain technologies. With high value and daily trade volume, cryptocurrencies can be utilized for various financial applications, such as digital assets and online retail.
- *Internet-of-Things (IoT) network:* Its anonymity and security make blockchain applicable to many IoT networks, e.g., Internet-of-Vehicles [32]–[35], energy trading [41], [42], electric vehicle charging [43], and smart home [44], for operations management, trading automation, and security enhancements.

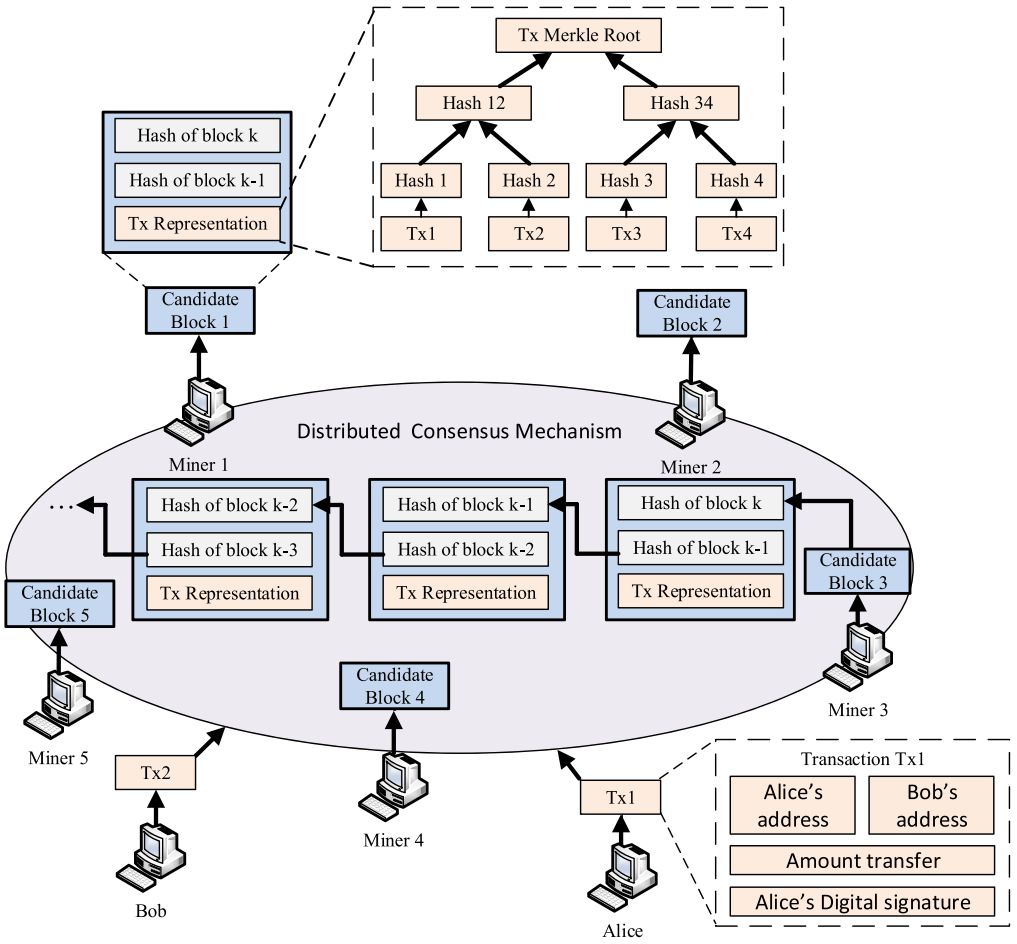

FIGURE 1. An illustration of a blockchain network.

- *Healthcare:* Blockchain technologies have been adopted by many healthcare systems to enhance the privacy of patient data [45], improve interoperability across devices [46], and maintain an immutable decentralized database of medical records [47].
- *Military:* Blockchains have the potential to be applied in various military operations, such as enhancing data integrity in supply chain management, ensuring transparency in equipment management [48], and providing a distributed and decentralized database for military intelligence [49].
- *Service providers:* Blockchain networks have also been employed by many service providers. Blockchain technology can support automatic payments, contents distribution, and services delivery [50], [51].

B. CONSENSUS MECHANISMS

Nodes in a blockchain network can be faulty, performing arbitrary or malicious behaviors, or possessing misinformation due to connection latency, i.e., Byzantine failures. The consensus mechanism is thus the core component of a blockchain network, which ensures that every participant agrees on the state of the network in such trustless environments. The consensus mechanism also governs other operations of the network, such as transaction adding and incentivizing the participants to behave properly.

1) PROOF-OF-WORK

Early blockchain networks were developed based on Proof-of-Work (PoW) mechanism. Generally, the nodes in a PoW-based blockchain network reach consensus by participating in a solution searching process, where each node must find a nonce for its proposed new block. When the nonce, the previous blocks hash, and the transactions in the new block are used as the input of the hash function, e.g., SHA-256, the hash function output must be in a target range so that the block can be accepted. Due to the property of the hash function, the nonce can only be found by repeatedly trying different nonce values until the output is within the target range. When a participant finds the nonce, it will

broadcast the block along with the transactions to other nodes. Then, if the new block is verified and determined to be the first block mined after the last block in the chain, it will be integrated into the current chain and become the latest block in the chain.

In PoW, the participants compete with each other to be the first to find the correct nonce. This solution searching procedure can be considered to be a weighted random coin-tossing process where a participant with a higher hash rate (computational power) might have higher chances to be the block winner (leader) who can receive the reward. The probability p_i that participant i is selected to be the leader in a network of N participants is

$$p_i = \frac{c_i}{\sum_{j=1}^{N} c_j}, \tag{1}$$

where c_i is the hash rate of participant i. This computation leads to the large amount of energy consumption for blockchains using PoW consensus mechanisms, as the participants try to increase their hash rates to have a higher chance to be the leader and receive rewards. Moreover, since participants with low hash rates have very low chances to win a block and receive rewards, they often join mining pools to have more opportunities to get revenues. A mining pool consists of participants who want to collaborate by contributing their computing resources to the pool. In this way, mining tasks will be distributed to the miners, and due to huge computing resources, mining pools often get much higher opportunities to win a new block than individuals. While joining a mining pool provides more stable incomes, the nodes in the pool often do not contribute to the transaction validation and propagation since they only perform the nonce search process in a specific range. Thus, mining pools have been dominating processes making new blocks in most of current blockchain networks. For example, the top five mining pools control up to 62.7% total hash rate of the Bitcoin network [3]. This is the most serious issue of PoW-based blockchain networks because it is against the decentralized spirit of blockchain technology. Another issue of PoW protocols is delay. In a PoW-based blockchain network, when a block is added to the chain, there is still a possibility that this block will not be included in the main chain for several reasons, e.g., network delay causing several versions of the chain or two participants finding two blocks simultaneously. This possibility decreases exponentially as the block is deeper in the chain. Therefore, a block is considered to be finalized only when it is a certain k, usually six blocks deep in the chain. This delays the transaction confirmation significantly. Moreover, PoW mechanism is also vulnerable to 51% attack. In particular, if a single party controls more than 51% of the network's total computational power, they can spend their coins multiple times (in cryptocurrency networks) or prevent other transactions by adding conflicting blocks to the chain. While 51% attacks might not be a serious problem for large blockchain networks, the newly established networks with small and limited total computational power are especially vulnerable [4].

2) PROOF-OF-CONCEPTS

Based on the PoW framework, the Proof-of-Concepts (PoX) consensus mechanisms have been developed with two major aims: to replace the PoW solution searching with useful calculations and to improve the performance of PoW in terms of security, incentives, and resource usage. To make better use of the computational resource, several consensus mechanisms require the participants to solve practical mathematical problems such as searching for three types of prime number chains in Primecoin [6], solving matrix product problems in Proof-of-Exercise [7], and calculating useful functions in Proof-of-Useful-Work [8]. Other PoX consensus mechanisms are designed for distributed data storage service such as Permacoin [9], KopperCoin [10], and Filecoin [11]. Generally, these consensus mechanisms divide the data files into segments and distribute them to multiple participants in the network. To participate in the mining process, the nodes have to provide proofs of storage, and the more storage volume a node offers, the better chances it is selected to be a leader.

Other PoX consensus mechanisms have been developed with the aim to improve the performance of PoW. The problem of mining pool formation is addressed by designing nonoutsourceable puzzles to replace the PoW solution searching process, such as in [12] and [13]. In these networks, the solution searching processes financially disincentivize mining pools formation because the node who found the solution can steal the reward. Other consensus mechanisms have been developed to reduce the computational requirement of PoW. The Spacemint [14] network employs a Proof-of-Space protocol, in which the consensus nodes must provide proof of storage when participating in the solution searching process. Different from [9]–[11], the stored files are not useful and only serve as proofs. Nevertheless, this is still beneficial as storing a large file consumes negligible energy compared to nonce searching. In Proof-of-Human-Work protocol [15], the Completely Automated Public Turing-Test to tell Computers and Humans Apart (CAPTCHA) is employed to involve human activities and reduce computational requirements in the solution searching process.

3) PROOF-OF-STAKES

The first Proof-of-Stakes (PoS) network, Peercoin [16], was developed as a PoX consensus mechanism with the aim to reduce the computational requirements of PoW. Participants with higher coin age, i.e., product of network tokens and their holding time, have higher chances to be selected. Specifically, each node in Peercoin solves a PoW puzzle with its own difficulty, which can be reduced by consuming coin age. In the more recent PoS networks, the solution searching is completely removed, and the block leaders are no longer selected by computational power. Instead, they are selected based on the stakes that they are holding.

TABLE 1. Consensus mechanisms comparisons.

	PoW	PoS	Hybrid
Leader selection	Based on hash rate	Based on stake	Depends on variant
Energy consumption	Significant	Negligible	Medium to negligible
Hardware requirement	High	None	Medium to none
Block generation speed	Slow	Fast	Medium to high
Transaction confirmation speed	Slow	Fast	Medium to high
Applications	Bitcoin, Ethereum, etc.	Cardano, Algorand, etc.	Casper, Peercoin, etc.

With the stake-based leader selection process, a node's chance to be selected to be a leader no longer depends on its computational power, and thus energy consumption of PoS mechanisms is significantly reduced compared with that of PoW. Moreover, the block generation and transaction confirmation speeds are kept at relatively low constant rates by the PoW networks to ensure security because there are many different blocks proposed by the miners. In contrast, since only one block is made in each round of PoS mechanisms, the block generation and transaction confirmation speeds are usually much faster, and thus PoS mechanism starts to become popular recently. In this paper, the PoS mechanisms are discussed comprehensively in Section III.

4) HYBRID CONSENSUS MECHANISMS

Aiming to reduce the high resources consumption of PoW, early PoS-based protocols are developed from standard PoW consensus mechanisms, and thus still incorporate some PoW elements, which makes hybrid PoW-PoS protocols. The Peercoin protocol discussed above can be considered to be a hybrid consensus mechanism, which utilizes PoS to reduce the high computational requirement of PoW. Another typical example is the Proof-of-Activity (PoA) protocol [17], which employs the PoW to create empty blocks and the PoS to verify blocks and add transactions. Based on the PoA, the Snow White protocol [18] was developed in which the main difference is that PoS is employed first to choose a number of candidates. These candidates then compete with each other via the PoW to create blocks.

Other hybrid consensus mechanisms often elect a committee to verify blocks and confirm transactions. The Hybrid Consensus protocol periodically elects a committee based on the hashes of previous blocks to add and confirm transactions. The Peercensus protocol [19] selects committee members from the previous block creators. Different from the Hybrid Consensus protocol [20], the committee is responsible for both transaction adding and block confirmation in the Peercensus protocol.

The hybrid protocols inevitably inherit the strength and weakness of the consensus mechanisms that they are created from to some extent. Typically, the energy consumption of these consensus mechanisms is lower than that of the PoW, but it is still higher than that of pure PoS protocols. In addition, the block generation and transaction confirmation speeds are also higher than those of PoW due to their usage of PoS and voting committee. The major differences between the protocols can be found in Table 1.

III. PROOF-OF-STAKE-BASED MECHANISMS

A. PROOF-OF-STAKE: FUNDAMENTAL BACKGROUND

Proof-of-Stake (PoS) protocols were developed as energy-saving alternatives to PoW. Instead of computational power resources, leaders are selected based on their stakes, i.e., contributions to the blockchain network. Particularly in the PoS consensus mechanism, the stake of a node is the number of digital tokens, e.g., coins in cryptocurrencies, that it holds or deposits. Instead of consuming a lot of energy for the searching process as in the PoW, a leader will be selected based on its stakes to perform mining process and add a new block to the chain as illustrated in Fig. 2. To simulate the stake-based leader selection process, the Follow-the-Satoshi (FTS) algorithm has been adopted in many PoS-based blockchain networks such as Cardano, Sp8de, and Tezos. In these networks, all the tokens are indexed. The FTS algorithm is a hash function that takes a seed (i.e., a string of arbitrary length such as the previous block's header or a random string created by some other selected nodes) as the input. The FTS algorithm then outputs a token index. Using the index, the algorithm searches the transaction history to find and select the current owner of that token to be the leader. Therefore, the probability p_i that node i is selected to be the leader in a network of N participants is

$$p_i = \frac{s_i}{\sum_{j=1}^{N} s_j}, \tag{2}$$

where s_i is the stake of participant i. This means that the more stake a node holds, the higher chance it is selected to be the leader.

Besides the advantage of low energy consumption, the PoS mechanisms have faster transaction confirmation speed than that of the PoW mechanisms. In a blockchain network, the confirmation of a transaction depends on two main factors, namely transaction throughput and block confirmation time. The transaction throughput is the number of transactions per second Tx/s a network can process, which is vital to the performance of the network especially when there are many pending transactions. Tx/s can be calculated by

$$Tx/s = \frac{Block_{size}}{Tx_{size} \times Block_{time}}. \tag{3}$$

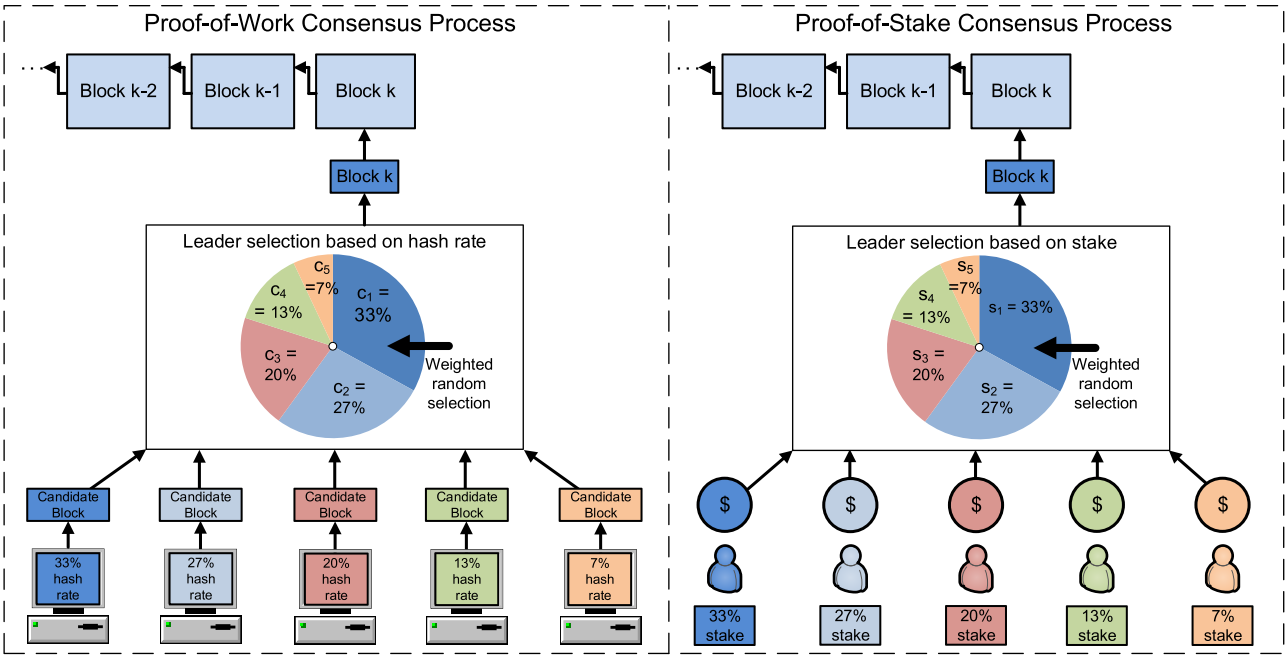

FIGURE 2. PoW and PoS consensus mechanisms comparison.

For example, the Bitcoin network has $Block_{size} = 1\ MB$, $Tx_{size} = 250\ bytes$, and $Block_{time} = 600s$, so it can process around 7 transactions per second. The Tx/s determines how quickly a transaction is added to the chain, whereas the block confirmation time dictates how fast the transaction is confirmed after it is added. The block confirmation time depends on $Block_{time}$, i.e., the average time it takes for a new block to be added to the chain, and the finality of the consensus mechanisms. In the Bitcoin network, a transaction usually has to wait for $k = 6$ blocks before it can be confirmed, so the average confirmation time is $k \times Block_{time} = 3600s = 1hr$. Typically in PoS networks, the block size is larger, and the block time is much shorter, thus the transaction throughput is much higher, e.g., up to 875 Tx/s in [29]. Moreover, some PoS networks can achieve immediate finality, i.e., $k = 1$, so their transaction confirmation time is significantly shorter, e.g., down to 1 second in [30]. Similar to PoW, some PoS protocols such as [16]–[18], [21], [25], [28] adopt the longest chain rule which ensures that when there are multiple versions of the chain (forks), the honest participants will only adopt the longest fork. As a result, the finality in these protocols is delayed. In contrast, protocols such as [29], [30] can achieve immediate finality by voting to confirm block after each round.

The security of PoS protocols depends on various factors. Among them, network synchrony is crucial to the security of many PoS protocols because the leader selection processes are simulated by voting rounds, where the voters send their votes to other participants. Since the network cannot guarantee that all the messages are properly sent in practice due to network delay and connection complexity, network synchrony has to be taken into account when considering the protocol's security. Some PoS protocols are proven to be secure as long as the network is partially synchronous, where messages sent will reach their destinations within a certain time limit, or asynchronous, i.e., messages may not reach their destinations.

Apart from the network synchrony, the incentive mechanism is also vital to the security of a PoS consensus mechanism. On the one hand, the reward scheme has to incentivize consensus participation by rewarding block creators and validators. On the other hand, it also has to penalize malicious behaviors and prevent various attacks that specifically target PoS, such as the attacks that involve creating a large number of blocks because it is much easier to create blocks in PoS. The PoS protocols often have both reward and penalty mechanisms, such as [25], [28], [30].

Below, we discuss in more details some emerging PoS-based protocols which have been widely implemented in practice, namely Ouroboros, Chains-of-Activity, Casper, Algorand, and Tendermint. Their core components, namely the consensus processes, are illustrated in Fig. 3, and the protocols are then compared in Table 2.

B. OUROBOROS

Ouroboros [21] is a pure stake-based protocol, which employs a dynamic committee selected based on the stake distribution. The protocol divides time into epochs. In each epoch, the committee members participate in a 3-phased coin-tossing protocol to create the seeds for the FTS algorithm.

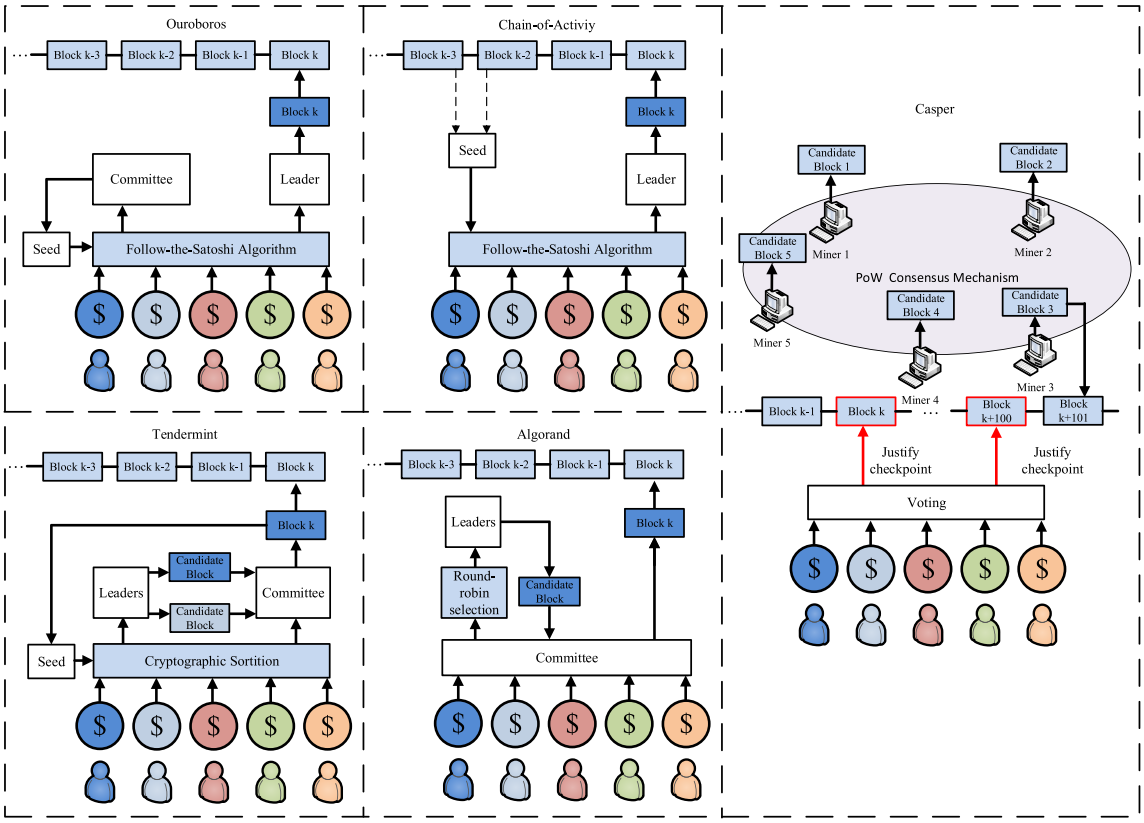

FIGURE 3. Illustrations of several PoS consensus processes.

The FTS algorithm then outputs some coin indices, and the current owners of the chosen coins are selected to be the leaders and become the committee members in the next epoch. Different from PoW protocols, in Ouroboros the leaders only create empty blocks. The input endorsers are responsible for confirming and adding the transactions to the blocks. The block rewards are shared between the committee members, the leaders, and the input endorsers to encourage participation in the consensus process. A stake delegation mechanism, i.e., stakeholders can delegate their right to participate in the committee, is also incorporated to incentivize small stakeholders to contribute to the consensus processes.

Under a partial synchrony network assumption, Ouroboros is proven to be safe when the adversary controls strictly less than 51% of the total stake. Since partial synchrony cannot be guaranteed in practice, Ouroboros considers the asynchronous nodes to be a part of the adversary nodes. The dynamic stake distribution is also taken into account and incorporated into the adversary's stake. It was also shown in [21] that the seed creation process cannot be biased by the adversary, and thus grinding attack, i.e., the block proposers may try different block's hash in the attempt to influence the next leader selection round, is mitigated. The attacks where the adversary secretly builds alternative forks to later overtake the main chain, e.g., nothing-at-stake attack and long-range attack, are mitigated by having only one designated leader in each round. The incentive mechanism is also analyzed in the paper, and being honest is proven to be a δ-equilibrium strategy for the participants. However, the protocol still cannot withstand 51% attacks, and bribe attacks are not formally discussed.

Ouroboros has the advantages of low transaction confirmation time, e.g., 2 minutes [22], and high transaction throughput, e.g., around 257 Tx/s [23]. Moreover, because only the chosen leaders can create blocks in Ouroboros, energy consumption is negligible compared with those of PoW-based networks. Another advantage of Ouroboros over many protocols, including some PoS protocols, is that it has formal definitions and strong theoretical background to support its security and incentive compatibility. As a result, Ouroboros has been adopted by several cryptocurrencies, such as Cardano (https://www.cardano.org) and Sp8de (https://sp8de.com).

C. CHAINS-OF-ACTIVITY

Similar to Ouroboros, in the Chains-of-Activity (CoA) protocol [25], the leader is selected by the FTS algorithm. However, the seed for the FTS algorithm is different from Ouroboros. In CoA, the chain is divided into groups of blocks of length l, and time is divided into epochs such that in each epoch, exactly l blocks are added to the chain. The hash of each block is used to determine a seed of that block. The seeds

TABLE 2. Summary of PoS-based protocols.

Protocol	Ouroboros [21]	Chains-of-Activity [25]	Casper [28]	Algorand [29]	Tendermint [30]
Type	PoS	PoS	PoS-PoW hybrid	PoS	PoS
Consensus Process	-Dynamic committee -Leader selection by 3-phased coin-tossing protocol -Utilize FTS algorithm	-Leader selection by stake and previous blocks -Utilize FTS algorithm	-Leader selection by PoW -Validators vote via BFT protocol to justify the checkpoint blocks.	-Dynamic committee -Leader selection based on stake -Utilize VRF	-Leader selection by round-robin selection -Validators vote to confirm blocks.
Transaction Adding	Input endorsers	Block creator	Block creator	Block creator	Block creator
Incentive Mechanism	Rewards are divided between the slot leaders and the input endorsers	-Leader collect reward -Leader's deposit will be confiscated for malicious behaviors.	Deposit is confiscated for malicious behaviors.	Undefined	-Rewards divided between validators. -Deposit is confiscated for malicious behaviors
Network Synchrony	Partial Synchrony	Undefined	Partial Synchrony	Asynchronous period in between synchronous periods	Partial Synchrony
Adversary Toleration	$1/2$	Undefined	$1/3$	$1/2$	$1/3$
Security issues	51% attack, bribe attack	Ignore adversary toleration, network synchrony, and dynamic stake distribution	Depends on underlying chain	Ignore incentive compatibility	-Ignore dynamic stake distribution -Leader selection is not clearly defined
Finality	Delayed	Delayed	Delayed	Immediate	Immediate
Transaction confirm	2 minutes	6 minutes	Depends on underlying chain	20 seconds	1 second
Transaction throughput	257 Tx/s	40 Tx/s	Depends on underlying chain	875 Tx/s	800 Tx/s
Applications	Cardano, Sp8de	Tezos	Ethereum (planned)	Algorand, Arcblock	BigchainDB, Ethermint

of all the blocks created in an epoch are combined to seed the FTS algorithm for determining the next epoch's leaders. At each round in an epoch, a leader is selected by the FTS algorithm to collect transactions and create a new block. The selected leader has to make a deposit before creating a block. The block reward can be claimed by the leader if the block is created properly, and the deposit will be confiscated in cases of malicious behavior. The CoA protocol also introduces the checkpoint blocks, i.e., the blocks that extend the chain by exactly T blocks, to solidify the chain and prevent long adversarial forks from taking over.

The CoA protocol is proven to be secured against a number of attacks. By seeding the FTS algorithm with hashes from the previous group of blocks, the protocol can effectively mitigate grinding attacks. Similar to the Ouroboros protocol, there is only one designated leader to create a block in each round. Thus, nothing-at-stake and long-range attacks are mitigated. Long-range attack is an attack that specifically targets the protocols where the leaders are determined before their designated epoch. In these protocols, after realizing that they are going to be leaders in the next epoch, the stakeholders might sell their stakes, so that they can behave maliciously without consequences. With the checkpoint blocks mechanism, every block from the first block to the second most recent checkpoint block can never change, and thus long-range attack is mitigated by the CoA protocol. The deposit scheme helps to prevent double-spending attacks, where the attackers create conflicting blocks to revert confirmed transactions, and bribe attacks, where the attackers bribe the leaders to conduct double-spending attacks.

In the CoA protocol, there is only one block created at each round, and thus energy consumption is small compared with that of the PoW mechanisms. CoA also has low transaction confirmation time, around 6 minutes [26], and high transaction throughput, $40Tx/s$ [27]. However, the incentive compatibility is not formally analyzed, and the network synchrony and adversary toleration threshold, which is crucial to the network security, are completely ignored in the paper. The cryptocurrency Tezos (https://tezos.com) is designed partially based on the CoA protocol.

D. CASPER

The Casper protocol [28] was developed by the Ethereum network in an attempt to ease the transition from the current PoW protocol to a pure PoS protocol, i.e., it can work on top of existing PoW protocols. In this context, Casper does not interfere with the leader selection process. Instead, it employs a dynamic committee, which votes via a Byzantine-Fault-Tolerance (BFT) protocol to justify the checkpoint blocks at every fixed interval, e.g., every 100 blocks. Every block up to the second latest justified checkpoint is considered to be finalized. To join the committee, a validator has to make a deposit to gain voting right proportional to that deposit, which will be slashed for malicious behaviors.

Casper is proven to be secure as long as 2/3 of the voting power is controlled by honest validators in a partially synchronous network. By incorporating a withdrawal delay, i.e., the validator has to wait for a long period of time before the deposit can be withdrawn, the protocol can handle dynamic stake distribution and long-range attack. The other security issues are implied to be handled by the underlying chain.

Another advantage of Casper is that it can work on top of other PoW protocols, thereby providing additional security to the underlying chain. However, Casper's performance relies on the underlying PoW mechanism. In addition, another issue is that the incentive mechanism is undefined in the paper, despite its key roles in ensuring the participants follow the protocol properly. Ethereum (https://www.ethereum.org) has been developing Casper, and it is expected to be implemented for future PoW-based blockchain protocols.

E. ALGORAND

Similar to Ouroboros, the Algorand [29] protocol also operates under a committee. However, the protocol uses a cryptographic sortition mechanism instead of the FTS algorithm to select the leaders and committee members based on the stake distribution. The cryptographic sortition [29] is a Verifiable Random Function (VRF) that takes a private key of a consensus node and a seed as inputs and outputs a hash and a proof for public verification. Each consensus node is assigned a range of hash values proportional to its stake amount. If the hash is within a node's assigned range, the node is selected, and thus the node's chance to be selected is directly proportional to its stake amount. The main difference between the cryptographic sortition mechanism and the FTS algorithm is that with cryptographic sortition, the selected node is not revealed until it submits the proof, and thus the node will not be targeted in advance by the adversaries. The initial seed for the VRF is generated at the beginning using distributed random number generator and subsequently used to create a new seed via VRF for the next round. The protocol also does not rely solely on the leader selection process for security. The committee is responsible for voting blocks which will be added to the chain in each round, meaning that the block is immediately finalized.

Algorand can operate for an asynchronous period, as long as they are followed by a synchronous period. Under this assumption, Algorand is proven to be safe as long as 51% of the total stake is controlled by honest participants. Because the committee votes to finalize every block, i.e., there is no fork, many attacks associated with forks, e.g., double-spending, long-range, nothing-at-stakes, and bribe attacks, are mitigated. By using a node's private key and the seed as inputs, and distributing the private key in advance of the seed, grinding attack is mitigated as the adversary needs to influence the leader selection process at the same time.

Although there is more than one block created at each round in Algorand, the number of blocks created is still small, and the participants do not compete in hash rate to create blocks. Thus, the energy consumption of the Algorand protocol is low compared to that of the PoW mechanisms. Moreover, Algorand has a high transaction throughput, up to 875 Tx/s [29]. The protocol also has a significant advantage over many other PoS and PoW protocols since it provides immediate finality, i.e., the blocks and transactions are immediately finalized, and thus the transaction confirmation time is much faster, e.g., around 20 seconds [29], than those of the protocols adopting the longest chain rule such as Ouroboros and PoW protocols. However, similar to Casper, a significant issue is that the incentive mechanism is undefined in the paper. Algorand is currently adopted by several cryptocurrencies, including Algorand (https://www.algorand.com) and Arcblock (https://www.arcblock.io).

F. TENDERMINT

The Tendermint protocol [30] employs the BFT voting protocol for block confirming. In Tendermint, the validators gain the right to vote by making a deposit. A proposer is selected from the validators based on their voting right to propose a block and include transactions in each round via a deterministic round-robin selection scheme. Similar to Algorand, the validators vote to confirm the proposed blocks in Tendermint, and thus blocks and transactions are immediately finalized. The block rewards are distributed among validators to incentivize consensus participations, and the deposits are confiscated for malicious behaviors.

Under the assumption of partial synchrony network, Tendermint is proven to be secure as long as 2/3 of the voting power is controlled by honest participants. Similar to Algorand, there is no fork in Tendermint, and thus fork related attacks are mitigated. However, the round-robin leader selection scheme is not clearly defined. The dynamic stake distribution is also ignored in the paper.

The energy consumption of the Tendermint protocol is low compared to PoW mechanisms because there is only one block created in each round. Similar to Algorand, Tendermint has high transaction throughputs, e.g., up to 800 Tx/s, and low transaction confirmation time, e.g., 1 second on average [31], due to the blocks being immediately finalized. Although proven to be secure against several types of attacks, the protocol generally lacks

formal definitions and theoretical background, and the incentive mechanism is not analyzed. Currently, Tendermint has several applications in practice, such as BigchainDB (https://www.bigchaindb.com), a blockchain database, and Ethermint (https://ethermint.zone), a cryptocurrency network.

IV. APPLICATIONS OF POS CONSENSUS MECHANISMS TO INTERNET-OF-VEHICLES NETWORKS

The rapid development of the Internet-of-Things and networking technologies has driven the automotive industry towards smart vehicles with sensing and communication abilities, which in turns necessitates a platform for data communicating and processing, i.e., Internet-of-Vehicles (IoV) networks. In these networks, a huge amount of data is communicated among the network nodes, e.g., vehicles, road-side units (RSUs), to improve transport safety and service qualities. However, the development of IoV faces critical security and privacy issues. IoV networks often rely on centralized authorities, which can become the single point of failure due to cyber attacks, capacity limitations, or malfunctioning. Moreover, since the vehicles continuously leave and join the network, it is difficult to establish trusts among network participants, and thus data privacy becomes a significant issue.

With the benefits of decentralization, security, and privacy, blockchain technology is a promising solution for the issues the IoV networks are facing. While the asymmetric keys and digital signatures enhance the privacy and security of the users, the distributed consensus mechanism ensures that the IoV network can operate in a decentralized and trustless environment. However, among the consensus mechanisms, PoW is not suitable for IoV networks, which consists of many devices with limited computational capacity. Besides the high computational requirement, the delay is also a critical issue that hinders the application of PoW mechanisms in IoV networks where timing has a significant impact, e.g., delay might cause accidents or congestion. Thus, blockchain-based IoV networks such as [32]–[35] usually adopt the PoS mechanisms which do not require much computational power and has higher transaction speed.

A. DATA SHARING SYSTEM FOR IoV NETWORKS

In [32], a blockchain-based system for data sharing between vehicles and RSUs in an IoV network is proposed. To achieve the consensus, this system developed a variant of PoS, i.e., Delegated Proof-of-Stake (DPoS), where the stake is the reputation rating of the RSUs. To become a block proposer candidate, an RSU has to make a deposit, which will be confiscated for malicious behaviors, and its reputation rating must be higher than a certain threshold determined by the system. At each round, a block proposer will be selected from the candidates via the round-robin selection process to propose a block which consists of data sharing records and reputation ratings. The other candidates then vote to append the new block to the chain.

Although the proposed consensus mechanism has many similarities to Tendermint, e.g., the leader selected by the round-robin scheme, other candidates vote to confirm blocks, and deposit confiscated for malicious behaviors, it has several differences. Firstly, a stake is defined to be the reputation rating in this system, which is derived from a reputation calculation scheme using a subjective logic model based on the vehicle ratings of the RSUs. Secondly, an incentive mechanism is designed based on contract theory to distribute the rewards fairly between the block proposer and the other candidates.

B. CARPOOLING

With the carpooling service, e.g., Uberpool and Grabshare, the drivers can publish their destinations on a platform to find potential passengers with similar travel path, which is useful to reduce traffic congestion, traveling time, and pollution. In [33], a blockchain platform is designed for carpooling services, in which the asymmetric keys and digital signatures are used to enhance the security and privacy of the passengers and drivers. The PoS consensus mechanism is adopted to ensure the integrity of the carpooling records stored in the chain. Different from [32], only the RSUs participate in the consensus process in this platform. The blocks consist of the carpooling records (transactions), and the stake distribution. Each RSU's stake is the number of carpooling records that it processed, and the leader for each round is selected with probability proportional to its stake amount.

The consensus process in [33] is similar to that of the CoA protocol. The only difference is that instead of using the FTS algorithm, the leader in this platform is selected by the leader selection function, which takes the stake distribution, the RSU's public key, and the time stamp as inputs, and outputs the leader's ID.

C. VEHICLE TRUST MANAGEMENT SYSTEM

Since vehicles dynamically and constantly join and leave an IoV network, it is difficult for them to fully trust the messages they received, which necessitates a trust management system for evaluating the credibility of the message senders. In [34], a blockchain-based decentralized trust management system is proposed, which employs a hybrid PoW-PoS mechanism for reaching the consensus on the trust rating data stored in the chain. In this system, a vehicle broadcasts its rating for each message that it received. All the ratings for a message are collected by the RSUs to calculate the offset value of the message. The RSUs then participate in a PoW mining process, where they can use the sum of absolute offsets as stakes to lower the mining difficulty. The first RSU finding the nonce can add the new block to the chain, which consists of the offsets values of the messages. A vehicle can assert the credibility of a message sender by querying any RSU, which will then calculate the trust value of the sender by accumulating all its messages ratings.

Since the RSUs usually have similar computational power, the more stakes the RSU has, the higher chance it is selected

to be the leader. The stake amount is limited with an upper bound value determined by the network to ensure no single RSU continuously wins the election. However, an issue of this system is that the PoW mining process unnecessarily consumes a lot of energy and can be replaced by a pure stake-based leader selection for better energy efficiency. Similar to [33], a critical issue is that the incentive mechanism is completely ignored in [34]. Consequently, the security of these networks cannot be analyzed properly, especially in the events of attacks such as nothing-at-stakes attacks and long-range attacks.

D. VEHICULAR AD HOC BLOCKCHAIN

In [35], a blockchain-based framework for vehicular ad hoc network (VANET) was developed. Maintaining a VANET of many arbitrary nodes is difficult, especially in the context of IoV, as vehicles frequently join and leave the network. The proposed framework addresses this problem by allowing vehicles to form temporary connections to a small number of nodes, while the global state of the blockchain is maintained by the RSUs. Fundamentally, the network is split into smaller local networks, each under one RSU. In each network, the RSU and vehicles reach consensus via the Tezos protocol [36]. The RSUs then periodically send and receive information of the global blockchain from the main server.

The Tezos protocol employed in this framework was designed based on the CoA consensus mechanism. Similar to CoA, the leader is selected based on previous blocks in Tezos. However, there are also several validators selected by the FTS algorithm that will sign to confirm each proposed block. The block reward is shared among the block creator and validators if they behave properly. They also have to make deposits which will be confiscated for malicious behaviors. In this framework, the vehicles mostly interact and make transactions with each other, while the RSUs participate in the consensus process as the leader candidates and validators of the blockchain.

V. STAKE POOLS AND DECENTRALIZATION

A. STAKE POOLS AND STAKEHOLDERS

In the PoS networks, the probability that an individual stakeholder with a small stake amount is selected to be the leader is low. Moreover, to participate in the consensus process, a node must always be connected to the network, which incurs an operational cost. Therefore, small stakeholders often pool their stakes together to increase their opportunities to win blocks and share operational costs, which results in the formation of stake pools. Similar to the mining pools in PoW networks, a stake pool is considered to be a single node, and thus it poses a threat of centralizing the PoS networks. In particular, the stakeholders, e.g., RSUs, in the IoV networks often have to perform additional tasks, such as processing carpooling records [33] and vehicle trust rating inquiries [34]. Thus, the RSUs in these networks might be more inclined to join the stake pools to reduce their operational costs. In this section, we examine the stake pools from a game theoretical perspective to determine the strategic decisions of the stakeholders, and how these decisions affect the decentralization of the PoS networks.

B. SYSTEM MODEL

Consider N stakeholders with stakes $\mathbf{S} = (s_1, \ldots, s_N)$ and M stake pools with costs $\mathbf{c} = (c_1, \ldots, c_M)$ and fees $\boldsymbol{\alpha} = (\alpha_1, \ldots, \alpha_M)$ in the network. The pool costs are charged for joining the pool and maintaining its operations. The pool's fee is the profit margin of the pool's owner, which is usually 3% in real-world stake pools, e.g., Stakecube [53]. When the stakeholder i invests an amount s_i^m in the pool m, the expected reward r_i^m is given by

$$r_i^m = \rho_m \varphi_i^m (1 - \alpha_m) R - c_m e^{-s_i^m}, \tag{4}$$

where ρ_m is the proportion of pool m's stake in the total network stake, φ_i^m is the proportion of player i's stake in the total stake of pool m, and R is the block reward. The pool charges a fee of α_m percentage from each stakeholder's reward and a cost of $c_m e^{-s_i^m}$. It is worth noting that the cost is inversely proportional to s_i^m, which incentivizes the stakeholders to invest more stake into the pool. Let $\mathcal{N}_{-i}$ denote the set of all the stakeholders except stakeholder i, the stake proportion of pool m is

$$\rho_m = \frac{s_i^m + \sigma_m + \sum_{k \in \mathcal{N}_{-i}} s_k^m}{\tau}, \tag{5}$$

where $\tau = \sum_{i=1}^{N} \sum_{m=1}^{M} s_i^m$ is the total stake of the network, $\sum_{k \in \mathcal{N}_{-i}} s_k^m$ is the stakes invested in pool m by all the other stakeholders except stakeholder i, and σ_m is the current stake of pool m. Thus, ρ_m is the chance that the pool m is selected to be the leader and can receive the block reward R. When pool m receives the reward, it calculates each stakeholder's share based on how much the stakeholder invested in the pool, which is

$$\varphi_i^m = \frac{s_i^m}{s_i^m + \sigma_m + \sum_{k \in \mathcal{N}_{-i}} s_k^m}, \tag{6}$$

for stakeholder i. The cost and fee of the pool are then deducted from each stakeholder's share before it is finally delivered to each stakeholder.

C. GAME THEORETICAL ANALYSIS

To determine the rational stakeholder strategies, the system can be analyzed by applying the non-cooperative game theory. Non-cooperative game [37] is one of the most important branches of game theory, which models the situations of conflicting interests among the players. In a non-cooperative game, each player acts independently to maximize the profit which is affected by the actions of all players. A non-cooperative game in strategic form is denoted by $\mathcal{G}(\mathcal{N}, (\mathcal{S}_i)_{i \in \mathcal{N}}, (r_i)_{i \in \mathcal{N}})$, which consists of three components: the set of players $\mathcal{N} = (1, \ldots, N)$, the strategy set $\mathcal{S}_i$ consists of possible strategies for each player i, and the payoff function

of each player r_i. Let $\mathcal{S}_{-i}$ denote the strategy set of all players except player i, the strategy $\mathbf{s}_i'$ is strictly dominated by $\mathbf{s}_i$ if:

$$r_i(\mathbf{s}_i', \mathbf{s}_{-i}) < r_i(\mathbf{s}_i, \mathbf{s}_{-i}), \forall \mathbf{s}_{-i} \in \mathcal{S}_{-i}. \quad (7)$$

In other words, $\mathbf{s}_i'$ is strictly dominated by $\mathbf{s}_i$ if $\mathbf{s}_i$ yields a better payoff given any possible strategies of the other players. In this case, the dominated strategies can be eliminated because the player has no reason to choose a strategy that always gives worse payoff. If there exists a $\mathbf{s}_i$ which dominates all other possible strategies of player i, $\mathbf{s}_i$ is the dominant strategy. In the case where every player has a dominant strategy, the system can reach a dominant-strategy equilibrium because all the players will rationally choose their dominant strategies. Nevertheless, dominant strategies do not often exist in many non-cooperative games.

Another type of desirable outcome of non-cooperative game is the pure-strategy Nash equilibrium [37] where every player cannot get a better payoff by unilaterally changing to any other strategies. Let $\mathbf{s}^*$ and $\mathbf{s}_{-i}^*$ respectively denote the strategy of player i and the strategies of all players except player i at the pure-strategy Nash equilibrium, then for every player $i \in \mathcal{N}$ we have:

$$r_i(\mathbf{s}_i^*, \mathbf{s}_{-i}^*) > r_i(\mathbf{s}_i, \mathbf{s}_{-i}^*), \forall \mathbf{s}_i \in \mathcal{S}_i. \quad (8)$$

In other words, at the Nash equilibrium, no player can acquire a better payoff by independently switching to any other strategy. At such state, if all the players act rationally, the system becomes stable because no player has the incentive to deviate from the Nash equilibrium [37].

In the considered stake-pool game, the players (stakeholders) can freely invest their stakes in any amount within their budgets in any pool. The strategy set $\mathcal{S}_i$ of player i consists of all possible strategies $\mathbf{s}_i = (s_i^1, \ldots, s_i^M)$ where $\sum_{m=1}^{M} s_i^m \leqslant s_i$, and the total payoff is $r_i = \sum_{m=1}^{M} r_i^m$. The payoff of player i from pool m can be expressed as:

$$\begin{aligned} r_i^m &= \rho_m \varphi_i^m (1-\alpha_m) R - c_i e^{-s_i^m}, \\ &= \left(\frac{s_i^m + \sigma_m + \sum_{k \in \mathcal{N}_{-i}} s_k^m}{\tau} \right) \\ &\quad \times \left(\frac{s_i^m}{s_i^m + \sigma_m + \sum_{k \in \mathcal{N}_{-i}} s_k^m} \right) (1-\alpha_m) R - c_m e^{-s_i^m}, \\ &= \frac{s_i^m}{\tau} (1-\alpha_m) R - c_m e^{-s_i^m}. \end{aligned} \quad (9)$$

As shown in (9), the payoff of player i in pool m increases when s_i^m increases. However, its payoff decreases as the other players increase their investments in any pool, i.e., τ increases, implying that the players have conflicting interests. Thus, non-cooperative game theory is applied to analyze the stake pools and the behaviors of the stakeholders.

Let $\mathcal{G}$ denote the game with N players and M pools. To analyze $\mathcal{G}$ from a game theoretical perspective, we first examine the existence of the Nash equilibrium of this game.

Theorem 1 The game $\mathcal{G}$ admits at least one Nash equilibrium.

Proof: See Appendix A. □

Theorem 1 states that there is at least one Nash equilibrium in $\mathcal{G}$. Nevertheless, the main concerns when analyzing the Nash equilibria of a game also involve the uniqueness of the Nash equilibrium as well as whether the player's strategies can converge to this point. To analyze the uniqueness and convergence to the Nash equilibrium, we first prove that for every player, the strategies which invest less than the available budget are strictly dominated by the strategies which invest all the budget.

Theorem 2 Let $\mathbf{s}_i'$ denote a strategy where player i invests less than its total budget, i.e., $\sum_{m=1}^{M} s_i^m < s_i, \forall s_i^m \in \mathbf{s}_i'$, and $\mathbf{s}_i$ is a strategy where player i invests all its budget, i.e., $\sum_{m=1}^{M} s_i^m = s_i, \forall s_i^m \in \mathbf{s}_i$. For every $\mathbf{s}_i', \mathbf{s}_i \in \mathcal{S}_i$, $\mathbf{s}_i'$ is dominated by $\mathbf{s}_i$.

Proof: See Appendix B. □

As a result of Theorem 2, the strategies where the players do not invest all the budget can be eliminated from the strategy space. Based on this result and [38], we prove that the game $\mathcal{G}$ has a unique Nash equilibrium and $\mathcal{G}$ can always converge to the equilibrium.

Theorem 3 The game $\mathcal{G}$ has a unique Nash equilibrium $\mathbf{s}^*$ and the convergence to $\mathbf{s}^*$ is guaranteed.

Proof: See Appendix C. □

To find the Nash equilibrium, an iterative algorithm (Algorithm 1) is developed. Generally, Algorithm 1 computes the best response strategy for player i when all the other players' strategies are fixed. The obtained result is then fixed as the new strategy of player i, and the algorithm continues to find the best response for player $i+1$ and so on. The algorithm is stopped when the players no longer make any move, i.e., the Nash equilibrium is reached.

Algorithm 1 employs a loop to find the best strategy for every player, starting from player 1. To find the best response, Algorithm 1 performs an exhaustive search which calculates the expected payoff for each possible strategy. During the search, if a better payoff is found, the value is recorded and the strategy is marked as the best response. The search continues until the whole strategy space is enumerated. Then, the newly found best response is fixed as the strategy for the player, and the algorithm continues to find the best response for the player 2 and so on. After the strategy of player N is set, the algorithm starts the loop again from player 1. The loop is repeated until there is no change in the strategy of every player during a whole loop. Since Algorithm 1 exhaustively enumerates the possible search space, it can be regarded as a brute force search algorithm. The main procedure of Algorithm 1 is the loop, and the complexity of Algorithm 1 depends on the input size (s_i), the number of nested loops (M), and the number of players N. Formally, the worst-case time complexity of Algorithm 1 is $O(N\eta^M)$, where η is the input size [52].

For example, consider a small game of two players with stake budgets $\mathbf{s} = (100, 200)$, two pools with costs $\mathbf{c} = (0.5, 0.3)$ and fees $\boldsymbol{\alpha} = (3\%, 3\%)$, and a block reward $R = 10$. The Pareto-optimal strategies, i.e., the strategies which give a player the best payoff without

Algorithm 1 Iterative Algorithm to Find the Nash equilibrium

repeat
  $max \leftarrow 0$
  for $s_1^1 := 0$ to s_1 **do**
    ...
    for $s_1^M := 0$ to $s_1 - \sum_{m=1}^{M-1} s_1^m$ **do**
      if $r_1 > max$ **then** ▷ Find the best strategy of player 1
        $max \leftarrow r_1$
        $(x_1^1, \ldots, x_1^M) \leftarrow (s_1^1, \ldots, s_1^M)$
      end if
    end for
  end for
  $(s_1^1, \ldots, s_1^M) \leftarrow (x_1^1, \ldots, x_1^M)$ ▷ Fix player 1's strategy
  ...
  $max \leftarrow 0$
  for $s_N^1 := 0$ to s_N **do**
    ...
    for $s_N^M := 0$ to $s_N - \sum_{k=1}^{M-1} s_N^m$ **do**
      if $r_N > max$ **then** ▷ Find the best strategy of player N
        $max \leftarrow r_2$
        $(x_N^1, \ldots, x_N^M) \leftarrow (s_N^1, \ldots, s_N^M)$
      end if
    end for
  end for
  $(s_N^1, \ldots, s_N^M) \leftarrow (x_N^1, \ldots, x_N^M)$ ▷ Fix player N's strategy
until No player changes strategy

decreasing the payoff of other players [37], are also calculated. In this example, the algorithm finds a unique Nash equilibrium where $s_1^1 = 35, s_1^2 = 65, s_2^1 = 36, s_2^2 = 164$ as shown in Fig. 4. The result shows that although a pool with lower cost and fee attracts more stakes from the players, if the pools are competitive, i.e., their costs and fees are not significantly different, the stakes will not converge into a single pool, and thus decentralization is ensured.

In the following, we prove that the Nash equilibrium of the considered stake-pool game is also Pareto optimal.

Theorem 4 The Nash equilibrium of the game $\mathcal{G}$ is Pareto-optimal

Proof: See Appendix D. □

D. PERFORMANCE ANALYSIS

To evaluate more general cases, 20 instances of $\mathcal{G}$ are simulated. Each instance represents a network consists of 1000 stakeholders and five pools with parameters derived from real-world stake pools [53]–[56] and cryptocurrency networks [24]. The parameters and results of each instance are shown in Table 3. The first 10 instances are created to examine the effects of pool parameters on the network stake distribution, while the remaining instances are simulated to study the effects of the block reward and total network stake. At each iteration of the simulation, Algorithm 1 is employed to find the best strategy for a player, while the other players fix their strategies. Similar to the two-player case, the algorithm stops when the Nash equilibrium is reached.

The simulation results of the first 10 instances are illustrated in Fig. 5. These instances represent the cases with different combinations of pool parameters, while the total network stakes and block rewards are fixed. Instance 1 is the case where there is a pool with the lowest cost and fee in the network. The simulation results show that at the Nash equilibrium, all the network stakes go to the best pool. Instances 2 and 3 show that when a pool reduces its fee or cost, it can attract a portion of stake from the dominating pool, resulting in the network stake divided into 2 pools. Similarly, instances 3 to 7 show that if the other pools decrease their costs or fees, some stakeholders will switch to those pools. As the pool owners continue to adjust their stakes and fees, the network stake will be divided into 5 pools as shown in instance 8. Instances 9 and 10 show the other combinations of pool parameters under which the network stakes are divided into all the pools.

The network stakes and block reward parameters are varied to study their effects on the stake distribution in the last 10 instances. Among them, instances 11 to 15 are simulated to examine the impacts of the block rewards. Fig. 6 illustrates the influences of R on the stake distribution at the Nash equilibria. At the beginning (instance 11), the stakeholders invest in all the pools. As R increases while the other parameters remain unchanged, the pool that charges the highest fee, namely pool 5, attracts fewer stakes. When $R = 10$, pool 5 becomes empty (instance 12). As shown in (4), each pool charges a fee directly proportional to the reward each player receives. Since the block reward is doubled in this case, the fee amount is also doubled, while the costs charged by the pools remain the same. As a result, the advantage of pool 5 in terms of the low cost no longer outweighs its disadvantage of the high fee, and thus all stakeholders leave pool 5. As R keeps increasing, the simulation shows that the pools which charge higher fees become less desirable, e.g., when $R = 25$, pools 4 and 5 become empty (instance 13), and when $R = 500$ all players invest to pool 1 which has the lowest fee (instance 15). Similarly, the reward function is inversely proportional to the total network stake τ. When τ decreases, the reward increases, and consequently the pools that charge higher fees become less desirable and eventually empty (instances 16 to 20) as shown in Fig. 7. In summary, the results show that while the pool's cost and fee are not controlled by the network providers, the block reward and the total network stake can be adjusted to maintain the decentralization of the network.

VI. CHALLENGES AND POTENTIAL SOLUTIONS OF POS PROTOCOLS

In addition to the huge advantages with many promising applications, the development of PoS consensus mechanisms

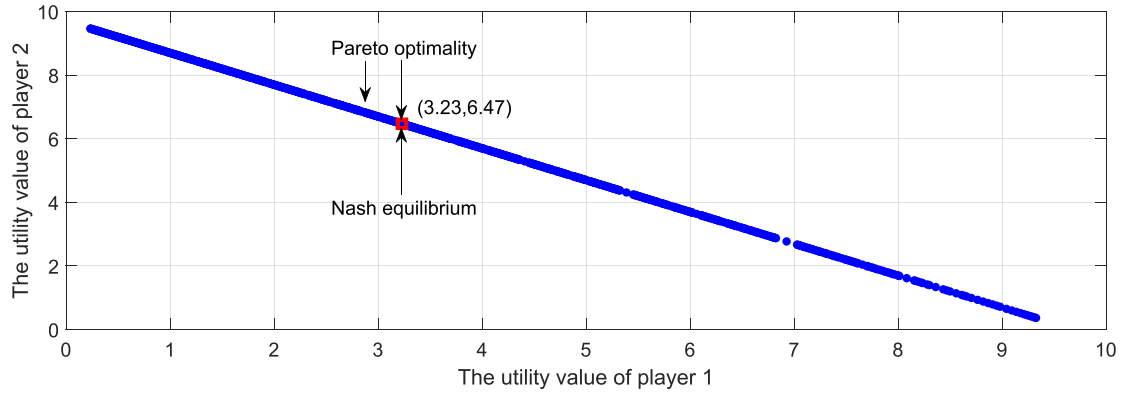

FIGURE 4. Pareto optimality and Nash equilibrium in the case with 2 players.

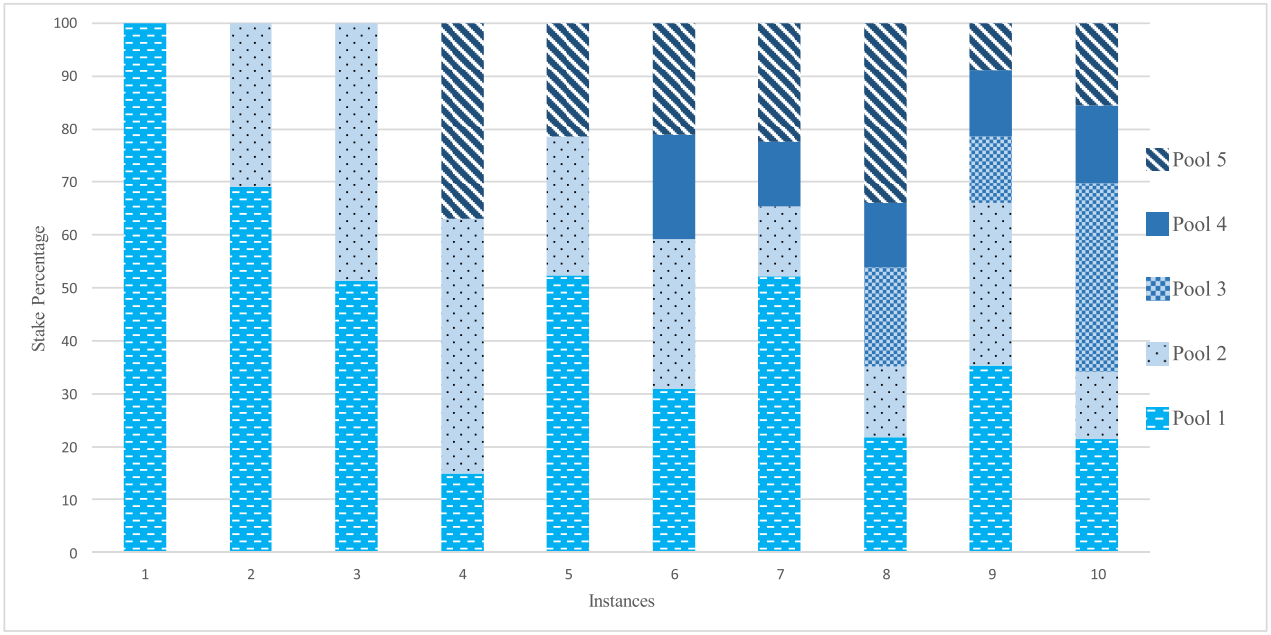

FIGURE 5. Simulation results of instances 1 to 10.

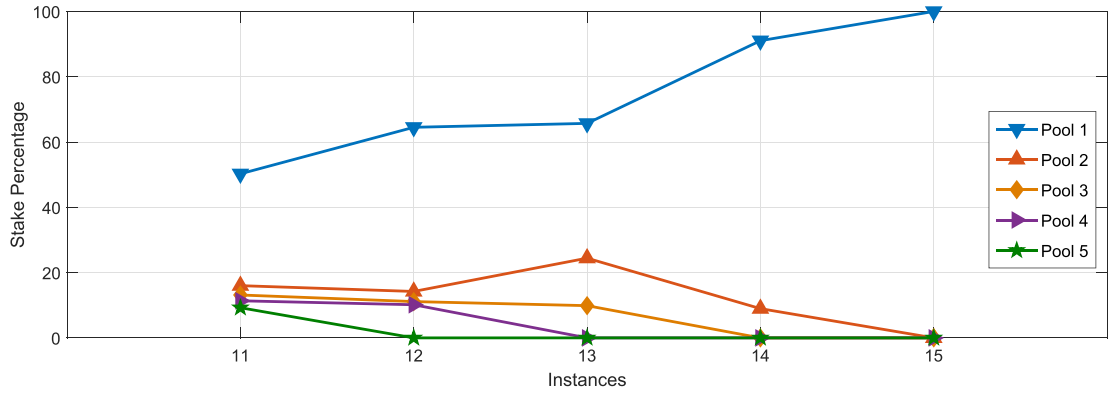

FIGURE 6. The influence of R on stake distribution.

is still in a nascent stage. Developing effective PoS mechanisms for future blockchain networks has been facing challenges for several reasons.

A. SECURITY ISSUES

The current designs of the PoS protocols are facing several security issues. Firstly, since the block generation consumes

TABLE 3. Parameters and results of 20 simulation instances.

No.	R	τ	Cost of pool (c)					Fee of pool (α)					Stake distrbution at pool (%)				
			1	2	3	4	5	1	2	3	4	5	1	2	3	4	5
1	3	10000	3	8	7	8	5	3	4	5	7	9	100.0	0	0	0	0
2	3	10000	3	8	7	8	5	3	2.5	5	7	9	69.1	30.9	0	0	0
3	3	10000	3	2	7	8	5	3	4	5	7	9	51.4	48.6	0	0	0
4	3	10000	3	2	7	8	5	3	4	5	7	2.5	14.9	48.1	0	0	37.0
5	3	10000	3	2	7	8	1	3	4	5	7	9	52.3	26.3	0	0	21.4
6	3	10000	3	2	7	8	1	3	2.5	5	7	9	30.9	28.3	0	19.8	21.0
7	3	10000	3	2	7	1.2	1	3	4	5	7	9	52.2	13.2	0	12.2	22.4
8	3	10000	3	2	7	1.2	1	3	2.5	5	7	9	21.9	13.3	18.7	12.2	33.9
9	3	10000	4	2	1.5	1.2	1	1	2	3	5	9	35.3	30.8	12.4	12.6	8.9
10	3	10000	5	2.5	2	1.2	1	1.5	2	2.5	4	5	21.4	12.8	35.6	14.6	15.6
11	5	10000	4	2	1.5	1.2	1	1	2	3	5	9	50.2	16.1	13.1	11.4	9.2
12	10	10000	4	2	1.5	1.2	1	1	2	3	5	9	64.5	14.2	11.1	10.2	0
13	25	10000	4	2	1.5	1.2	1	1	2	3	5	9	65.7	24.4	9.9	0	0
14	100	10000	4	2	1.5	1.2	1	1	2	3	5	9	91.1	8.9	0	0	0
15	500	10000	4	2	1.5	1.2	1	1	2	3	5	9	100.0	0	0	0	0
16	10	25000	25	12	7	4	1	1	2	3	5	9	58.3	12.1	11.9	10.2	7.5
17	10	2500	25	12	7	4	1	1	2	3	5	9	81.2	6.8	6.9	5.1	0
18	10	1000	25	12	7	4	1	1	2	3	5	9	92.3	4.5	3.2	0	0
19	10	500	25	12	7	4	1	1	2	3	5	9	95.2	4.8	0	0	0
20	10	250	25	12	7	4	1	1	2	3	5	9	100.0	0	0	0	0

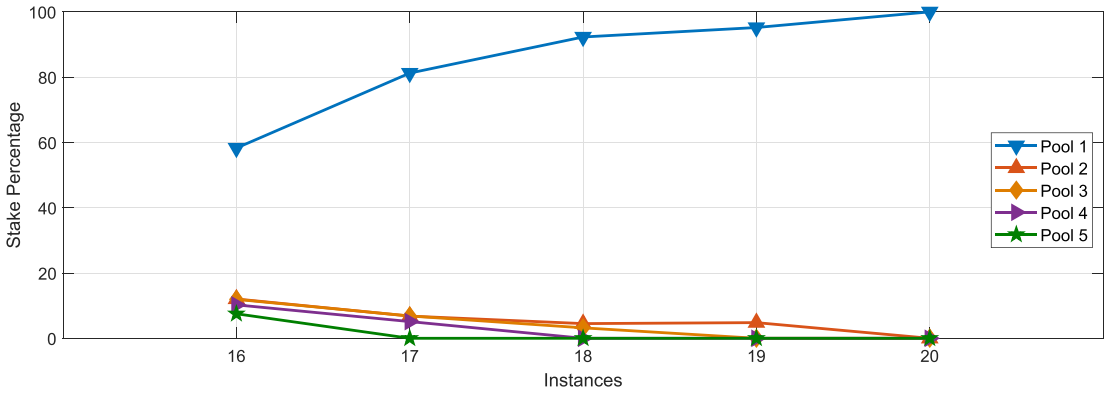

FIGURE 7. The influence of τ on stake distribution.

negligible resources, rational participants may try to create different blocks or forks, i.e., nothing-at-stake attacks [4]. Secondly, the adversary may try to bribe the leader, i.e., bribe attacks, to perform double-spending attacks [4]. To mitigate these attacks, the protocols can confiscate a leader's deposit in case of malicious behaviors as shown in [30] and [28]. In the protocol where there is no penalty mechanism, e.g., [21], the nothing-at-stake attack can be mitigated by having exactly one leader in each round. However, without a penalty mechanism, it is difficult to prevent bribe attacks.

Another type of attack that specifically targets on the PoS protocols using voting mechanisms is long-range attack [28]. For voting-based PoS protocols, the committee members may sell their stakes immediately at the beginning of the epoch they are selected. They are then unaffected by the incentive mechanism yet still have the voting rights. Consequently, they may behave maliciously without being affected by the penalization. Some protocols deal with such attacks by locking the stake of the committee member for a predefined period of time after the epoch ended [28]. By using a committee to vote for every block, once a block is appended to the chain it is finalized. Thus, the transaction history cannot be changed, and all the mentioned attacks are mitigated.

Some PoS protocols where the leader is selected based on the header of the previous block are also vulnerable to grinding attacks [4]. To mitigate such kind of attacks, we can use the seeds which cannot be influenced by the adversary, e.g., the hashes of previous blocks in [25] or the seeds created by the committee in [21]. A common issue of most PoS consensus mechanisms is that they lack theoretical background and formal definitions to support their security. There are many attacks targeting PoS networks, but they have not yet

been extensively investigated. A formal security model for the PoS protocols is also desirable, yet studies on this topic have been limited.

B. INCENTIVE COMPATIBILITY

Similar to PoW and PoX protocols, the incentive mechanisms, including consensus participation rewards and malicious behavior penalties, play a key role in ensuring the proper behaviors of participants in PoS-based protocols. Generally, the incentive mechanisms are designed to ensure that following the protocol properly outweighs the economic gains from malicious behaviors. However, many protocols lack analyses of the incentive mechanisms. The user's rational behaviors must be taken into account in consensus mechanisms, especially in PoS protocols, where the stake distribution affects the consensus process, yet the stake trade has high liquidity. Moreover, most protocols often ignore the stake trade outside of the network when considering their security. A potential solution to these problems is analyzing the user's rational behaviors using game theoretical approach, such as in [21], to design the effective incentive mechanisms.

C. PROTOCOL DESIGNS

Generally, each presented protocol includes a set of factors (e.g., consensus process, transaction adding process, and incentive mechanism). Each factor has impacts on several aspects, e.g., security, processing speed, and finality, of the protocol, and the question of to what extent each factor influences each aspect lacks a quantitative answer. Thus, rigorous analyses of each factor design are needed to evaluate their effects on the performances of the blockchain networks, as well as their mutual interactions. Based on the analyses, a systematic approach to protocol factor design can be developed for future blockchain networks.

VII. CONCLUSION

In this paper, we have provided an overview of the consensus mechanisms, the core unit of a blockchain network. We have then presented and compared several notable PoS consensus mechanisms, which have many advantages over the widely used PoW mechanisms. We have also discussed PoS blockchain applications in the field of IoV, and analyzed the formation of stake pools in PoS networks. We have shown that maintaining an appropriate ratio between the block rewards and the total network stakes is crucial to the decentralization of the network. Finally, we have discussed several challenges in developing effective consensus mechanisms for future blockchain network and the potential solutions to address these problems.

APPENDIX A
PROOF OF THEOREM 1

According to [37], if the payoff functions are concave and the strategy sets of the two players are compact and convex, there exists at least one Nash equilibrium in this game. To prove that the game admits at least one Nash equilibrium, we first prove that the reward functions of all the players are concave. The reward function of player i is:

$$r_i = \sum_{m=1}^{M} r_i^m. \tag{10}$$

A sufficient condition to prove that r_i is concave is that the payoff from every pool r_i^m is concave. The reward of player i from pool m is:

$$r_i^m = \frac{s_i^m}{\tau}(1-\alpha_m)R - c_m e^{-s_i^m}. \tag{11}$$

Let $\mathcal{M}_{-m}$ denote the set of all pools except pool m, $\frac{s_i^m}{\tau}$ can be expressed as:

$$\frac{s_i^m}{\tau} = \frac{s_i^m}{s_i^m + \sum_{j\in\mathcal{M}_{-m}} s_i^j + \sum_{k\in\mathcal{N}_{-i}} \sum_{h=1}^{M} s_k^h}, \tag{12}$$

which has the form $\frac{x}{x+a}$ and thus $\frac{s_i^m}{\tau}(1-\alpha_m)$ is concave ($(1-\alpha_m) > 0$, otherwise the pool charges more than 100% fee, which is impractical). Since $-c_m e^{-s_i^m}$ is also concave ($e^{-s_i^m}$ is convex and $-c_m$ is negative), r_i^m is concave. Thus, the reward function of every player is concave. In addition, the strategy sets of all players are defined as compact and convex sets. As a result, this game admits at least one Nash equilibrium.

APPENDIX B
PROOF OF THEOREM 2

The total reward function of player i is:

$$r_i = \frac{\sum_{m=1}^{M}(1-\alpha_m)s_i^m}{\sum_{k=1}^{N}\sum_{j}^{M} s_k^j} R - \sum_{m=1}^{M} c_m e^{-s_i^m}. \tag{13}$$

Now assume that player i is employing strategy $\mathbf{s}_i'$ which invests less than the available budget, i.e., $\sum_{m=1}^{M} s_i^m < s_i$. In this case, if the player chooses a strategy $\mathbf{s}_i$ which invests the remaining budget amount into a pool m the reward function becomes:

$$r_i = \frac{\sum_{j=1}^{M}(1-\alpha_j)s_i^j + (1-\alpha_m)\Delta s_i^m}{\sum_{k=1}^{N}\sum_{j}^{M} s_k^j + \Delta s_i^m} R - \sum_{j\in\mathcal{M}_{-m}} c_j e^{-s_i^j} - c_m e^{-(s_i^m + \Delta s_i^m)}, \tag{14}$$

where Δs_i^m is the extra amount invested in pool m. Then, the difference between the payoff of the strategy $\mathbf{s}_i$ and the strategy $\mathbf{s}_i'$ is expressed in (15), as shown at the top of the next page. For the strategy $\mathbf{s}_i$ to yield better payoff than the strategy $\mathbf{s}_i'$, the condition $r_i - r_i' > 0$ must hold. As can be seen from (15), $e^{-s_i^m} - e^{-(s_i^m + \Delta s_i^m)}$ is always positive because $s_i^m + \Delta s_i^m > s_i^m$. Then, a sufficient condition for $r_i - r_i'$ to be positive is that $(\alpha_j - \alpha_m) \geq 0$. Since there is no limit on the amount of stake a player can invest in a pool, if player i chooses to invest Δs_i^m in the pool with the lowest fee, i.e., $\alpha_m \leq \alpha_j, \forall j \in \mathcal{M}$, then $(\alpha_j - \alpha_m)$ will always be nonnegative. As a result, $r_i - r_i'$ is always positive, regardless of the strategies of the

$$
\begin{aligned}
r_i - r_i' &= \frac{\sum_{j=1}^{M}(1-\alpha_j)s_i^j + (1-\alpha_m)\Delta s_i^m}{\sum_{k=1}^{N}\sum_{j}^{M} s_k^j + \Delta s_i^m} R - \frac{\sum_{m=1}^{M}(1-\alpha_m)s_i^m}{\sum_{i=1}^{N}\sum_{m=1}^{M} s_i^m} R + \sum_{j=1}^{M} c_j e^{-s_i^j} - \sum_{j\in\mathcal{M}_{-m}} c_j e^{-s_i^j} - c_m e^{-(s_i^m+\Delta s_i^m)}, \\
&= \frac{(1-\alpha_m)(\sum_{i=1}^{N}\sum_{m=1}^{M} s_i^m) - \sum_{j=1}^{M}(1-\alpha_j)s_i^j}{(\sum_{i=1}^{N}\sum_{m}^{M} s_i^m)(\sum_{i=1}^{N}\sum_{m}^{M} s_i^m + \Delta s_i^m)} \Delta s_i^m R + c_m(e^{-s_i^m} - e^{-(s_i^m+\Delta s_i^m)}), \\
&= \frac{\sum_{k\in\mathcal{N}_{-i}}\sum_{j=1}^{M}(1-\alpha_m)s_k^j + \sum_{j\in\mathcal{M}_{-m}}(\alpha_j-\alpha_m)s_i^j}{(\sum_{i=1}^{N}\sum_{m}^{M} s_i^m)(\sum_{i=1}^{N}\sum_{m}^{M} s_i^m + \Delta s_i^m)} \Delta s_i^m R + c_m(e^{-s_i^m} - e^{-(s_i^m+\Delta s_i^m)}). \qquad (15)
\end{aligned}
$$

other players. This means that $\mathbf{s}_i'$ always gives worse payoff than $\mathbf{s}_i$, and thus $\mathbf{s}_i'$ is always dominated by $\mathbf{s}_i$.

APPENDIX C
PROOF OF THEOREM 3

Let $\theta(\mathbf{s}, \omega)$ denote the weighted nonnegative sum of the payoff functions of all the players, we have:

$$\theta(\mathbf{s}, \omega) = \sum_{i=1}^{N} \omega_i r_i(\mathbf{s}_i), \qquad (16)$$

where ω_i is the weight of players i. The pseudogradient $g(\mathbf{s}, \omega)$ of $\theta(\mathbf{s}, \omega)$ is defined by

$$g(\mathbf{s}, \omega) = \begin{bmatrix} \omega_1 \frac{\partial r_1}{\partial s_1^1} & \cdots & \omega_1 \frac{\partial r_1}{\partial s_1^M} \\ \vdots & \ddots & \vdots \\ \omega_N \frac{\partial r_N}{\partial s_N^1} & \cdots & \omega_N \frac{\partial r_N}{\partial s_N^M}. \end{bmatrix}$$

According to Rosen's theorem [38], if $\theta(\mathbf{s}, \omega)$ is diagonally strictly concave for some fixed $\omega_i > 0, \forall i \in \mathcal{N}$, the game has a unique Nash equilibrium. In [38], it is proven that a sufficient condition for $\theta(\mathbf{s}, \omega)$ to be diagonally strictly concave is that the matrix $\Psi = [G(\mathbf{s}, \omega) + G^T(\mathbf{s}, \omega)]$ is negative definite, where $G(\mathbf{s}, \omega)$ is the Jacobian of $g(\mathbf{s}, \omega)$ with respect to $\mathbf{s}$. The Jacobian $G(\mathbf{s}, \omega)$ can be calculated by:

$$G = \begin{bmatrix} \omega_1 \frac{\partial^2 r_1}{\partial s_1^1 \partial s_1^1} & \omega_1 \frac{\partial^2 r_1}{\partial s_1^2 \partial s_1^1} & \cdots & \omega_1 \frac{\partial^2 r_1}{\partial s_1^M \partial s_N^1} \\ \omega_1 \frac{\partial^2 r_1}{\partial s_1^1 \partial s_1^2} & \omega_1 \frac{\partial^2 r_1}{\partial s_1^2 \partial s_1^2} & \cdots & \omega_1 \frac{\partial^2 r_1}{\partial s_1^M \partial s_N^2} \\ \vdots & \vdots & \ddots & \vdots \\ \omega_N \frac{\partial^2 r_N}{\partial s_N^1 \partial s_1^M} & \omega_N \frac{\partial^2 r_N}{\partial s_N^2 \partial s_1^M} & \cdots & \omega_N \frac{\partial^2 r_N}{\partial s_N^M \partial s_N^M}. \end{bmatrix} \qquad (17)$$

As proven in Theorem 2, the strategies where there is any player who invest less than the budget can be eliminated from the strategy space. Thus, the total network stakes become a constant, i.e., $\tau = \sum_{i=1}^{N} s_i$, and the reward function of player i becomes:

$$r_i = \frac{\sum_{m=1}^{M}(1-\alpha_m)s_i^m}{\tau} R - \sum_{m=1}^{M} c_m e^{-s_i^m}. \qquad (18)$$

Then, the partial derivative of r_i with respect to s_i^m is:

$$\frac{\partial r_i}{\partial s_i^m} = \frac{(1-\alpha_m)}{\tau} R + c_m e^{-s_i^m}. \qquad (19)$$

As shown in (19), $\frac{\partial r_i}{\partial s_i^m}$ is a function depending only on s_i^m. Thus, if we take the partial derivative again with respect to any variable other than s_i^m, it becomes zero, which is the value for any non-diagonal elements of $G(\mathbf{s}, \omega)$ (17). The second order partial derivative with respect to s_i^m is:

$$\frac{\partial^2 r_i}{\partial s_i^m \partial s_i^m} = -c_m e^{-s_i^m}. \qquad (20)$$

If we choose $\omega_1 = \ldots = \omega_N = 1$, Ψ becomes:

$$\begin{bmatrix} -2c_1 e^{-s_1^1} & \cdots & 0 & 0 & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & -2c_M e^{-s_1^M} & 0 & \cdots & 0 \\ 0 & \cdots & 0 & -2c_1 e^{-s_2^1} & \cdots & 0 \\ \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & \cdots & 0 & 0 & \cdots & -2c_M e^{-s_M^N}. \end{bmatrix} \qquad (21)$$

In this game, the matrix Ψ (21) is a symmetric diagonal matrix with all negative diagonal elements, which satisfies the condition $(-1)^k D_k > 0$, where D_k is the k^{th} leading principal minors. Thus, the matrix is negative definite and therefore, $\theta(\mathbf{s}, \omega)$ is diagonally strictly concave. As proven in [38], if $\mathcal{G}$ satisfies the diagonally strict concavity property, $\mathcal{G}$ has a unique Nash equilibrium and starting from any feasible point in $\mathcal{S}$ the game will converge to the Nash equilibrium.

APPENDIX D
PROOF OF THEOREM 4

A strategy set $\mathbf{s}_i$ is Pareto-optimal if no player can get a better payoff without decreasing the reward of any other player [37]. Let $\mathbf{s}_i^*$ and $\mathbf{s}_{-i}^*$ denote the strategies at the equilibrium of player i and all other players except player i, respectively. Let r_i^* denote the total payoff of player i at the equilibrium. Suppose (for the sake of contradiction) that there exists another

set of strategies $\mathbf{s}'_{-i}$ of the other players except player i such that $r'_i < r^*_i$, i.e.,

$$\frac{\sum_{m=1}^{M}(1-\alpha_m)s_i^m}{\tau'}R - \sum_{m=1}^{M} c_m e^{-s_i^m} < \frac{\sum_{m=1}^{M}(1-\alpha_m)s_i^m}{\tau^*}R - \sum_{m=1}^{M} c_m e^{-s_i^m}, \quad (22)$$

which means $\tau' > \tau^*$. However, by Theorem 2 we have $\sum_{j=1}^{M} s_i^j = s_i, \forall i \in \mathcal{N}$ at $\mathbf{s}^*$, which means $\tau^* \geq \tau'$. Thus, there exists no $\mathbf{s}'_{-i}$ such that $r'_i < r^*_i$. In other words, at the equilibrium no player can change its strategy to decrease any other player's reward.

Furthermore, by the Nash equilibrium definition (8), $\mathbf{s}^*_i$ is the best response to $\mathbf{s}^*_{-i}$, i.e., $r_i(\mathbf{s}^*_i, \mathbf{s}^*_{-i}) > r_i(\mathbf{s}_i, \mathbf{s}^*_{-i})$. Thus, player i cannot increase r_i by deviating from $\mathbf{s}^*_i$. Since at $\mathbf{s}^*$ the players also cannot decrease the reward of any other player, $\mathbf{s}^*$ is Pareto-optimal.

REFERENCES

[1] 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.

[2] CoinMarketCap. *Global Charts*. Accessed: Nov. 3, 2018. [Online]. Available: https://coinmarketcap.com/charts/

[3] Blockchain. *Hashrate Distribution and Estimation of Hashrate Distribution Amongst the Largest Mining Pools*. Accessed: Nov. 3, 2018. [Online]. Available: https://www.blockchain.com/pools?

[4] W. Wang, D. T. Hoang, P. Hu, Z. Xiong, D. Niyato, P. Wang, Y. Wen, and D. I. Kim, "A survey on consensus mechanisms and mining strategy management in blockchain networks," *IEEE Access*, vol. 7, pp. 22328–22370, 2018.

[5] Stats. *Bitcoin Block Explorer*. Accessed: Nov. 3, 2018. [Online]. Available: https://btc.com/stats

[6] S. King. (Jul. 2013). Primecoin: Cryptocurrency with prime number proof-of-work, Self-Published Papers. Accessed: Nov. 3, 2018. [Online]. Available:http://primecoin.io/bin/primecoin-paper.pdf

[7] A. Shoker, "Sustainable blockchain through proof of exercise," in *Proc. IEEE 16th Int. Symp. Netw. Comput. Appl. (NCA)*, Cambridge, MA, USA, Jan. 2017, pp. 1–9.

[8] M. Ball, A. Rosen, M. Sabin, and P. N. Vasudevan, "Proofs of useful work," Int. Assoc. Cryptologic Res., Tech. Rep. 2017/203, 2017. [Online]. Available: https://eprint.iacr.org/2017/203

[9] A. Miller, A. Juels, E. Shi, B. Parno, and J. Katz, "Permacoin: Repurposing Bitcoin work for data preservation," in *Proc. IEEE Symp. Secur. Privacy*, May 2014, pp. 475–490.

[10] H. Kopp, C. Bösch, and F. Kargl, "KopperCoin—A distributed file storage with financial incentives," in *Proc. 12th Int. Conf. Inf. Secur. Pract. Exper.*, Zhangjiajie, China, Nov. 2016, pp. 79–93.

[11] *Filecoin: A Decentralized Storage Network*, Protocol Labs, San Francisco, CA, USA, Aug. 2017.

[12] A. Miller, A. Kosba, J. Katz, and E. Shi, "Nonoutsourceable Scratch-off puzzles to discourage bitcoin mining coalitions," in *Proc. 22nd ACM SIGSAC Conf. Comput. Commun. Secur. (CCS)*, 2015, pp. 680–691.

[13] P. Daian, I. Eyal, A. Juels, and E. G. Sirer, "(Short Paper) PieceWork: Generalized outsourcing control for proofs of work," in *Financial Cryptography and Data Security* (Lecture Notes in Computer Science). 2017, pp. 182–190.

[14] S. Park, K. Pietrzak, J. Alwen, G. Fuchsbauer, and P. Gazi, "Spacecoin: A cryptocurrency based on proofs of space," Int. Assoc. Cryptologic Res., Tech. Rep. 2015/528, 2015. [Online]. Available: https://eprint.iacr.org/2015/528

[15] J. Blocki and H.-S. Zhou, "Designing proof of human-work puzzles for cryptocurrency and beyond," in *Proc. 14th Int. Conf. Theory Cryptogr.*, Beijing, China, Oct. 2016, pp. 517–546.

[16] S. King and S. Nadal. (Aug. 2012). PPCoin: Peer-to-peer crypto-currency with proof-of-stake. Self-Published Paper. [Online]. Available: https://peercoin.net/assets/paper/peercoin-paper.pdf

[17] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of activity: Extending bitcoin's proof of work via proof of stake [extended abstract]y," *ACM SIGMETRICS Perform. Eval. Rev.*, vol. 42, no. 3, pp. 34–37, Dec. 2014.

[18] P. Daian, R. Pass, and E. Shi, "Snow white: Provably secure proofs of stake," Int. Assoc. Cryptolog. Res., Tech. Rep. 2016/919, Sep. 2016. [Online]. Available: https://eprint.iacr.org/2016/919

[19] C. Decker, J. Seidel, and R. Wattenhofer, "Bitcoin meets strong consistency," in *Proc. 17th Int. Conf. Distrib. Comput. Netw. (ICDCN)*, 2016, Art. no. 13.

[20] R. Pass and E. Shi, "Hybrid consensus: Efficient consensus in the permissionless model," in *Proc. 31st Int. Symp. Distrib. Comput. (DISC)*, Vienna, Austria, vol. 91, Oct. 2017, pp. 39:1–39:16.

[21] A. Kiayias, A. Russell, B. David, and R. Oliynykov, "Ouroboros: A provably secure proof-of-stake blockchain protocol," in *Proc. 37th Annu. Int. Cryptolog. Conf. (CRYPTO)*, Santa Barbara, CA, USA, Aug. 2017, pp. 357–388.

[22] Cardano. *Ouroboros Proof of Stake Algorithm*. Accessed: Mar. 14, 2019. [Online]. Available: https://cardanodocs.com/cardano/proof-of-stake/

[23] D. Bluetower. (Jan. 19, 2019). Cardano (ADA)—Ouroboros hydra and Cardano scalability to Visa level TPS. ELEVENEWS. Accessed: Mar. 14, 2019. [Online]. Available: https://elevenews.com/2019/01/19/cardano-ada-ouroboros-hydra-and-cardano-scalability-to-visa-level-tps/

[24] Cardano. *Incentives and Staking in Cardano*. Accessed: May 13, 2019. [Online]. Available:https://staking.cardano.org/

[25] I. Bentov, A. Gabizon, and A. Mizrahi, "Cryptocurrencies without proof of work," in *Proc. Int. Conf. Financial Cryptogr. Data Secur.* Springer, 2016, pp. 142–157.

[26] I. Stones. (Sep. 4, 2018). *Overview of Tezos, Economics Model*. Accessed: Mar. 14, 2019. [Online]. Available:https://medium.com/infinity-stones/overview-of-tezos-economical-model-e197f773c6c4?fbclid=IwAR1O6qawaVSUPbK5X2B0pCnErWy97X_35rsqQkPqawLQSsNgUFYwdoAxf1U

[27] ChainBits. (Jan. 31, 2019). *Tezos (XTZ) Review—True Decentralized Governance for Blockchain*. Accessed: Mar. 14, 2019. [Online]. Available: https://www.chainbits.com/reviews/tezos-review/?fbclid=IwAR36FPU7vavgPq__qDs-oCWwlODTcprjBLOVtb3UdAO-LoZ_8BJyE4CrIwg

[28] V. Buterin and V. Griffith, "Casper the friendly finality gadget," 2017, *arXiv:1710.09437*. [Online]. Available: https://arxiv.org/abs/1710.09437

[29] Y. Gilad, R. Hemo, S. Micali, G. Vlachos, and N. Zeldovich, "Algorand: Scaling byzantine agreements for cryptocurrencies," in *Proc. 26th Symp. Oper. Syst. Principles*, 2017, pp. 51–68.

[30] J. Kwon. (2014). *Tendermint: Consensus Without Mining (Draft)*. [Online]. Available: https://tendermint.com/static/docs/tendermint.pdf

[31] Interchain Foundation. (Oct. 27, 2017). *A Beginner's Guide to Ethermint—Cosmos Blog*. Accessed: Mar. 14, 2019. [Online]. Available: https://blog.cosmos.network/a-beginners-guide-to-ethermint-38ee15f8a6f4?fbclid=IwAR00pLh7Spzf_-afrOF69U0RYmqE2a-SPyDL3EXLe8NdAVHWjf9xALyLrNRY

[32] J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim, and J. Zhao, "Towards secure blockchain-enabled Internet of vehicles: Optimizing consensus management using reputation and contract theory," 2018, *arXiv:1809.08387*. [Online]. Available: https://arxiv.org/abs/1809.08387

[33] M. Li, L. Zhu, and X. Lin, "Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4573–4584, Jun. 2018.

[34] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet Things J.*, vol. 6, no. 2, pp. 1495–1505, Apr. 2019.

[35] B. Leiding and W. V. Vorobev. *Tezos-Based Vehicular Ad Hoc Blockchains*. [Online]. Available: https://uploads-ssl.webflow.com/5a4ea18a81f55a00010bdf45/5b996ad89cfdafcbce83f6f9_20180912_Tezos-Vehicular-Ad-Hoc-Blockchains–v1.0.pdf

[36] L. M. Goodman. (2014). *Tezos—A Self-Amending Crypto-Ledger White Paper*. Accessed: Nov. 3, 2018. [Online]. Available: https://www.tezos.com/static/papers/white_paper.pdf

[37] Z. Han, D. Niyato, W. Saad, T. Başar, and A. Hjørungnes, *Game Theory in Wireless and Communication Networks: Theory, Models, and Applications*. Cambridge, U.K.: Cambridge Univ. Press, 2012.

[38] J. B. Rosen, "Existence and uniqueness of equilibrium points for concave N-person games," *Econometrica*, vol. 33, no. 3, pp. 520–534, 1965.

[39] S. Nakamoto. (May 2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[40] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum Project, Zug, Switzerland, Yellow Paper EIP-150 Rev., Aug. 2017, vol. 151.

[41] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," *IEEE Trans. Depend. Sec. Comput.*, vol. 15, no. 5, pp. 840–852, Sep./Oct. 2016.
[42] 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. Informat.*, vol. 14, no. 8, pp. 3690–3700, Aug. 2018.
[43] 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.
[44] A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "LSB: A lightweight scalable blockchain for IoT security and privacy," 2017, *arXiv:1712.02969*. [Online]. Available: https://arxiv.org/abs/1712.02969
[45] D. Ivan, "Moving toward a blockchain-based method for the secure storage of patient records," in *Proc. ONC/NIST Blockchain Healthcare Res. Workshop*, Gaithersburg, MD, USA, 2016, pp. 1–11.
[46] K. Peterson, R. Deeduvanu, P. Kanjamala, and K. Boles, "A blockchain-based approach to health information exchange networks," in *Proc. NIST Workshop Blockchain Healthcare*, vol. 1, 2016, pp. 1–10.
[47] G. Baxendale, "Can blockchain revolutionise EPRs?" *ITNOW*, vol. 58, no. 1, pp. 38–39, Mar. 2016.
[48] A. Sudhan and M. J. Nene, "Employability of blockchain technology in defence applications," in *Proc. Int. Conf. Intell. Sustain. Syst. (ICISS)*, Dec. 2017, pp. 630–637.
[49] A. McAbee, M. Tummala, and J. McEachen, "Military intelligence applications for blockchain technology," in *Proc. 52nd Hawaii Int. Conf. Syst. Sci.*, 2019, pp. 1–10.
[50] W. Wang, D. Niyato, P. Wang, and A. Leshem, "Decentralized caching for content delivery based on blockchain: A game theoretic perspective," in *Proc. IEEE Int. Conf. Commun. (ICC)*, May 2018, pp. 1–6.
[51] N. Herbaut and N. Negru, "A model for collaborative blockchain-based video delivery relying on advanced network services chains," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 70–76, Sep. 2017.
[52] J. Kleinberg and T. Eva, *Algorithm Design*. Harlow, U.K.: Pearson, 2014.
[53] *Stakecube, Crypto Shib*. Accessed: May 13, 2019. [Online]. Available: https://cryptoshib.com/stakecube/
[54] MyCointainer. *Earn Profits by Holdings Cryptoassets*. Accessed: May 13, 2019. [Online]. Available: https://www.mycointainer.com/
[55] Max and Max. *Our Fee Structure. Medium*. Accessed: May 26, 2019. [Online]. Available: https://medium.com/brunchpool/our-fee-structure-5d951bc16976
[56] BTCPOP. *PEER-TO-PEER*. Accessed: May 13, 2019. [Online]. Available: https://btcpop.co/home.php

CONG T. NGUYEN received the B.E. degree in electrical engineering and information from the Frankfurt University of Applied Sciences, in 2014, and the M.Sc. degree in global production engineering and management from the Technical University of Berlin, in 2016. Since 2016, he has been a Teaching Assistant with Vietnamese German University, Vietnam. His research interests include operations research, blockchain technology, game theory, and optimizations.

DINH THAI HOANG (M'16) received the Ph.D. degree in computer science and engineering from Nanyang Technological University, Singapore, in 2016. He is currently a Faculty Member with the School of Electrical and Data Engineering, University of Technology Sydney, Australia. His research interests include emerging topics in wireless communications and networking, such as ambient backscatter communications, vehicular communications, cybersecurity, the Internet of Things, and 5G networks. He is also an Exemplary Reviewer of the IEEE TRANSACTIONS ON COMMUNICATIONS, in 2018, and the IEEE TRANSACTIONS ON WIRELESS COMMUNICATIONS, in 2017 and 2018. He is also an Editor of the IEEE WIRELESS COMMUNICATIONS LETTERS and the IEEE TRANSACTIONS ON COGNITIVE COMMUNICATIONS AND NETWORKING.

DIEP N. NGUYEN (M'13–SM'19) received the M.E. degree in electrical and computer engineering from the University of California at San Diego (UCSD) and the Ph.D. degree in electrical and computer engineering from The University of Arizona (UA). He was a DECRA Research Fellow with Macquarie University and a Member of Technical Staff with Broadcom, CA, USA, ARCON Corporation, Boston, consulting the Federal Administration of Aviation, on turning detection of UAVs and aircraft, and the U.S. Air Force Research Laboratory, on anti-jamming. He is currently a Faculty Member with the Faculty of Engineering and Information Technology, University of Technology Sydney (UTS). His recent research interests include computer networking, wireless communications, and machine learning application, with emphasis on systems' performance and security/privacy. He has received several awards from LG Electronics, UCSD, The University of Arizona, the U.S. National Science Foundation, and the Australian Research Council.

DUSIT NIYATO (M'09–SM'15–F'17) received the B.E. degree from the King Mongkuk'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 and, by courtesy, the School of Physical and Mathematical Sciences, Nanyang Technological University, Singapore. He has published more than 340 technical papers in the area of wireless and mobile computing. He is an inventor of four U.S. and German patents. He has authored a few books, including *Dynamic Spectrum Access and Management in Cognitive Radio Networks*, *Game Theory in Wireless and Communication Networks: Theory, Models, and Applications*, and *Wireless Device-to-Device Communications and Networks* (Cambridge University Press). He is a Highly Cited Researcher, in 2017. He received the Best Young Researcher Award of the IEEE Communications Society (ComSoc) Asia Pacific and the IEEE Communications Society Fred W. Ellersick Prize Paper Award. He was a Guest Editor of the IEEE JSAC. He is also a Distinguished Lecturer of the IEEE Communications Society. He serves as an Area Editor for the IEEE TWC, a Senior Editor of the IEEE WIRELESS COMMUNICATIONS LETTERS, an Editor of the IEEE TCOM, the IEEE COMST, the IEEE TMC, and the IEEE TCCN.

HUYNH TUONG NGUYEN received the Ph.D. degree in computer science from François Rabelais University. He is currently a Faculty Member with Ho Chi Minh City University. He is an expert in algorithms and resolutions (simulation, modeling, and optimization) for real-life problems, including manufacturing scheduling, transportation problems, education management and assessment, digital currency, and cryptography. His work has appeared in the *Asian Journal of Computer Science and Information Technology*, the *European Journal of Operational Research*, the *Journal of Scheduling*, and *Mathematical Problems in Engineering*.

ERYK DUTKIEWICZ (M'05–SM'15) received the B.E. degree in electrical and electronic engineering and the M.Sc. degree in applied mathematics from The University of Adelaide, in 1988 and 1992, respectively, and the Ph.D. degree in telecommunications from the University of Wollongong, in 1996. His industry experience includes management of the Wireless Research Laboratory at Motorola, in 2000. He is currently the Head of the School of Electrical and Data Engineering, University of Technology Sydney, Australia. He holds a professorial appointment at Hokkaido University, Japan. His current research interests include 5G and the Internet-of-Things networks.