How Can Incentive Mechanisms and Blockchain Benefit with Each Other? A Survey

RONG HAN, The State Key Lab of ISN, School of Cyber Engineering, Xidian University, China
ZHENG YAN, The State Key Lab of ISN, School of Cyber Engineering, Xidian University, China and Department of Communications and Networking, Aalto University, Finland
XUEQIN LIANG, The State Key Lab of ISN, School of Cyber Engineering, Xidian University, China
LAURENCE T. YANG, School of Computer Science and Technology, Hainan University, China

In a blockchain-based system, the lack of centralized control requires active participation and cooperative behaviors of system entities to ensure system security and sustainability. However, dynamic environments and unpredictable entity behaviors challenge the performances of such systems in practice. Therefore, designing a feasible incentive mechanism to regulate entity behaviors becomes essential to improve blockchain system performance. The prosperous characteristics of blockchain can also contribute to an effective incentive mechanism. Unfortunately, current literature still lacks a thorough survey on incentive mechanisms related to the blockchain to understand how incentive mechanisms and blockchain make each other better. To this end, we propose evaluation requirements in terms of the properties and costs of incentive mechanisms. On the one hand, we provide a taxonomy of the incentive mechanisms of blockchain systems according to blockchain versions, incentive forms, and incentive goals. On the other hand, we categorize blockchain-based incentive mechanisms according to application scenarios and incentive goals. During the review, we discuss the advantages and disadvantages of state-of-the-art incentive mechanisms based on the proposed evaluation requirements. Through careful review, we present how incentive mechanisms and blockchain benefit with each other, discover a number of unresolved issues, and point out corresponding potential directions for future research.

CCS Concepts: • **General and reference → Surveys and overviews**; • **Theory of computation → Algorithmic game theory and mechanism design**; • **Security and privacy → Distributed systems security;**

Additional Key Words and Phrases: Blockchain, incentive mechanism, monetary incentive, non-monetary incentive

ACM Reference format:
Rong Han, Zheng Yan, Xueqin Liang, and Laurence T. Yang. 2022. How Can Incentive Mechanisms and Blockchain Benefit with Each Other? A Survey. *ACM Comput. Surv.* 55, 7, Article 136 (December 2022), 38 pages.
https://doi.org/10.1145/3539604

This work is supported in part by the National Natural Science Foundation of China under Grant 62072351; in part by the Academy of Finland under Grant 308087, Grant 335262, Grant 345072, and Grant 350464; in part by the open project of ZheJiang Lab under Grant 2021PD0AB01; and in part by the 111 Project under Grant B16037.
Authors' addresses: R. Han and X. Liang (corresponding author), The State Key Lab of ISN, School of Cyber Engineering, Xidian University, Xi'an, China; emails: ronghan@stu.xidian.edu.cn, dearliangxq@126.com; Z. Yan, The State Key Lab of ISN, School of Cyber Engineering, Xidian University, Xi'an, China and Department of Communications and Networking, Aalto University, Espoo, Finland; email: zyan@xidian.edu.cn; L. T. Yang, School of Computer Science and Technology, Hainan University, Haikou, China; email: ltyang@hainanu.edu.cn.

0360-0300/2022/12-ART136 $15.00
https://doi.org/10.1145/3539604

1 INTRODUCTION

Blockchain, as the core technology embedded in Bitcoin [65], is intrinsically a decentralized database that records data in blocks chronologically. Advanced cryptography technology enables the blockchain with decentralization, immutability, traceability, transparency, anonymity, without depending on a trusted third party. These characteristics make the blockchain technology advanced in overcoming single-point-failure problems suffered by centralized systems. The development of blockchain has experienced three stages: Blockchain versions 1.0, 2.0, and 3.0. Recent years have witnessed the prosperity of blockchain technology in broader scenarios other than cryptocurrencies, include cloud computing, **Internet of Things (IoT)**, **Internet of Vehicles (IoV)**, healthcare, and so on.

On the one hand, the security of blockchain highly depends on the participation of massive system entities [77], which increases the difficulty of a single entity to dominate the system and perform malicious behavior, e.g., tampering blocks. Unfortunately, the system entities are rational in practice, and they strategically behave according to which action can bring them profits. An incentive mechanism has already been embedded into the Bitcoin system once it was designed in 2008 [65]. A consensus node (called miner) obtains financial rewards that consist of fixed Coinbase rewards (or mining rewards) and transaction fees when successfully mining a block through **Proof-of-Work (PoW)** consensus [65]. Similarly, the rewards of a miner that generates a confirmed block in Ethereum include the fixed Coinbase rewards, the total execution fee consumed by all programs in the confirmed block, and the rewards for involving uncle blocks (that are the orphan blocks excluded from the longest/main chain) [10]. Even though the underlying incentive mechanisms in blockchain technologies provide essential incentives to the miners, they ignore the motivation of other types of system nodes. For example, full nodes that keep and maintain a complete and up-to-date copy of the blockchain should be motivated to send historical block data to the newly joined nodes for preventing attackers from tampering with historical data and controlling a system. Propagation nodes play a crucial role in broadcasting transaction records and blocks. It is essential to motivate them to behave actively and cooperatively. Some researchers have acknowledged this problem, and they have proposed many incentive mechanisms for motivating all stakeholders to participate and cooperate in blockchain systems.

On the other hand, motivating system entities to participate and behave cooperatively is an economically effective approach to suppress the influence of selfish behavior. Such an economic approach has already been investigated as an incentive mechanism, which applies a variety of internal or external incentives to standardize and relatively immobilize the expected behavior of system entities [20]. How to apply incentive mechanisms to motivate system entities to actively participate has been well studied in References [68, 85, 100, 102]. Researchers also investigated how to design incentive mechanisms for encouraging cooperative behavior in References [86, 91, 92]. Numerous papers have surveyed the technologies applied in incentive mechanisms in the field of mobile crowdsensing [43, 75, 98], heterogeneous networks [37], and delay-tolerant networks [45]. These incentive mechanisms are generally executed by centralized third parties while the centralized parties are not fully reliable in practice. Moreover, most centralized incentive mechanisms are implemented manually, which is time-consuming and inevitably complicate the incentive distribution process. Introducing blockchain into an incentive mechanism supports decentralized incentive execution and eliminates security and privacy risks brought by the centralized party. At the same time, smart contract technology can automatically issue incentives and prevent disputes during incentive distribution. We notice the research on this topic and discover the effectiveness and feasibility of introducing the blockchain technology into incentive mechanism design.

Existing surveys with regard to blockchain principally concentrate on consensus mechanisms [71, 84, 90], solutions to security and privacy issues [5, 42, 60, 69], and applications [19, 31, 67].

Moreover, the surveys related to incentive mechanisms mostly investigate the technologies applied in a centralized manner [43, 48]. Only few surveys have reviewed the incentive mechanisms in blockchain in recent years. Huang et al. [41] discussed issuing mechanisms and allocating mechanisms of blockchain tokens in digital economy. The token refers to a digital equity certificate circulated in the blockchain, for example, cryptocurrencies like bitcoins and Ethers. Yu et al. [97] focused on the incentive layer and token models in the blockchain network. Wang et al. [84] reviewed the research on incentive compatibility of the Bitcoin PoW consensus protocol. Liu et al. [60] reviewed game theory-based incentive mechanisms to prevent miners from launching attacks on a blockchain system. However, there still lacks a comprehensive survey on the incentive mechanisms in blockchain systems and blockchain-based incentive mechanisms. With the high popularity of blockchain, it becomes essential to review incentive mechanisms related to the blockchain to understand how incentive mechanisms and blockchain benefit each other.

In this article, we review the incentive mechanisms in different versions of blockchain technologies and blockchain-based incentive mechanisms published from the year 2010 to the present, especially since the mid-2010s. We collect papers with the following keywords: blockchain, incentive mechanism, and smart contract from five mainstream databases: IEEE Explorer, ACM Digital Library, Elsevier, ScienceDirect, and Springer. To precisely evaluate the effectiveness of these incentive mechanisms, we propose a set of evaluation requirements regarding incentive properties (i.e., individual rationality, incentive compatibility, incentive truthfulness, incentive fairness, social welfare maximization, incentive automation, incentive privacy, and incentive sustainability) and costs (i.e., computational complexity and backward compatibility). We thoroughly review the incentive mechanisms in Blockchain 1.0, 2.0, and 3.0 by classifying them based on incentive forms and goals, as well as blockchain-based incentive mechanisms by classifying them based on incentive scenarios and goals. Our review is performed by evaluating each paper with the proposed requirements. In the end, we specify some open issues discovered from our survey and accordingly indicate several future research directions. Table 1 evidently compares our article with existing surveys. Specifically, the main contributions of our article can be summarized as follows:

- We are the first to propose a set of requirements regarding incentive properties and costs for evaluating the effectiveness of existing blockchain-related incentive mechanisms, which contains some general requirements that can be applied to evaluate all incentive mechanisms and some specific requirements that are personalized for different scenarios. These requirements provide instructive guidelines for devising practical and effective incentive mechanisms.
- We thoroughly review the current literature on the incentive mechanisms in Blockchain 1.0, 2.0, and 3.0, and blockchain-based incentive mechanisms by discussing their advantages and disadvantages in detail referring to the proposed requirements. Furthermore, we conclude which incentive form is suitable for which incentive goal in blockchain systems and the incentive performance in different application scenarios as well as the applications and limitations of different forms of blockchain-based incentive mechanisms. Specifically, we discover that (1) the monetary incentive is suitable for encouraging node participation willingness, (2) the reputation-based incentive is suitable for scenarios where nodes need to be monitored, (3) the gamified incentive can be used in simple game scenarios or work as an auxiliary method, and (4) the hybrid incentive provides desirable performance at high costs.
- We figure out a number of open issues and propose research directions to motivate further investigation into blockchain-related incentive mechanisms. Concretely, (1) we identify that the design of transaction fees and mining pools, as well as the incentives to broadcast nodes and full nodes needs further investigation; (2) existing incentive mechanisms seldom

Table 1. Comparison of Our Survey with Other Existing Surveys

Covered Topic	[41]	[97]	[84]	[60]	Our Survey
Propose requirements of incentive mechanisms	N	N	N	N	Y
Review incentive mechanisms in blockchain	Y	Y	N	N	Y
Review blockchain-based incentive mechanisms	N	N	N	N	Y
Propose taxonomy of incentive mechanisms	N	N	N	N	Y

Y: satisfied; N: unsatisfied.

suppress various attacks; (3) fairness and automation are important incentive properties that should be satisfied when designing incentive mechanisms for blockchain systems; (4) privacy and backward compatibility are two important properties that should be fulfilled in blockchain-based incentive mechanisms; and (5) blockchain-based incentive mechanisms should also take a serious look at the incentive to miners.

The rest of this article is organized as follows. Section 2 provides an introductory overview of blockchain. Section 3 gives the taxonomy of incentive mechanisms and proposes a set of requirements to evaluate the performance of incentive mechanisms. Consequently, Sections 4 and 5 review the incentive mechanisms in Blockchain 1.0, 2.0, and 3.0, and blockchain-based incentive mechanisms, respectively, as well as discuss the effectiveness of each incentive mechanism based on the proposed requirements. Section 6 discusses how incentive mechanisms and blockchain benefit with each other. Furthermore, we discover open issues and present future research directions in Section 7. Finally, we conclude this article in the last section.

2 BACKGROUND

This section briefly introduces the basic concepts related to blockchain, its prevalent consensus mechanisms, along with the types of blockchain. We also present some infamous attacks launched to blockchain networks at the end of this section.

2.1 Blockchain

Blockchain is a distributed infrastructure that employs block-chain data structures to verify and maintain the information recorded in blocks, adopts consensus mechanisms for information generation and update, and applies cryptography to protect data and information security.

Take the Bitcoin blockchain as an example; it is composed of blocks that are chained chronologically. Figure 1(a) illustrates the structure and components of each block, which consists of a block header and a block body. The block header stores control information, including the version number of this block, the hash value of its previous block, timestamp, nonce, the hash value of Merkle Root, and a difficulty target. The block body stores verified transaction records. The issuance of new coins is also regarded as a transaction, which is called a Coinbase transaction. All the bitcoins circulating in the Bitcoin system originate from system issuance.

Nodes in the blockchain network are the computers that run the blockchain system and participate in peer-to-peer networks. These nodes can be divided into three categories based on their functions in the system.

- **Broadcast nodes.** They execute the blockchain operation protocol and participate in the verification and spread of transaction records and block information.
- **Mining nodes.** They participate in the consensus mechanisms and create new blocks. They are also called as miners.

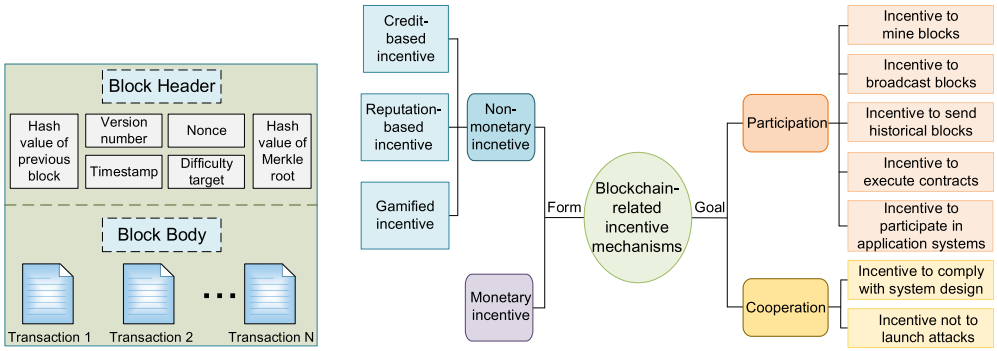

Fig. 1. (a) Block structure and components of Bitcoin; (b) taxonomy of blockchain-related Incentive mechanisms.

- **Full nodes (Bitcoin Core).** These nodes keep and maintain a complete and up-to-date copy of the blockchain and they have all the functions of broadcast nodes and mining nodes.

In what follows, we alternatively use "system node" and "system entity" based on presentation context. Generally, they represent the same meaning, i.e., an object in a system that has some functions. "System node" is normally used for presenting a blockchain network system, while "system entity" is often used when illustrating an incentive mechanism.

The general blockchain workflow is described as follows. First, a new transaction occurs between both parties and the transaction is broadcasted to the blockchain network. The node that receives this transaction verifies whether it is legal. After passing the verification, the transaction will be incorporated into a block by miners. All miners in the whole network execute a same consensus mechanism to create a valid block. Finally, the block is broadcasted to other nodes for verifying its legality. After successfully passing the verification, this block is appended to the blockchain.

Several miners may successfully find blocks at the same time, resulting in multiple valid blocks appearing at the same block height. This situation is called forking. Different blockchain systems deal with forks in different ways. For example, to ensure that only a unique main chain is kept in the Bitcoin blockchain system, a unique main chain is selected according to the longest chain rule.

In the Bitcoin blockchain, since mining bitcoins is extremely competitive, it becomes more and more impossible for an individual miner to find a block as more and more miners poured into the network. Mining pools collect the computing power of individual miners to mine a block together and distribute the rewards to its pool members (i.e., miners) according to predefined policies [70], which successfully reduces the variance of miners' incomes. However, the accumulation of computing power is contrary to the decentralization goal of blockchain design, which may lead to a centralization problem. Moreover, the competition between mining pools promotes new attacks, e.g., block withholding attack, fork after withholding attack.

2.2 Consensus Mechanisms

In a distributed system, nodes reach a trust relationship according to a consensus mechanism for guaranteeing system consistency and continuity. Herein, we briefly introduce several popular consensus mechanisms.

2.2.1 Proof-of-Work. PoW proves how much work has been done, which normally requires a prover to perform time-consuming computation while its computation result is effortless to verify [33]. In Bitcoin, the miners rely on machine computing power to perform mathematical operations

by getting a hash code of the next block that can satisfy its difficulty requirement (i.e., with expected number of zeros). The miner that solves the puzzle of PoW first gets the accounting right. PoW holds the characteristics of security, fairness, and easy verification while wasting computation resources. Moreover, due to the centralization of computing power, independent miners are increasingly difficult to finish a mining task.

2.2.2 Proof-of-Stake. Compared with PoW, **Proof-of-Stake (PoS)** does not require miners to continuously mine for generating a new block, but via various combinations of random selection, wealth or age (i.e., so called stake) to confirm a block. Therefore, PoS is more energy-saving than PoW. PoS defines a concept of coinage, a number derived from the product of the number of coins multiplied by the number of days the coins have been held. The system allocates corresponding stakes to coin holders according to their coinages [57]. The more stakes held by a coin holder, the less difficulty of its block mining is. Once the stake holder successfully mines a block and receives mining rewards, the number of coins it holds is reset to zero and the calculation of its coinage is restarted. The ability of a node to acquire new stakes depends on the stakes it already held thus causing unfairness. PoS has low energy consumption and short consensus time, but it tends to lead to centralization.

2.2.3 Delegated Proof-of-Stake. The emergence of **Delegated Proof-of-Stake (DPoS)** solves the problem that a small number of accounts with a large amount of currency in PoS can control the generation of blocks. DPoS divides the consensus mechanism into two stages. First, all nodes vote to decide which nodes can be trusted. Second, these voted nodes perform transaction verification and accounting [57]. DPoS reduces the number of verification nodes, decreases energy consumption, and achieves high efficiency. However, a fixed number of verification nodes may impact decentralization.

2.2.4 Practical Byzantine Fault Tolerance. **Practical Byzantine Fault Tolerance (PBFT)** solves the low-efficiency problem in the original Byzantine fault tolerance algorithm. PBFT is a state machine copy replication algorithm. Two kinds of nodes exist in PBFT, which are primary nodes and backup nodes. Once a primary node receives a request from a client, a three-stage procedure will be performed: pre-prepare, prepare, and commit, after which a reply is sent back to the client [62]. The efficiency of PBFT depends on the number of participating nodes. PBFT performs well when there are few nodes in the network and the probability of forking is low. The scalability of PBFT-based blockchain system is poor.

2.3 Blockchain Classification

According to the open scope of blockchain to the public, existing blockchains can be classified into three categories. A public blockchain is the blockchain where everyone can join or leave freely without specific authorization. Anyone can read and send transactions on the public blockchain. A private blockchain is limited to internal use within an organization. A consortium blockchain is only open to internal members or authorized members of external institutions.

A permissioned blockchain requires system nodes to obtain approval before participating. Therefore, private blockchains and consortium blockchains are permissioned blockchains. The above three types of blockchains, no matter public, private, or consortium, have their pros and cons. The choice of blockchain depends on application scenarios and application requirements.

2.4 Attacks in Blockchain

Attackers exploit the vulnerabilities of the blockchain network to launch attacks for obtaining illegitimate incomes. We list some attacks against blockchain algorithms and protocols below.

2.4.1 51% Attack. An attacker that holds at least 51% of the total network computing power can launch this attack to arbitrarily modify blocks [73]. This attack is also called a majority attack. By controlling 51% network computing power, a miner can make a target block be an orphan block by disabling transactions in that block. The 51% attack is a way to raise double-spending, which refers to the same Unspent Transaction Output spent in two transactions. Double-spending often takes advantage of time delay in transaction confirmation caused by block consensus.

2.4.2 Selfish Mining Attack. Selfish mining refers to that a miner or a mining pool does not publish and distribute its newly mined block while continuing to mine the next block and maintaining its leading position in mining [27]. Selfish mining bets on the probability of mining successfully with hashing power and damages the fairness of the blockchain network.

2.4.3 Block Withholding Attack. The block withholding attack is an attack against the mining pool [72]. After a miner successfully mines a block, it withholds this block without broadcasting, thus the mining pool cannot get the reward for the block. However, the miner launching the **Block Withholding Attack (BWA)** can share the rewards obtained by the blocks mined by others according to the allocation rules of the mining pool. Therefore, the BWA causes little financial loss to the miner and the attack cost of the miners is very low. BWA also occurs between mining pools [25].

2.4.4 Sybil Attack. Sybil attack refers to a malicious node illegally presenting multiple identities to the outside world. These identities of the node are usually called Sybil nodes. In the blockchain network, there is no cost for nodes to create new identities. An attacker can utilize this vulnerability to launch the Sybil attack by forging its identity to join the network. After mastering a number of identities, the attacker can freely conduct malicious activities [78].

2.4.5 Denial-of-Service Attack. **Denial-of-Service (DoS)** attack refers to deliberately attacking the defects of a system protocol or directly exhausting the resources of an attacked object through brutal means [11]. In blockchain-related systems, when generating a block consumes few resources, malicious miners can continuously generate invalid blocks to launch DoS attacks on the system. Attackers can also employ malicious behaviors to make it impossible for honest miners to profit from mining, thereby stopping miners mining and making the blockchain stop running.

3 TAXONOMY AND EVALUATION REQUIREMENTS OF INCENTIVE MECHANISMS

This section first introduces the taxonomy of incentive mechanisms as shown in Figure 1(b) and then proposes a set of requirements to evaluate the effectiveness of existing incentive mechanisms.

3.1 Taxonomy of Incentive Mechanisms

3.1.1 Incentive Forms. Existing incentive mechanisms in blockchain can be divided into two categories according to incentive forms: monetary incentive and non-monetary incentive.

The monetary incentive is designed for regulating the behavior of system entities from an economic perspective. It increases the utility of entities when they participate in the system by rewarding entities with money, thereby giving the entities motivation to join the system. The monetary incentive mechanisms employ economic balance to increase the cost of attacking or behaving selfishly to prevent attacks and encourage the entities to cooperate.

Existing non-monetary incentive can be further divided into credit-based incentive, reputation-based incentive, and gamified incentive. Both the credit-based incentive and the reputation-based incentive manage the relationships among system entities with trust. However, reputation stands for the comprehensive trust of a group in an individual, while credit emphasizes the subjective dependence of a trustor on a trustee. A large number of studies apply these two incentive

mechanisms to prevent collusion between untrusted individuals. The gamified incentive takes advantage of entities' psychological tendency to play games, provides the entities with a pleasant emotional experience in the process of completing system tasks, actively guides entities to behave as system design. Common gamified incentive mechanisms use points and badges as incentives.

3.1.2 Incentive Goals. Incentive mechanisms can be classified based on incentive goals. The incentive mechanisms can encourage nodes to participate in maintaining the safety and sustainability of a blockchain system. They can also prevent various attacks and mitigate blockchain weaknesses to make the system work in a normal and expected way. Therefore, incentive mechanisms play a crucial role in the blockchain system [8]. Generally, there are two main types of incentive goals: incentive for system participation and incentive for cooperation with other nodes.

Participation. Blockchain requires the participation of a plethora of nodes to ensure security and decentralization. Existing system design naively holds an assumption that the nodes will actively participate as expected. However, the nodes are rational and profit-driven in practice, therefore, they need incentives to participate. We further classify the participation incentives in Blockchain 1.0 and 2.0 according to the functions of system nodes. Specifically, we consider the incentives for mining blocks, broadcasting blocks, sending historical blocks, and executing contracts. When discussing the incentive mechanisms in Blockchain 3.0 and blockchain-based incentive mechanisms, we refer the participation incentives to participation in specific application scenarios.

Cooperation. Another immature assumption of existing blockchain systems is that all system nodes will strictly perform as system design. In practice, the profit-driven nodes will maximize their profits through various selfish or malicious behaviors, such as violating the system design and exploiting vulnerabilities for attacking the system. These behaviors could cause short-term or long-term threats to the system and harm the profits of other system nodes. To overcome this problem, we can introduce an incentive mechanism into the system to encourage node cooperation. Specifically, the cooperation discussed in this article includes two types of behaviors: strictly executing the system protocols and discouraging from initiating attacks.

3.2 Requirements

To judge the effectiveness and practicality of incentive mechanisms, we propose the following requirements regarding the properties and costs of incentive mechanisms. Our evaluation on existing works in Sections 4 and 5 is based on these requirements.

3.2.1 Properties.

Individual Rationality (IR). System entities are rational stakeholders in practice driven by individual profits or benefits. An incentive mechanism with individual rationality ensures nonnegative benefits for system entities for motivating participation willingness. The monetary incentive mechanisms could easily satisfy individual rationality by manually adjusting utility parameters.

Incentive Compatibility (IC). When all system entities take selfish actions to maximize their individualized benefits, they care little about the influence of their selfish behavior on system performance. There are enormous tragic examples concerning this situation, for example, the tragedy of the commons [35]. System entities all adopt selfish behaviors in an attempt to maximize their own interests without contributing to the system. This will cause the system performance to be damaged or even crashed, every entity can no longer profit from the system, and tragedy happens. If an incentive mechanism that can guarantee the individual interest of each system entity is compatible with group interest [74], then the system could achieve sustainable and healthy development. We

refer to such a property as incentive compatibility, which is an essential property to be considered when designing an incentive mechanism.

Incentive Truthfulness (IT). Selfishness could result in dishonest behavior of system entities if being dishonest can bring benefits. An effective incentive mechanism should be capable of encouraging the system entities to behave honestly and tell the truth. Such a truthful incentive mechanism enables a system to operate in a long run. When the selfish action with IC is dishonest behavior, the incentive compatibility and truthfulness are not distinguished.

Incentive Fairness (IF). Fairness involves two implications. First, the amount of reward that a system entity receives is proportional to its contribution. Second, a system entity must successfully pay the required amount of reward to the entities with contributions as expected. Fairness additionally supports the honest behavior of system entities and encourages these system entities to contribute as much as possible.

Social Welfare Maximization (SW). Social welfare represents the summation of the net benefits of all system entities. The designer of an incentive mechanism has absolute control in determining system parameters. It is rational for the designer to decide the parameters to maximize its own benefit. However, a system with higher social welfare could be more attractive for massive system entities. The potential costs for increasing social welfare will later pay off when more system entities are involved. Therefore, a system that applies an incentive mechanism with social welfare maximization is more acceptable than other systems without such a requirement.

Incentive Automation (IA). Blockchain is a distributed system without a centralized node to manage the whole system. Therefore, an incentive mechanism should bring little centralized management for being compatible with the decentralization of blockchain. Incentive trigger, task allocation, and reward distribution should be performed automatically. Furthermore, automatic incentive eliminates the weakness of centralized incentive management, e.g., refusing to pay and modifying payment information. A widely applied method to achieve automation is to compile incentive mechanisms into Smart Contracts. Therefore, the fulfillment of automation is discussed in the incentive mechanisms in Blockchain 2.0 and 3.0 and blockchain-based incentive mechanisms.

Incentive Privacy (IP). In practical application systems based on blockchain, most of the privacy threats are the disclosure of transaction information and off-chain information such as user identities. Therefore, we consider privacy protection in terms of transaction information and user information. Normally, the incentive mechanisms are for blockchain working nodes in Blockchain 1.0 and 2.0, where incentive information is expected to be public for a motivation purpose. Therefore, we do not consider privacy preservation as a requirement when discussing the performance of incentive mechanisms in Blockchain 1.0 and 2.0. However, it is inevitable to consider specific privacy requirements when designing incentive mechanisms in Blockchain 3.0 and blockchain-based incentive mechanisms with regard to concrete application scenarios. When users of these applications submit or upload information to the open blockchain, curious people can easily derive private information from the blocks. The risk of privacy disclosure reduces the enthusiasm of the users to participate in these applications. Therefore, protecting user privacy can make the incentive mechanisms in Blockchain 3.0 and blockchain-based incentive mechanisms more feasible.

Incentive Sustainability (IS). A feasible incentive mechanism needs to stimulate the long-term participation of all types of nodes. Sustainability can avoid loss and imbalance of system participants, which results in negative effects on the system, such as resource monopoly, thus ensuring long-term system operations.

Incentive Scalability (SC). Scalability refers to the ability of an incentive mechanism to remain efficient and effective as the number of participating entities increases. A blockchain system usually requires a large number of participation nodes to ensure system security and reliability. Therefore, the incentive mechanism should be scalable to ensure its applicability. Specifically, the scalability of the incentive mechanism of the blockchain system is usually dependent on the scalability of the system, which is restricted by the architecture or throughput of the system. Considering the focus of this article is incentive mechanisms, we only evaluate the fulfillment of this requirement in Section 5, where the blockchain-based incentive mechanisms are surveyed.

3.2.2 *Costs.*

Time Cost: Computational Complexity (CC). A feasible incentive mechanism should have acceptable computational complexity, especially when no powerful centralized entities are present to maintain the execution. Specifically, a public blockchain network is dynamic because of its openness and all system entities can enter and leave at any time. Therefore, its computational overhead is considerably heavy and a lightweight incentive mechanism is highly needed. Notably, CC is normally considered when an algorithm is introduced into the incentive mechanism.

Implementation Cost: Backward Compatibility (BC). Backward compatibility means that an incentive mechanism can work well with previous versions of the blockchain. This requirement is reasonably essential, since not all blockchain entities are up to date, while all entities are qualified for gaining incentives. Since blockchain-based incentive mechanisms need to replace their original mechanisms, we ignore this requirement in our review in Section 5.

4 INCENTIVE MECHANISMS IN BLOCKCHAIN

This section reviews existing incentive mechanisms in Blockchain 1.0, 2.0, and 3.0. We review the literature works by classifying them based on incentive forms and incentive goals. For each work, we first specify incentive mechanism design and then comment on its pros and cons based on the requirements proposed in Section 3. Table 2 summarizes all of our findings.

4.1 Monetary Incentive

The monetary incentive is commonly applied to provide direct motivation to system entities with tangible rewards. This type of incentives has been employed to encourage mining blocks, broadcasting blocks, sending historical blocks, executing smart contracts, participation in an application system, cooperation in complying with system design, and preventing from attacking.

4.1.1 *Incentives to Participate.*

The blockchain system requires the participation of multiple nodes to ensure its security and decentralization. Specifically, in Blockchain 1.0 and 2.0, miners are required for mining. Broadcast nodes should actively broadcast blocks and transactions, and full nodes are expected to send historical block records to new nodes. Besides, the nodes in Blockchain 2.0 are also required to execute smart contracts. The node participation is also necessary for maintaining system operations in Blockchain 3.0. However, rational and profit-driven nodes may hesitate to join due to the resource consumption cost and the risk of privacy leakage.

Incentives to mine blocks. The consensus mechanism applied in the Bitcoin blockchain is based on PoW, which consumes massive computation resources of miners. Therefore, the miners need to be motivated for mining blocks. The monetary incentive for miners in the Bitcoin blockchain system is block rewards, including transaction fees and Coinbase rewards.

However, the total amount of bitcoins issued is limited and the Coinbase reward for each mined block decreases every four years. Therefore, transaction fee is playing a more and more

important role in motivating the participation of miners. Researchers found that if there is no Coinbase reward for mining, then the Bitcoin system would be unstable [12, 49, 64]. Tsabary and Eyal [80] found that only issuing transaction fees is insufficient for motivating miners thus forming a mining gap. Jiang and Wu [44] thought that when the transaction fees become considerable, rational miners prefer to include transactions with high transaction fees to their blocks and generate large-size blocks that involve as many transactions as possible. However, large-size blocks take a long time to be verified and reach a consensus. Moreover, transactions with low transaction fees could be ignored. Therefore, the efficiency and fairness of the Bitcoin blockchain system will be adversely affected if purely using transaction fee-based incentive mechanisms.

Lewenberg et al. [54] proposed an incentive mechanism to motivate miners with low computing power and poor connections to actively participate in mining. The paper used a Directed Acyclic Graph structure and an inclusive protocol, in which the transaction fees included in the block that is not on a main chain is also rewarded to the miner of the block. However, if the transaction has already appeared in the block on the main chain, then the off-chain block miner cannot get the fee. When the block is released too slowly, the transaction fee rewards will be reduced. This protocol is suitable for situations where a block size is large or a block interval is short. By motivating nodes to include different transactions instead of only selecting transactions with high fees, system throughput is improved. Miners with poor connections have a high probability of generating off-chain blocks. The inclusive protocol compensates the miners that generate off-chain blocks with transaction fees, which makes the weak miners suffer little loss. Therefore, marginalized miners are willing to participate in mining in a continuous way, which helps avoiding the monopoly of mining by miners with powerful computational resources and high-speed connectivity, so this mechanism meets IS. Although the blocks generated by weak miners are not on the main chain, these miners can still get corresponding rewards. Thus, the mechanism satisfies IF and IR. The inclusive protocol, which rewards miners with off-chain blocks, reduces the cost of selfish mining attacks. Therefore, the incentive mechanism fails to meet IC and IT, since miners still have motivation to launch selfish mining attacks. SW and BC were not discussed in this paper. IA and CC are not supported in this mechanism, since smart contract was not applied and no concrete algorithm was involved.

Incentives to broadcast blocks. The blockchain network needs broadcast nodes to spontaneously forward the received transactions and block information to their neighbor nodes for improving the performance and security of the network. However, there is no incentive for transaction propagation in traditional blockchain design. Moreover, a broadcast node that receives the latest block can privately mine the next block without broadcasting this block for increasing its competitiveness. Researchers have investigated how to implement incentive mechanisms for motivating broadcast nodes to spread transactions and blocks in blockchain networks.

Babaioff et al. [6] defined the blockchain network as a forest of d-ary directed trees with a height of H and proposed a hybrid reward scheme for motivating nodes to broadcast transactions. When the height of broadcast nodes is less than the predetermined threshold in the directed tree, each intermediate node on the transaction propagation path shares the same reward β with the root node. A miner that authorizes the transaction (located at the lth node in the propagation path) gets $1 + (H - l + 1) \times \beta$ reward. When a broadcast node does not broadcast the transaction to neighboring nodes, it will lose its reward for being an intermediate node, which is unprofitable. Therefore, the incentive mechanism meets IT and IC. However, it does not consider other structures of networks and different processing capabilities of different nodes. Therefore, IF, SW, BC, and IS of the incentive mechanism become unknown. IA and CC were not touched.

Abraham et al. [1] proposed an incentive mechanism to encourage broadcast nodes to propagate transactions and blocks in a peer-to-peer network. In this incentive mechanism, when a miner

successfully mines a block, each broadcast node on the transaction propagation path will receive a transaction propagation fee as the reward set by the miner. This mechanism can prevent Sybil attacks, mitigate selfish mining, and encourage nodes to spread transactions and behave honestly. Therefore, this incentive mechanism meets IC and IT. But this work only provides theoretical analysis, without evaluating its computational complexity. It does not consider privacy and automation. IF, SW, BC, and IS were not mentioned in this work, and IA and CC were not touched.

Ersoy et al. [24] proposed an incentive mechanism for public blockchain network nodes to spread transactions. Transaction fees are allocated to the broadcast nodes on the propagation path according to different shares. This path is one of the transaction propagation paths from the transaction initiator to the block generator. The authors regulated that the closer the broadcast node is to the block generator, the greater the contribution it makes and the more rewards it gets. Therefore, the mechanism meets IF. According to the mathematical analysis, when a broadcast node propagates the transaction to all its neighbor nodes, it will maximize its revenue. For a profit-driven broadcast node, it will do its best to broadcast the transaction, so the mechanism satisfies IC and IT. There is no mention of SW, BC, and IS. This mechanism does not touch IA and CC.

Incentives to send historical blocks. When a new node joins a blockchain network, it needs to initiate a request to the full nodes for obtaining historical block records. However, a selfish full node may refuse to send the records to this node due to selfish reasons like bandwidth consumption. Therefore, researchers proposed some reward-based incentive mechanisms for motivating the full nodes to enthusiastically send historical block data.

Wang and Wu [88] proposed that the new node should reward the full node that delivers the historical block record. In the mechanism, both parties need to lock some coins. If the new node agrees to pay p coins to the full node, then it needs to lock $2p$ coins, and the full node locks p coins. Only with the signatures of both nodes can the locked coins be retrieved. According to the equilibrium analysis after modeling the interactions of the new node and the full node as a non-cooperative game that both nodes want to maximize their benefits, the best strategy for the full node is to send the complete and real historical block records, and the best strategy for the new node is to request the historical block records and pay the corresponding reward. Therefore, this mechanism satisfies IT and IC. The coin-locking strategy achieves IF. However, a micro-payment channel is added to the incentive mechanism, so that the mechanism does not satisfy BC. There is no evidence to evaluate whether the incentive mechanism fulfills SW and IS. We do not need to consider IA and CC.

Incentives to execute contracts. As the initiator of Blockchain 2.0, the Ethereum blockchain is currently very prevalent due to the support of smart contracts. However, Aldweesh et al. [2] found that in the Ethereum blockchain, the incentives for miners to execute contracts are not proportional to the cost of miners, which could lead to the imbalance of incentives and adversely affect reliable operation of the Ethereum blockchain.

Both PoW and PoS reward miners that own the majority of resources, such as computing power and stakes. Dai et al. [22] introduced a new consensus mechanism, which is called **Proof of Value (PoV)**. PoV rewards the smart contracts that generate a value. PoV regards the token transaction volume in a smart contract as the value of this smart contract. Once the smart contract is successfully invoked, the system will issue the rewards to its owners. The higher the transaction volume of the smart contract is, the more token rewards its owner receives. Furthermore, PoV also introduces incentive parameters to adjust the production speed of tokens. Due to no specific description on token reward distribution, it is impossible to comment on the efficiency of this incentive mechanism.

Incentives to participate in application systems. The blockchain technology has been applied into various scenarios, such as transportation, power grids, data transfer [28] and collection [58], trust evaluation [59, 93] and trustworthy authentication [30], which opened the Blockchain 3.0 era. The entities of these blockchain-based systems are profit-driven and rational; therefore, incentive mechanisms are essential to encourage their participation willingness.

Hu et al. [39] designed an incentive mechanism to encourage participation willingness in a multi-microgrid system. They proposed a collaborative intrusion detection method based on blockchain to improve the accuracy of detection results. Each microgrid node generates detection targets through a periodic trigger mode. All nodes reach a consensus on the detection results with the DPoS consensus mechanism. The detection results are stored in blocks. In this mechanism, the detection coefficients of the nodes are regarded as stakes. When a node generates a block, it will not only obtain economic incentives but also gain an increase in its detection coefficient, which will enhance its probability of mining the next block. But if the node behaves dishonestly, then its detection coefficient will decrease. The incentive mechanism encourages a single microgrid to participate in consensus and improves the detection accuracy of this system. The mechanism satisfies IR, IT, and IC. The authors did not consider IP. The mechanism is not automatic and it does not meet IA. IF, SW, BC, and IS were not mentioned in this work. We do not need to consider CC.

Lei et al. [53] proposed a two-chain structured scalable public blockchain, named Groupchain, for fog computing in IoT. Groupchain contains two kinds of blocks: group blocks and vice blocks. Miners employ PoW to generate group blocks and become members of a leader group. Each leader group member can submit vice blocks that contain transactions. The vice block submitted by one member must be collectively signed by the other group members for being regarded as a valid block and linked to the blockchain. To encourage more miners to join the Groupchain network, the author included a bonus mechanism based on a Coinbase reward and transaction fees. Furthermore, additional compensation will be given to miners who have failed in the competition of becoming a member of the leader group. Therefore, the mechanism meets IF. The paper does not give a detailed introduction to the bonus mechanism, but it ensures that the miners' income is non-negative so that rational miners can join the Groupchain network. Unfortunately, the authors did not consider IA and IP. It is hard to judge whether this incentive mechanism fulfills other requirements.

4.1.2 Incentives to Cooperate.

Incentives to comply with system design. With the widespread utilization of blockchain technology and the implementation of incentive mechanisms to encourage participation, more and more users are willing to join the blockchain network. However, the lack of centralized regulation of user behavior, along with the selfish and profit-driven characteristics of massive users, brings a non-cooperation problem to the blockchain systems. Researchers have proposed some effective incentive mechanisms for motivating selfish nodes to comply with the system design.

The Bitcoin protocol stipulates that miners should mine based on the latest known block in the main chain (also called Frontier strategy). However, selfish miners may deviate from this rule for deliberately generating a fork and obtaining more block rewards than behaving normally. Koutsoupias et al. [50] suggested an incentive mechanism to motivate miners to follow the Frontier strategy. Specifically, a miner that finds a block should pay forward a certain reward to the first miner that successfully mines based on his block. This new mechanism incentivizes other miners to continue mining on specific branches. This pay-forward method increases the cost of dishonest mining and incentivizes miners to follow the Frontier strategy, thus improving system stability. Meanwhile, the incentive mechanism encourages a miner to mine based on the latest block it received, thus increases the probability of extending the main chain, so the mechanism meets IC and

IT. However, the income earned by miners is not proportional to their payments. The pay-forward incentive aims at miners with high computational abilities. So, the mechanism does not satisfy IF. Since it modifies the original protocol of blockchain, it does not support BC. SW and IS were not mentioned. And the authors did not consider IA and CC.

Szalachowski et al. [79] revised the Bitcoin consensus mechanism and proposed Strongchain to make the mining process transparent. Strongchain adopts a weak solution, the difficulty of finding which is lower than the difficulty required to mine a block. When a miner finds and releases a weak solution, the remaining miners continue to solve the PoW puzzle on the basis of the weak solution. Such a method utilizes all resources to generate a block in a joint way and avoids computation resource waste, unlike the Bitcoin system. Strongchain rewards not only a miner that generates a final block but also a miner that finds a weak solution. Such a reward-based incentive mechanism motivates miners with weak solutions to broadcast their solutions and other miners will actively attach these weak solutions to their solutions. Miners cannot benefit if violating the consensus protocol, so the reward mechanism meets IC and IT. The reward for the miner with weak solutions is related to its contribution, which ensures that the reward mechanism satisfies IF. The reward mechanism does not introduce any significant overhead or calculations, which meet BC. According to the experiment, the reward gap for miners with different computation powers is not large, which avoids the loss of small miners and the monopoly of large miners, so this mechanism satisfies IS. SW was not mentioned in this work. IA and CC were not considered, either.

Incentives not to launch attacks. As we specified before, a selfish miner may refuse to publish and distribute a valid block to the rest of the network and then continues to mine the next block and maintains its leading position. When the rest of the network is about to catch up with the selfish miner, the miner then releases a portion of discovered blocks into the network. Such a selfish attack damages the fairness of the blockchain network. Some studies focus on preventing selfish attacks of miners, as presented below.

Eyal et al. [26] proposed a novel protocol Bitcoin-NG, which improves the throughput and delay of Bitcoin protocol to a certain extent. In Bitcoin-NG, time is divided into epochs, blocks are divided into microblocks and key blocks. Transactions are all placed in microblocks. The consensus process of Bitcoin-NG is divided into two parts. First, a leader is elected through PoW, and then the leader produces microblocks. The purpose of the revised consensus mechanism in Bitcoin-NG is to expand the longest and heaviest chain that is distinguished from chain length and weight. The weight of a chain refers to the number of key blocks on the chain. In Bitcoin-NG, the incentive for miners is still derived from Coinbase reward and transaction fees. To obtain all the transaction fees of microblocks, leader miners will detain microblocks and mine on microblocks to become the leader of the next epoch. Therefore, to motivate miners to follow the extended longest and heaviest chain protocol and avoid selfish mining attacks, the authors concluded based on mathematical calculations that 60% of the transaction fees obtained by the miners of the current epoch through packaging transactions should be distributed to the leaders of the next epoch, and the remaining 40% can be its final reward. This distribution mechanism makes miners obtain fewer benefits if launching selfish mining attacks on the blockchain system than the benefits obtained by following the protocol so that the incentive mechanism meets IC and IT. Compared with the leader miner of the current epoch, the leader miner of the next epoch that follows the protocol makes more contributions to the stability of the system, thus receives more transaction fee rewards, so the mechanism satisfies IF. SW, BC, and IS were not mentioned in this work and IA and CC were not considered, either.

However, Yin et al. [96] discovered some defects in the analysis of Bitcoin-NG incentive mechanisms. When analyzing a mathematical inequality to avoid selfish mining attacks, Eyal et al. [26]

did not consider a scenario where the current leader that mines honestly becomes the leader of the next epoch. Namely, the longest chain extension is over-simplification in Reference [26]. Yin et al. thoroughly reanalyzed the incentive mechanisms and presented an optimal proportion of transaction fee distribution. The final result is that the optimal ratio of transaction fee allocation is $\frac{3}{11}$ and $\frac{8}{11}$.

When a miner holds 51% of the total computing power, it can launch a double-spending attack for obtaining extra profits. This miner can change the information on the main chain arbitrarily, which greatly damages the security, fairness, and decentralization of the blockchain network. Therefore, incentive mechanisms that can resist double-spending attacks are highly needed.

Chen and Wang [16] proposed a sharding protocol with no data overhead using a two-layer architecture. One layer is the root chain to ensure system security by occupying most of computation power over the whole system and the other layer is based on shards to increase system throughput. To resist the double-spending attack initiated by miners, it is necessary to ensure that most of the computation power over the whole system is contributed to the root chain. In addition, the computation power of the shard is uniformly distributed in each shard to guarantee it can work functionally. The rewards to miners in shards and root chain are satisfied with the following equation:

$$\frac{BlockReward(root)}{BlockReward(block)} = \frac{HashPower(root) \times BlockIntervalBlockInterval(root)}{HashPower(shard) \times BlockIntervalBlockInterval(shard)}. \quad (1)$$

This reward distribution mechanism meets IR and IT. This mechanism can incentivize miners to distribute their hash computation power reasonably, thus the mechanism meets IC. However, IF, SW, BC, and IS were not considered in the incentive mechanism, neither IA and CC.

In addition to attacks on blockchain networks, miners can also conduct BWA on mining pools. After a miner successfully mines a block, it withholds this block without broadcasting, thus the mining pool cannot get the reward from the block. This attack caused great losses to the mining pool. The following works aim to resist the BWA.

Bag and Sakurai [7] analyzed the utility function of a BWA attacker and proposed a special reward-based incentive mechanism to reduce the incentives of the attacker. The miner that solves the PoW puzzle and submits the full PoW solution to its mining pool will receive a special reward. The remaining revenue for finding a new block will be distributed to all miners according to the shares they submit. The miner who launches BWA to the mining pool cannot receive a special reward. The reward distribution scheme enables the incentive mechanism to meet IF. The incentive mechanism discourages the attacker to launch the BWA, thus the mechanism satisfies IC and IT. According to theoretical analysis, this mechanism does not reduce the benefits of honest miners but reduces the revenue of the attacker in the long run, thus the incentive mechanism meets IS. There is no discussion on SW and BC of the incentive mechanism. IA and CC were not considered.

Alzahrani and Bulusu [4] proposed a new consensus mechanism based on Tendermint [9]. Each proposer that creates a new block is randomly mapped to a leader, which then randomly selects some nodes (called validators) to validate the newly proposed block. This mechanism improves security by randomly selecting a set of validators when a new block is mined. The protocol involves a reward and punishment based incentive mechanism to regulate the behavior of validators. This Bayesian game-based mechanism adjusts the utility of different behaviors by rewarding honest behaviors and punishing dishonest behaviors. Therefore, the protocol meets IC and IT. The authors also asserted the effectiveness of the proposed mechanism in defending BWA. However, the incentive mechanism needs to update the original protocol and does not meet BC. There is no discussion on IF, SW, and IS of the incentive mechanism. IA and CC were not considered.

A DoS attack destroys the availability of a target system. It attacks the target system's network service function via its defects or directly consumes its system resources, making the target system unable to provide normal services. For blockchain-related systems, attackers employ the DoS attacks to slow down the systems or force them to stop functioning.

The Groupchain network proposed by Lei et al. [53] can be easily attacked by malicious miners due to the small size of the leader group. For example, malicious miners can easily attack the blockchain system through the DoS attack by continuously generating invalid vice blocks that are not resource-consuming. Therefore, the authors proposed a deposit-based incentive mechanism to prevent the DoS attack. New members that join the leader group need to pay deposits to historical members. If a member behaves honestly in a specific period, then the deposits will be returned. Otherwise, the deposits are assigned to the historical members. In summary, the deposit mechanism can prevent newly joined leader group members (miners) from launching DoS attacks. The income of new members is non-negative, so the mechanism meets IR. The authors did not consider IA and IP. The paper does not give a detailed introduction to the deposit mechanism, so we cannot judge if this mechanism can meet other requirements.

4.2 Reputation-based Incentive

Compared with monetary incentives, reputation-based incentives pay more attention to encouraging nodes to collaborate. The reputation-based incentives usually apply reputation values to regulate node behaviors. For example, setting reputation thresholds can motivate the nodes to behave cooperatively for keeping their reputation values at a high level.

To standardize the mining process in mining pools, Nojoumian et al. [66] proposed a reputation-based paradigm for motivating miners to follow the mining protocol regulated by its mining pool and mine honestly. A mining pool is composed of multiple alliances and the alliance is composed of multiple mutually trusted miners. The members of each alliance share the same reputation value. The reputation value reflects the performance of miners in the system, which is calculated according to their mining performance, honest and dishonest behaviors. A pool manager sends an invitation to the miners according to the reputation value of the miners for forming a new alliance and increasing the mining pool's chance of successful mining. Miners with high reputation values have a high probability of being invited to join the mining pool for gaining more benefits. Therefore, this reputation mechanism can encourage miners to mine honestly. The mechanism meets IR, IC, and IT. The benefit of a miner is proportional to its reputation value; thus, the mechanism satisfies IF. There is no discussion on SW, BC, and IS. IA and CC were not considered.

4.3 Gamified Incentive

Different from monetary incentives and reputation-based incentives, gamified incentives employ the psychological factors of nodes to guide node behaviors. Gamified incentives provide nodes with a sense of accomplishment instead of real benefits such as money and reputation.

Kano and Nakajima [47] provided miners with gamified incentives based on psychological factors to operate services and participate in mining work to solve the problem of centralized mining. The game element is the nonce value in a block corresponding to the shape of the puzzle on a 5 by 5 board. The mining work is performed by a miner through visualized nonce value manipulation, which makes the mining work interesting. The paper does not provide technical details of the incentive method, thus we cannot evaluate if it can satisfy our proposed requirements.

4.4 Hybrid Incentive

Monetary incentives motivate system entities to participate and collaborate from an economic perspective. However, monetary incentives are unable to avoid accidental dishonest behaviors.

Non-monetary incentives usually provide entities intangible rewards and mental satisfaction, which cannot meet the economic demands of entities. Therefore, some scholars proposed hybrid incentives to overcome the shortcomings of monetary incentives and non-monetary incentives.

4.4.1 Incentives to Cooperate. To incentivize miners to comply with protocol design and behave honestly, Han et al. [34] proposed a new consensus mechanism called **Proof-of-Credit (PoC)**, which is a special PoS mechanism that regards credits as stakes. The consensus process is divided into two stages: candidate election and leader election. The first step is to verify whether a node is eligible to become a candidate. After the node becomes the candidate, a certain amount of deposit is required. When the candidate deviates from such an agreement, the deposit is forfeited. The second step is to elect leaders from candidates to generate blocks. The authors proposed a hybrid incentive mechanism that consists of transaction fees incentive and credit incentive. High credit means a high probability of becoming a leader and gaining benefits. All candidates who honestly execute the agreement and broadcast valid candidate blocks will equally share transaction fees, thus this mechanism meets IF. The mechanism can resist selfish mining attacks and double-spending attacks. If an attacker wants to carry out a selfish mining attack, then it risks losing the promised deposit and credit. And an attacker with poor credit will not be selected as a candidate, thus cannot prepare for a fork in advance and conduct a double-spending attack. Therefore, this mechanism satisfies IC and IT. The incentive mechanism needs to update the original protocol, so it does not meet BC. SW and IS were not mentioned while IA and CC were not considered in this paper.

When applying blockchain into Industrial IoT, the security and efficiency of consensus become a main concern. Wang et al. [81] proposed a reputation-based incentive mechanism to encourage miners to behave honestly. Each miner is identified with a reputation value. According to the mechanism, a miner with a high reputation value can generate new blocks with low difficulty. When a miner successfully mines a block and the block is finally confirmed, the miner can obtain reputation rewards and token rewards. When a miner does not generate blocks for a long time or does not generate an expected number of blocks, it will be punished. This reputation mechanism requires users to register with their real identities, so unless an attacker can register with someone else's information, the mechanism can resist Sybil attacks. In the long run, if a miner acts unfavorably to the blockchain system, then its reputation value will decrease, and the difficulty of its mining will increase, which will harm its income. Therefore, the mechanism meets IC, IT, and IS. Its IF and SW cannot be judged. The mechanism does not consider IP. The authors did not deploy the incentive mechanism on the smart contract; thus, the mechanism does not satisfy IA. Its CC is $o(1)$. The incentive mechanism can be built on any Proof-of-X (X stands for any content, e.g., work and stake) protocol and meets BC. Based on Reference [81], Wang et al. [82] considered the situation when the blockchain is applied to IoT and proposed a distributed reputation layer by applying the same incentive mechanism as that in Reference [81].

In a vehicular energy network, renewable energy can be transmitted through **electric vehicles (EVs)** and energy nodes (wireless charging/discharging facilities). When EVs act as energy sellers, energy nodes act as energy buyers and vice versa. Energy nodes are selfish and they may behave dishonestly to maximize their benefits. Wang et al. [87] proposed a secure energy delivery framework based on a consortium blockchain to prevent malicious behaviors of energy nodes, which adopts a reputation consensus protocol. The higher the reputation of an energy node, the higher the probability to mine successfully and receive rewards. The monetary incentive comes from transaction fees charged in energy transactions. At the same time, the energy node that has successfully mined will also get an increase in reputation. When the energy node acts maliciously such as refusal to pay and transaction forgery, its reputation value will decrease. When the

reputation value of a node is lower than a threshold, it will be put into a blacklist. Therefore, each energy node in the network is encouraged to improve its charging/discharging service for EVs and discouraged to behave maliciously to increase its reputation value. The incentive mechanism meets IR, IC, IT, and IF. The mechanism is not automatic and it does not meet IA. The mechanism does not consider IP. There is no discussion on SW, BC, and IS and no need to consider CC.

4.4.2 Incentives to Participate and Cooperate. A reliable and effective vehicle announcement network is required in the Internet of Vehicles. Li et al. [55] proposed a novel blockchain-based privacy-preserving incentive announcement network called CreditCoin to encourage users to participate and honestly forward information. In CreditCoin, traffic tasks are managed by a cloud application server and the transactions between users are forwarded through the blockchain network. After constructing a transaction, the user forwards the transaction to nearby **roadside units (RSUs)**, and then the RSUs vote on the validity of the transaction. Later, a consensus server confirms the valid transactions and adds them into the blocks on the chain. To encourage users to participate in the network and forward traffic information honestly and reliably, a reputation-based incentive mechanism is proposed. The reputation points are called coins. Users receive coins by forwarding or receiving data packets, which encourages them to be online and keeps the network active. In a certain period, unused coins will be halved to prevent the accumulation of coins that can be used for attacks. The mechanism meets IR, IC, and IT. This incentive mechanism achieves conditional privacy by tracing malicious nodes when an unexpected event occurs, therefore, it meets IP. This incentive mechanism needs to update the system, so it does not satisfy BC. The mechanism is not automatic, thus IA cannot be supported. IF, SW, and IS were beyond discussion and there is no need to consider CC.

5 BLOCKCHAIN-BASED INCENTIVE MECHANISMS

So far, we have already reviewed the effectiveness of involving incentive mechanisms to motivate participation willingness and suppress non-cooperation behavior in blockchain in Section 4. We will further investigate how blockchain technology can contribute to incentive mechanism design in this section. Specifically, we review blockchain-based incentive mechanisms by hierachically classifying existing works according to incentive forms, application scenarios, and then incentive goals. We summarize the main contributions of each work and comment on their pros and cons in Table 3 based on the proposed requirements. We study how blockchain can benefit incentive mechanisms by removing centralized parties herein. Since the structure of previous centralized incentive mechanisms is converted to distributed ones, BC cannot be fulfilled in all incentive mechanisms presented in this section.

5.1 Monetary Incentive

5.1.1 Crowdsensing. A crowdsensing system employs terminal devices (or mobile users) as the sensors to collect and process data. The crowdsensing system needs to collect large-scale sensory data, therefore requires the participation of a large number of devices. However, the devices will face some issues after participation. The collected data may contain private information (like location) of the devices. Moreover, the sensing tasks consume resources like batteries. Therefore, rational users refuse to participate in crowdsensing without enough incentives. An incentive mechanism is needed to motivate various devices to participate. Unfortunately, existing centralized incentive mechanisms rely on a centralized platform to execute, which is impractically assumed to be trusted. Moreover, single-point failure problem also exists in centralized incentive mechanisms. Blockchain can employ appropriate consensus mechanisms to get rid of the dependence on a trusted centralized platform and eliminate the single-point failure problem [29]. How

Table 2. Summary of Incentive Mechanisms in Blockchain

Reference	Blockchain Version	Blockchain Type	Consensus Mechanism	Incented Entity	Incentive Goal	Incentive Form	Incentive Model	IR	IC	IT	IF	SW	IA	IP	IS	SC	CC	BC
[54]	1.0	–	Directed Acyclic Graph	Miners	Participation	Monetary incentive	Inclusive model	Y	N	N	Y	–	*	*	Y	*	*	–
[6]	1.0	Public blockchain	PoW	Broadcasting nodes	Participation	Monetary incentive	Hybrid reward scheme	Y	Y	Y	–	–	*	*	–	*	*	–
[1]	1.0	Public blockchain	PBFT	Broadcasting nodes	Participation	Monetary incentive	Fee sharing with same rewards	Y	Y	Y	–	–	*	*	–	*	*	–
[24]	1.0	Public blockchain	Not restricted	Broadcasting nodes	Participation	Monetary incentive	Fee sharing with different rewards	Y	Y	Y	Y	–	*	*	–	*	*	–
[88]	1.0	Public blockchain	–	Full nodes	Participation	Monetary incentive	Coin-locking strategy	Y	Y	Y	Y	–	*	*	–	*	*	N
[22]	2.0	Public blockchain	PoV	Owners of smart contracts	Participation	Monetary incentive	Token reward distribution model	Y	–	–	–	–	Y	–	–	*	*	–
[39]	3.0	–	DPoS	Microgrid nodes	Participation	Monetary incentive	Economic incentive and detection coefficient model	Y	Y	Y	–	–	N	N	–	*	*	–
[53]	3.0	Public blockchain	PoW	Miners	Participation	Monetary incentive	Bonus mechanism	Y	–	–	Y	–	N	N	–	*	*	–
[50]	1.0	Public blockchain	PoW	Miners	Cooperation	Monetary incentive	Pay forward	Y	Y	Y	N	–	*	*	–	*	*	N
[79]	1.0	Public blockchain	PoW and weak solution	Miners	Cooperation	Monetary incentive	Weak solution reward mechanism	Y	Y	Y	Y	–	*	*	Y	*	*	Y
[26]	1.0	Public blockchain	Leader election and leader generates microblocks	Miners	Cooperation	Monetary incentive	Transaction fee distribution ratio: 40%–60%	Y	Y	Y	Y	–	*	*	–	*	*	–
[16]	1.0	Public blockchain	PoW	Miners	Cooperation	Monetary incentive	Reward distribution mechanism	Y	Y	Y	–	–	*	*	–	*	*	–
[7]	1.0	Public blockchain	PoW	Miners of mining pools	Cooperation	Monetary incentive	Special reward	Y	Y	Y	Y	–	*	*	Y	*	*	–
[4]	1.0	Public blockchain	Leaders randomly select validators	Validators	Cooperation	Monetary incentive	Reward and punishment model	Y	Y	Y	–	–	*	*	–	*	*	N
[53]	3.0	Public blockchain	PoW	Miners	Cooperation	Monetary incentive	Deposit mechanism	Y	–	–	–	–	N	N	–	*	*	–
[66]	1.0	Public blockchain	PoW	Miners of mining pools	Cooperation	Reputation-based incentive	Reputation-based paradigm	Y	Y	Y	Y	–	*	*	–	*	*	–
[47]	1.0	–	PoW	Miners	Participation	Gamified incentive	Visualized values	–	–	–	–	–	*	*	–	*	*	–
[34]	1.0	Public blockchain	PoC	Miners	Cooperation	Hybrid incentive	Credit incentive and transaction fee incentive	Y	Y	Y	Y	–	*	*	–	*	*	N
[81]	3.0	–	–	Miners	Cooperation	Hybrid incentive	Reputation rewards and token rewards	Y	Y	Y	–	–	N	N	Y	*	$o(1)$	Y
[87]	3.0	Permissioned blockchain	Proof of Reputation	Energy nodes	Cooperation	Hybrid incentive	Reputation model and mining reward	Y	Y	Y	Y	–	N	N	–	*	*	–
[55]	3.0	Public blockchain	BFT-based consensus	Vehicle nodes	Participation and cooperation	Hybrid incentive	Reputation model and coin model	Y	Y	Y	–	–	N	Y	–	*	*	N

Y: satisfied; N: unsatisfied; –: not mentioned or specified; *: untouched or no need to be considered.
IR: Individual Rationality; IC: Incentive Compatibility; IT: Incentive Truthfulness; IF: Incentive Fairness; SW: Social Welfare Maximization; IA: Incentive Automation; IP: Incentive Privacy; IS: Incentive Sustainability; SC: Incentive Scalability; CC: Computational Complexity; BC: Backward Compatibility.

Table 3. Summary of Blockchain-based Incentive Mechanisms

Reference	Application Scenario	Blockchain Type	Consensus Mechanism	Incented Entity	Incentive Goal	Incentive Form	Incentive Model	IR	IC	IT	IF	SW	IA	IP	IS	SC	CC	BC
[83]	Crowdsensing	Public blockchain	–	Mobile users	Participation	Monetary incentive	Cryptocurrency-based reward	Y	Y	Y	Y	–	N	Y	–	–	*	N
[95]	Crowdsensing	Permissioned blockchain	–	Vehicle users in general tasks	Participation	Monetary incentive	Bidding mechanism	Y	–	Y	–	–	Y	N	–	N	–	N
[95]	Crowdsensing	Permissioned blockchain	–	Vehicle users in urgent tasks	Participation	Monetary incentive	Time-window-based method	Y	–	Y	–	–	Y	N	–	N	$O(n)$	N
[40]	Crowdsensing	Ethereum blockchain	PoW	Users	Participation	Monetary incentive	Stackelberg game	Y	–	–	Y	–	Y	Y	Y	–	*	N
[76]	Cloud computing	Consortium blockchain	–	Data owners	Cooperation	Monetary incentive	Shapley value	Y	Y	Y	Y	–	Y	N	–	–	*	N
[23]	Cloud computing	–	–	Computing cloud	Cooperation	Monetary incentive	Contract-based incentive	Y	Y	Y	–	–	Y	N	–	N	*	N
[17]	Internet of Vehicles	Consortium blockchain	–	Data seller	Participation	Monetary incentive	Auction-based incentive	Y	Y	Y	Y	Y	Y	N	–	Y	$O(n)$	N
[18]	Internet of Vehicles	–	PBFT	Electric vehicles	Participation	Monetary incentive	Contract-based incentive	Y	Y	Y	–	–	Y	N	–	–	*	N
[21]	Data sharing system	Public blockchain	PoW	Mobile devices	Participation	Monetary incentive	Mining rewards	–	–	–	–	–	N	N	–	N	*	N
[103]	Data sharing system	–	–	Data owners	Participation	Monetary incentive	Shapley value	Y	Y	Y	Y	–	Y	N	–	–	*	N
[32]	Location-based services	–	–	Mobile users	Participation	Monetary incentive	Single-round sealed-bid double auction	Y	Y	Y	–	–	Y	Y	-	–	Polynomial time	N
[13]	Delay tolerant network	–	–	Forwarder nodes	Cooperation	Monetary incentive	Bitcoin reward distribution model	Y	Y	Y	–	–	N	N	–	–	*	N
[89]	Content distribution	–	–	Content helpers	Cooperation	Monetary incentive	Prepayment and deposit mechanism	Y	–	–	–	–	Y	N	–	–	*	N
[3]	Internet of Things	Consortium blockchain	Proof-of-Authority	Service providers	Cooperation	Reputation-based incentive	Reputation model	Y	Y	Y	Y	–	Y	N	–	–	*	N
[36]	Machine learning	Public blockchain	–	Participants	Participation	Gamified incentive	Gamified incentive framework	–	–	–	–	–	Y	N	–	–	*	N
[46]	Crowdsensing	Ethereum blockchain	–	Workers	Participation and cooperation	Hybrid incentive	Basic incomes and quality commissions, and reputation model	Y	Y	Y	Y	–	Y	Y	–	–	*	N
[101]	Cloud computing	Ethereum blockchain	–	Witness	Participation and cooperation	Hybrid incentive	Economic incentive and auditing model	Y	Y	Y	Y	–	Y	N	–	–	*	N
[15]	Internet of Vehicles	–	–	Drivers	Participation and cooperation	Hybrid incentive	Monetary rewards and reputation evaluation	Y	–	–	Y	–	Y	N	–	N	*	N
[52]	Internet of Vehicles	–	–	Drivers	Participation and cooperation	Hybrid incentive	Monetary and reputation model	Y	Y	Y	Y	–	Y	N	–	N	*	N
[99]	Data sharing system	–	–	Data owners	Participation and cooperation	Hybrid incentive	Quality-of-Service and reputation mechanism	Y	Y	Y	Y	–	Y	N	–	–	*	N

Y: satisfied; N: unsatisfied; –: not mentioned or specified; *: untouched or no need to be considered.
IR: Individual Rationality; IC: Incentive Compatibility; IT: Incentive Truthfulness; IF: Incentive Fairness; SW: Social Welfare Maximization; IA: Incentive Automation; IP: Incentive Privacy; IS: Incentive Sustainability; SC: Incentive Scalability; CC: Computational Complexity; BC: Backward Compatibility.

to design decentralized incentive mechanisms based on blockchain has been investigated by many researchers.

To motivate mobile users to participate in crowdsensing, Wang et al. [83] proposed a blockchain-based incentive mechanism to realize privacy protection and provided cryptocurrency-based incentives to rational mobile users. After a server publishes a task, each user decides whether to accept the task according to its individualized task cost and the published reward by the server. After accepting a task, the user needs to upload correspondingly sensed data to the blockchain network. Miners evaluate the data quality according to an **expectation maximization (EM)** algorithm and apply the amount of mutual information to quantify the user's contribution. The server pays the users according to the evaluation results from miners. A signcryption method and a K-anonymity method are adopted to prevent miners from obtaining the user's private information when verifying data and identifying messages. Thus, the incentive mechanism meets IP. The evaluation of data quality enables the server to reward a large amount of incentive to the users with high data quality. Furthermore, the server needs to deposit some cryptocurrencies in advance to prevent it from refusing to pay. Therefore, the mechanism meets IF. The mechanism can incentivize users to provide truthful data, it meets IT and IC. However, the mechanism is not automatic and it does not meet IA. In this paper, the authors considered maximizing the social welfare of servers and users, without considering the social welfare of miners. So, we cannot judge whether the mechanism satisfies SW. There is no discussion on IS, SC, and CC.

Yin et al. [95] proposed a bidding mechanism with time constraints and quality requirements for general tasks that need to impractically collect data. The task issuance, bid information submission, and reward allocation are all executed through smart contracts. Users submit bid prices, data quality and available periods for bidding and a center considers its budget and data quality requirements and selects some winning users on the premise of maximizing its own interests. When a large number of users submit related data, the center is overburdened, so the mechanism does not satisfy SC. The users that complete the task will receive tokens as a monetary reward. The mechanism ignores requests for excessive bidding prices, thus avoiding malicious bidding. Furthermore, a user that cannot provide data with promised quality will not be rewarded and can no longer participate in any crowdsensing tasks. Therefore, the bidding mechanism meets IT. However, the bid information is reviewed by the center so that the center can observe the specific information of the bid and guess user preferences, which violates the privacy preservation requirement; thus, the mechanism does not meet IP. Each rational user bids at a price higher than its resource consumption cost, so its income is non-negative and the bidding mechanism meets IR. This mechanism is executed through a smart contract and it meets IA. Unfortunately, this paper does not specify the details of reward distribution, so it is impossible to judge whether the bidding mechanism satisfies IC and IF. Whether a vehicle bid is the optimal bid of the vehicle to maximize its benefits is unknown, so it is not sure whether the bidding mechanism meets SW. CC and IS cannot be judged, either.

Single-user resources may not be sufficient enough to complete urgent tasks with delay sensitivity; therefore, multiple users should be motivated to complete the same tasks. The authors of Reference [95] proposed a multi-user collaboration mechanism based on a time window, which employs idle time between assigned tasks and idle resources of multiple users to handle urgent tasks. The assignment of tasks is accomplished by auction. The auction progress runs on a smart contract, thus this mechanism satisfies IA. The profit for the user that completes the emergent task is calculated according to its contribution to the accomplishment of this task. Simulation results show that the profits of each user increase with the rise of the number of cooperative users, which implies that more and more users would like to join the collaboration to complete emergent tasks. The time window improves the resource utilization rate of the user and shortens its task

completion time. Similar to the auction mechanism for general tasks, this mechanism does not pay attention to protecting the private information of the user, thus, the incentive model does not meet IP. And there is also a center for selecting users, so the model does not satisfy SC. But this method can still prevent users from false bidding and submitting false data, which meets IT. The user's income is non-negative, so this method meets IR. The CC of this incentive mechanism is $O(n)$. Similarly, it is hard to judge whether this mechanism fulfills the requirements of IC, IF, SW, and IS.

Hu et al. [40] considered long-term collection of high-quality sensory data under budget constraints and proposed a game theory-based incentive mechanism. Users are divided into two types, one is monthly salary users and the other is part-time users. A three-stage Stackelberg game is proposed to model the interactions between task initiators and monthly salary users. They applied blockchain to anonymize user identities; therefore, the incentive mechanism satisfies IP. The Stackelberg equilibrium helps fairly allocate tasks and rewards, thus it satisfies IF. The incentive mechanism makes use of smart contracts. Therefore, it meets IA. The mechanism maximizes the utility of task initiators and participants and incentivizes monthly salary participants to provide data sustainably, thus, the mechanism satisfies IS. IC, IT, SW, and SC were not mentioned in this paper. We do not need to consider CC.

5.1.2 Cloud Computing.

Incentives to comply with system design. To achieve safe and collaborative sharing of data in multiple clouds, Shen et al. [76] proposed a Shapley value-based revenue distribution incentive mechanism and used smart contracts to manage the flow of payments, which avoids denial of contract parties. According to experimental results, the incentive mechanism can successfully encourage data owners to provide real data. It distributes revenue based on the contributions of all parties, therefore, the mechanism satisfies IF and IA. If the data owners want to increase their profits, then they must honestly provide high-quality data, so this mechanism meets IC and IT. However, the incentive mechanism does not consider IP. And we cannot judge whether the incentive mechanism meets SW, IS and SC. CC is not related to the evaluation of this incentive mechanism.

Incentives not to launch attacks. With the development of cloud computing, verifiability has become a key issue to ensure the correctness of the programs executed in the cloud and further accelerated the application of cloud computing. There is an urgent need for a method with a reasonable cost to realize the verifiability of cloud computing. Dong et al. [23] proposed a method in which a client makes two clouds compute for the same task and cross-validates their results. The authors proposed a contract-based incentive mechanism to prevent two clouds from collusion by applying game theory and smart contracts, which supports IA. The two cloud needs to pay a certain amount of deposit. The deposit will be returned to the honest cloud while the deposit of the dishonest cloud will be confiscated and be regarded as a reward to the honest cloud. A prisoner contract is designed to eliminate collusion between clouds. Specifically, this contract rewards the cloud that reports collusion and punishes the dishonest cloud. This mechanism allows untrusted clouds to participate and encourages them to be honest. It ensures that the cloud can improve its interests if acting honestly; otherwise, it will be punished even more, so it meets IC and IT. When there is a dispute between the computing results of the two clouds, a third party will appear to resolve the dispute. Since the third party is not completely credible and may leak client data, thus, the incentive mechanism does not meet IP. Meanwhile, the existence of the third party will restrict the scalability of the incentive mechanism, thus the mechanism does not satisfy SC. We cannot judge whether the mechanism meets IF, SW, and IS. CC was not discussed in this work. Generally, CC is duplicated, since it applies dual cloud servers.

5.1.3 Internet of Vehicles. To encourage users to participate in data collection and sharing, and to solve the problem of data sharing in IoV applications, Chen et al. [17] proposed an auction-based incentive mechanism with the help of a consortium blockchain. Its auction procedure goes like follows. A data requester sends its data request to an auction platform and some data sellers collect requested data. Then the data sellers send their partial data to the auction platform. The platform adopts two algorithms to determine winning data sellers and the payment price based on the EM algorithm, respectively. At last, the winning data seller sends the complete data to the platform. RSUs work as miners to include transactions into blocks and link blocks to the blockchain. The mapping relationship between the user (data seller and data requester) information and the account name is stored in a database of a trusted organization. However, the third party is not completely trusted, so there still exists the risk of privacy leakage, thus the incentive mechanism does not meet IP. The utility of the data seller is non-negative, so the mechanism meets IR. The data sellers can get expected rewards due to employment of smart contract, which avoids denial of payment. Therefore, the mechanism meets IF and IA. The data sellers cannot obtain high benefits by submitting low-quality data, so the incentive mechanism meets IC. The data seller normally submits a real cost estimate when bidding, so the incentive mechanism satisfies IT. Social welfare from the perspective of the platform can be regarded as the social welfare of the system. The goal of this incentive mechanism is to maximize social welfare from the perspective of the platform. So, it meets SW. CC of this mechanism is $O(n)$, and it remains linear as the number of data sellers increases, thus the mechanism meets SC. Unfortunately, the fulfillment of IS is unknown.

Electric vehicles can be charged and discharged to solve the problem of regional energy shortages. But the owners of electric vehicles have no incentive to trade electricity. Chen et al. [18] proposed an incentive smart contract based on game theory to balance and optimize the interests of vehicles in electric power transactions. When the smart contract is triggered, the system automatically calculates incomes according to all possible decisions of two vehicles in the game and finds the optimal strategies for both vehicles. Then the two vehicles complete a power transaction and settle funds. They will receive energy coins based on their contributions after the transaction is completed. Therefore, the incentive smart contract meets IA and IR. When the electric vehicles launch a collusion attack, the energy currency rewards they received will be reduced. Hence, the incentive smart contract forces the electric vehicles to be cooperative, and meets IC and IT. The authors did not consider IP. We have no way to know whether the incentive meets other requirements. CC was not considered.

5.1.4 Others. This part mainly reviews incentive mechanisms in other application scenarios besides crowdsensing, cloud computing, and IoV. We divide these incentive mechanisms into two categories according to incentive goals: participation and cooperation.

Incentive to participate in application systems. Some papers do not focus their studies on specific scenarios. However, with the development of big data and artificial intelligence technologies, a large amount of data needs to be collected, so many studies focus on data sharing.

Cui et al. [21] proposed an incentive mechanism to encourage mobile devices to share data, which regards mining rewards as motivation. If a mobile device is willing to share data with other devices, then a base station will allocate the corresponding amount of computing power to the mobile device according to the shared data size. The mobile device applies the assigned computing power to mine and obtains the corresponding mining rewards. The relationship between the amount of computing power allocated and the size of the shared data can be linear or non-linear. If the linear relationship is formulated, then the mobile devices will allocate more cache to data with higher popularity, while the optimal strategy is to cache evenly when a non-linear relationship is formulated. When the number of mobile devices increases, the workload of the base station

increases, which limits the scalability of the mechanism. The mechanism does not satisfy the requirement of SC. This mechanism does not mention how mining rewards are distributed to mobile devices. Mobile devices may not receive the rewards they deserve, and it is also possible that the rewards for some mobile devices that share small data are not enough to offset their costs. Therefore, we cannot judge the properties of this incentive mechanism. This mechanism does not satisfy IA, nor does it consider IP.

Artificial intelligence companies use large amounts of medical data to build and train models and cooperate with medical institutions to provide diagnostic services for patients. Accurate diagnosis services require a large amount of real medical data for training. Zhu et al. [103] proposed a blockchain-based medical data sharing model based on the cooperation of all parties for patient diagnosis. The parties include a third party that builds training models, miners that maintain the blockchain, and data owners that provide training data. The income of the model is provided by patients who need to be diagnosed. The model uses Shapley value for income distribution and applies smart contracts to automatically control income distribution. The income of the data owner is allocated according to the contribution of his/her data quality to the training model, so he/she must provide real data for gaining a high profit. Therefore, the incentive model fulfills the requirements of IT and IC. The adoption of Shapley value realizes fair income distribution. And the use of smart contracts to distribute income prevents payment denial and realizes convenient and effective payment. Therefore, the incentive model meets IF and IA. However, the third party holds access to medical data, thus the model does not satisfy IP. The incentive model does not consider SW, IS and SC. CC is not suitable to be considered for evaluating this incentive model.

A location-based service requester needs to provide its location information to a service provider; therefore, the requester's privacy may be violated. K-anonymity is a commonly applied method for protecting location privacy. It is necessary to form a K anonymous group through cooperation with other mobile users that pay little attention to location privacy. However, the other mobile users have no motivation to participate in the anonymous group. Therefore, it is necessary to investigate an incentive mechanism for motivating mobile users to join the K anonymous group. Yang et al. [94] designed a single-round sealed-bid double auction as the incentive mechanism to motivate mobile users to join the K anonymous group. However, the auction is built based on a trusted intermediary agent. To remove this impractical assumption, Geng et al. [32] implemented the incentive mechanism proposed in Reference [94] with a smart contract for achieving a decentralized incentive mechanism. The application of the smart contract ensures that the incentive mechanism satisfies IA. To prevent an attacker from identifying a service requester through the transaction records, the authors constructed a public contract and a private contract to achieve the requirement of IP. The public contract is encrypted by group signature and verified by blind signatures. The private contract is only visible to the K anonymous group members for privacy preservation. The incentive mechanism treats service requesters as buyers for bidding, and other mobile users as sellers for pricing. The incentive mechanism encourages the buyers to provide realistic valuations and motivates the sellers to reveal its real costs, which meets IT and also IC. It also guarantees that the utilities of buyers and sellers are non-negative; thus, the mechanism meets IR. Regarding CC of the incentive mechanism, it is in polynomial time. SW, IF, IS and SC are unknown.

Incentives to cooperate: Comply with system design. To improve the efficiency of content distribution, maintain the control of **Content Providers (CPs)** in the process of distribution, and prevent coordinating **Content Helpers (CHs)** from occupying too much market share, Wu et al. [89] proposed a novel content distribution framework and constructed an incentive mechanism with smart contract. A CP issues payment to the CHs for content delivery. The CHs need to deposit

to the CP before content delivery. The prepayment and deposit are both managed by the smart contract. When the content is successfully distributed and the CH has obtained a verified delivery certificate, it can successfully receive the payment from CP and its deposit will be returned. However, if the CH is detected to be over-distributed or failed in delivery certificate verification, then its deposit will be confiscated. This mechanism can restrain the CH from colluding to obtain a fake delivery certificate to a certain extent. However, the paper does not give a detailed design of this mechanism, so we cannot compare punishments and benefits when CH is dishonest. Therefore, we cannot judge IC, IT, IF, SW, and IS. The authors did not consider IP. Smart contracts were used to achieve transparency and automation; thus, the mechanism satisfies IA. SC and CC were not considered.

Incentives to cooperate: Not launch attacks. The performance of a delay-tolerant network will be affected by selfish nodes that do not participate in message forwarding. Moreover, selfish behavior will lead to low delivery rates and long transmission delays. Chakrabarti and Basu [13] proposed a blockchain-based incentive mechanism to eliminate the selfish behavior in the delay-tolerant network. In this mechanism, the forwarder-nodes that successfully deliver messages will receive bitcoins as a reward according to a reward distribution method. Each intermediate forwarder-node will pay a certain amount of reward to the next-hop forwarder to collect a digitally signed acknowledgment (as a sign of cooperation). The revenue of the forwarder-node is non-negative, the model meets IR. When the forwarder-node wants to maximize the revenue, it will reduce the number of propagation hops, at the same time, the message delivery delay is reduced, so the incentive mechanism satisfies IC. To prevent the forwarder-node from being dishonest, when the message is successfully delivered, the reward can only be obtained after the digital signatures of the subsequent forwarder-nodes are confirmed. Therefore, the model meets IT. But the realization of the incentive mechanism is not automatic, so the model does not satisfy IA. The author did not consider IP. IF, SW, and IS are unknown. SC and CC were not discussed in this paper.

5.2 Reputation-based Incentive

Alghamdi et al. [3] proposed a security service supply scheme with a fair payment system for **lightweight customers (LC)** of the blockchain and a reputation-based incentive mechanism. The reputation of a **service provider (SP)** is the number of valid transactions. The SP sends a service code to the LC for correctness and it will obtain a reward from LC if the code is correct. The authors applied a smart contract to verify services. Thus, the incentive mechanism meets IA. The reputation mechanism can motivate the SP to provide correct services; therefore, it meets IC and IT. Applying a smart contract ensures fair and effective distribution of rewards, so the mechanism satisfies IF. The authors did not consider IP. SW, IS, and SC are unknown. CC was not touched.

5.3 Gamified Incentive

Machine learning requires a large number of large datasets for training while this kind of dataset is difficult to obtain. To encourage participants to collaboratively construct datasets and improve the availability of trained models, Harris and Waggoner [36] proposed a smart contract to host a continuously updated model. The datasets and trained models are publicly shared on the blockchain. The authors proposed a gamified incentive framework to encourage participants to contribute data to improve the accuracy of the model. The incentive framework uses the willingness of participants as a common good for encouraging the participants to cooperate for free. Besides, it rewards participants with some points and badges. This incentive framework introduces a smart contract to achieve transparency and automation of incentives, thus, it meets IA. This mechanism framework

requires the participants to upload data to the public chain, which leaks privacy. Therefore, the mechanism does not satisfy IP. SC and CC were not considered. Satisfaction of other requirements is unknown due to hardness of judgment or without discussion.

5.4 Hybrid Incentive

The hybrid incentive can not only motivate users to participate but also encourage them to behave honestly or collaboratively. In what follows, we review this part of existing works based on application scenarios.

5.4.1 Crowdsourcing. Kadadha et al. [46] adopted smart contracts to propose a fair and transparent incentive mechanism for improving worker participation in crowdsourcing. On the premise that honest workers submit similar solutions, a similarity evaluation method can be applied to evaluate the quality of solutions. The incomes of workers include basic incomes and quality commissions. The quality commission is proportional to the quality of the solution, which can prevent workers from submitting wrong or low-quality solutions. The reputation values of workers and task requesters are updated after the payment is completed. The reputation of a requester is related to the number of canceled tasks, and the reputation of a worker is related to the quality of its solution. To gain a high reputation, both workers and requesters avoid dishonest behaviors. Therefore, the mechanism meets IT and IC. The incentive mechanism is deployed in smart contracts and it meets IA. At the same time, no requesters can deny payment, and the quality of the solutions submitted by the workers is proportional to their incomes; thus, the hybrid incentive mechanism meets IF. In this paper, the address of the user (worker or requester) is a pseudonymous public key, so the user's identity will not be exposed, and the evaluation of the quality of the task solutions is done by smart contracts, which will not reveal the private information of the workers, so the incentive mechanism satisfies IP. The paper neither mentions SW and IS of the mechanism nor considers SC and CC.

5.4.2 Cloud Computing. Traditional cloud service level agreements lack a reliable automated execution platform. Zhou et al. [101] proposed a witness model using smart contracts and game theory and introduced a new role "witness" that can detect and report the violations of service providers. This model includes an auditing mechanism and an economic incentive mechanism. The auditing mechanism is to assess the reputation of a witness based on its behaviors. When its reputation is lower than a predefined threshold, the witness can no longer participate in detecting violations, this can incent the witness to behave honestly. The witness reports violations and then gains reasonable revenue, which is designed according to game theory. As mentioned, the incentive mechanism meets IC, IT, and IF. According to experiments, the witness has a light gas consumption, so the witness is motivated to participate in the detection. But the authors did not consider IP. The incentive mechanism makes use of the smart contract, and thus it meets IA. SW and IS are unknown. SC and CC were not considered.

5.4.3 Internet of Vehicles. With the development of autonomous driving technology, intelligent transportation will replace traditional driving modes in the future. When intelligent transportation is successfully applied, autonomous vehicles drive in a platoon. A vehicle at the front of the platoon acts as a leader, i.e., **platoon head (PH)**, and leads the other vehicles that are named as **platoon members (PMs)**. A PH needs to observe road conditions from time to time for adjusting driving direction. Therefore, being the PH consumes more energy than being a PM. No rational drivers will choose to become a PH.

Chen et al. [15] proposed a hybrid incentive mechanism based on reputation value and monetary reward for motivating drivers to work as the PH. The service of a PH is displayed according to

its reputation value. The reputation value of PH is constantly updated according to its behavior. The higher the reputation value is, the more likely the vehicle to be selected as a PH. The PMs pay PH platoon coins (that is cryptographic currency in the platoon blockchain) through a smart contract as a service fee. The service fee is charged according to its distance to the PH-led platoon. This mechanism diminishes fuel consumption and reduces mental energy consumption for the PM. Although the fuel consumption of PH is high, the service fee paid by each PM can offset it. The mechanism can ensure that the income of PM and PH is non-negative, thus holds IR. At the same time, PH service fees are paid through smart contracts, and there will be no overpayment, underpayment, or payment refusal, which meets IF and IA. However, the mechanism assumes that the number of platoons and members is limited, so its scalability is constrained and SC was not satisfied. The paper does not mention IC, IT, SW, and IS of the incentive mechanism. The paper did not consider IP. The evaluation requirement of CC does not apply to this mechanism.

Ledbetter et al. [52] investigated how to motivate drivers to join platoons and become the PH in autonomous driving. The authors proposed a hybrid incentive mechanism based on money and reputation. A driver that wants to join the platoon must meet a reputation threshold. The calculation of the service fee is different from that in Reference [15], which considers how much money the driver will save if he does not become the PH to calculate the amount that the PM should pay to the PH. To increase the effectiveness of the incentive mechanism, additional rewards will be paid to the PH. The incentive mechanism can ensure that the PH obtains a satisfactory utility, so the mechanism satisfies IR. If a PM gains more utility by joining the platoon at will, then he needs to pay a certain percentage of money to the PH, and his reputation value will be reduced, which greatly prevents malicious behavior. Therefore, the protocol meets IC and IT. All payments and calculations of the protocol are embedded in smart contracts, which can audit calculations and ensure IF, thus the mechanism meets IA. Similarly to Reference [15], this mechanism also assumes the limited number of platoons and members, thus, its SC was not satisfied. This work does not consider SW and IS, as well as IP. The evaluation requirement of CC does not apply to this protocol.

5.4.4 Others. Data exchange requires a safe and fair mechanism to ensure the interests of data providers and data security. Otherwise, the data providers lack motivation to share data. Zheng et al. [99] proposed a smart contract-based data asset exchange mechanism to ensure the reliability and transparency of data exchanges and introduced a Quality-of-Service-based incentive mechanism for encouraging data providers to share data. They also proposed a reputation mechanism, to encourage data providers to submit high-quality data. Therefore, the incentive mechanism meets IC and IT. The smart contract ensures the fairness and effective distribution of rewards; thus, the mechanism meets IF and IA. SW and IS were not mentioned. This mechanism does not consider IP and SC. CC is not applicable for evaluating this mechanism.

6 DISCUSSION

Various incentive mechanisms have been proposed to motivate the participation willingness and cooperative behaviors of blockchain system nodes. Researchers have resorted to the blockchain technology for improving incentive mechanism design in different scenarios. Specifically, the blockchain technology has been applied in incentive mechanisms in crowdsensing scenarios to replace the crowdsensing platform and therefore resolve the privacy and security issues caused by untrustworthy crowdsensing platforms. Smart contracts help the incentive mechanisms in cloud computing and the Internet of Vehicles realize automatic allocation of incentives and eliminate denial of payment problems. We have reviewed incentive mechanisms designed for blockchain systems and incentive mechanisms built based on the blockchain technology in Sections 4 and 5, respectively.

Table 4. Performance Comparison of Different Forms of Incentive Mechanisms under Different Goals in Blockchain Systems

Goal / Form	Participation	Cooperation
Monetary incentive	Effectively motivated	Untrusted behavior of nodes cannot be effectively avoided
Reputation-based incentive	Not applicable	Effectively motivated
Gamified incentive	Not applicable	Not applicable
Hybrid incentive	Effectively motivated	Effectively motivated

Table 5. Performance Comparison of Blockchain-based Incentive Mechanisms with Different Forms under Different Application Scenarios

Scenario / Form	Crowdsensing	Cloud computing	Internet of Vehicle	Other scenarios
Monetary incentive	Applicable to motivate participation	Applicable to motivate participation	Applicable to motivate participation	Applicable to motivate participation
Reputation-based incentive	Applicable but rarely used	Applicable for selecting and filtering nodes	Applicable for selecting and filtering nodes	Applicable for selecting and filtering nodes
Gamified incentive	Not applicable	Not applicable	Not applicable	Applicable for simple game scenarios
Hybrid incentive	Applicable but rarely used	Applicable	Applicable	Applicable

We conclude the following findings from Section 4 when investigating the performance of different forms of incentives under different goals in blockchain systems, as summarized in Table 4.

- All monetary incentive mechanisms usually satisfy IR, which is a prerequisite in practical applications for nodes to participate and cooperate. However, few incentive mechanisms consider the properties other than IR, IC, IT, and IF. Although some monetary incentives have taken IC and IT into account when setting participation as the goal of incentive, none of them pay attention to other properties such as IC. They assume that as long as the nodes can benefit from a system, the nodes have motivations to participate. Unfortunately, this can only provide temporary incentives without guaranteeing the cooperative and honest behaviors of these nodes after participating in the system. Most reviewed monetary incentives consider IC, IT, and IF when setting cooperation as the goal of incentive, since these properties are essential for node cooperation.
- The reputation-based incentive and gamified incentive are rarely employed solely in blockchain systems. According to our review, the reputation-based incentive motivates nodes to cooperate by adjusting reputation values, which is not applicable for participation motivation. Although the gamified incentive has been applied to motivate participation and cooperation, it does not work very well.
- The hybrid incentive combines multiple incentive forms, which compensates for the shortcomings of a single incentive and offers additional favorable properties.
- To sum up, the monetary incentive and the hybrid incentive can effectively motivate nodes to participate in the blockchain system, while the reputation-based mechanism and the hybrid incentive work well in motivating nodes to cooperate.

We sum up some discoveries from Section 5 by comparing the performance of different types of blockchain-based incentive mechanisms in different application scenarios, as concluded in Table 5.

- The monetary incentive mechanisms in crowdsensing are usually applied to motivate nodes to participate and provide real data, therefore, they satisfy IR and IT. Some of them achieve IA by automatically distributing rewards to system nodes with smart contracts. However, most of them do not consider other properties. Most of the monetary incentive mechanisms in cloud computing motivate nodes to cooperate and satisfy the requirements of IC and IT. The proposed monetary incentive mechanisms in the Internet of Vehicles achieve many desirable properties and effectively motivate the participation willingness of nodes. In other scenarios that require node participation and cooperation, only some monetary incentives satisfy IC and IT while most of them fail to consider IF.
- The reputation-based incentive mechanisms are rarely employed in crowdsensing and some IoV scenarios, since the literature normally adops auctions and other methods to motivate nodes to provide real data. In other scenarios, A sole reputation-based incentive mechanism only has good properties when system nodes need to be monitored. The gamified incentive is rarely used in almost all scenarios and it cannot achieve good properties literally.
- The hybrid incentive is often used in scenarios other than crowdsensing scenarios, where it combines the monetary incentive and reputation-based incentive for good properties.

Combining the above findings, we summarize the application of different forms of incentive mechanisms as follows.

(1) The monetary incentive is suitable for encouraging node participation willingness, which applies direct rewards according to node behaviors. Compared with obtaining nothing when not participating in the system, a node can get material rewards if involves into the system; therefore, the monetary incentive can effectively motivate participation. When motivating cooperation, the monetary incentive must reward good behavior more than untrustworthy behavior, which is difficult to guarantee complete fairness. Moreover, the system nodes in large-scale systems are not completely rational as they are not capable of witnessing the system status as a whole, which makes it difficult to motivate their trustworthy behavior.
(2) The reputation-based incentive is suitable for such scenarios where nodes need to be monitored. It generally sets up a reputation threshold as a benchmark to determine node permissions, where the reputation value is calculated according to node behavior based on pre-defined algorithms. Once a node performs untrustworthy behavior and its reputation value becomes lower than the threshold, its participation right could be deprived or the difficulty of obtaining profits is increased. Therefore, the reputation-based incentive can effectively motivate cooperation. Unfortunately, applying the reputation-based incentive solely has little effect on motivating participation.
(3) The gamified incentive can be used in simple game scenarios or work as an auxiliary method. It provides psychological satisfaction to system nodes and is rarely used in blockchain systems and other scenarios. Therefore, it faces a similar dilemma as the reputation-based incentive in terms of the incentive goal of participation, considering that it cannot directly provide any material rewards to the participants. The gamified incentive is suitable to serve as an embellishment while it cannot work well solely in motivating the participation enthusiasm and cooperation degree of nodes.
(4) The hybrid incentive owns the advantages of diverse types of incentive mechanisms and makes up for their shortcomings, so it significantly motivates participation and cooperation in various application scenarios. However, good performance comes at a price. The hybrid incentive generally introduces additional system nodes or requires additional workload for existing system nodes. Therefore, its execution overheads or economic costs are usually higher than those of a sole incentive.

(5) In summary, when an application scenario is complicated and the burden of a node is heavy or there are already other methods that have been applied to constrain node behavior, the monetary incentive and the reputation-based incentive can be applied to motivate participation and cooperation separately for satisfying overall incentive performance. In the application scenarios with lightweight nodes, the hybrid incentive can be employed to incent both participation and cooperation with expected performance.

In a nutshell, blockchain and incentive mechanisms benefit a lot from each other. The employment of a well-designed incentive mechanism ensures sustainably benign development of blockchain systems and the introduction of blockchain improves the performance of incentive mechanisms. However, we also find s series of problems in current research through extensively review, which will be presented in the next section.

7 OPEN ISSUES AND FUTURE DIRECTIONS

7.1 Open Issues

According to the above literature review, we figure out a number of open issues concerning the incentive mechanisms in blockchain and blockchain-based incentive mechanisms.

7.1.1 Open Issues in Incentive Mechanisms in Blockchain. First, many scholars have studied how transaction fees affect the behavior of miners. However, when designing the incentive mechanism, they just assume that transaction fees are included in the incentives, there is no specific mechanism for designating the transaction fees. Most rules about transaction fees only consider guiding the benign behaviors of miners while ignoring the user experience of blockchain users who pay the transaction fees, which will further indirectly influence the utilities of these users.

Second, most of the existing research on the incentives of broadcast nodes is based on a simplified blockchain network. For example, the blockchain network in Reference [6] is simplified as a forest of d-ary directed trees with a height of H. Ersoy et al. [24] simply considered a k-connected blockchain network when designing incentive mechanisms for the broadcast nodes. The blockchain network structure plays a vital role in the design of the incentive mechanism. The incentive mechanisms also affect the blockchain network structure by influencing the behavior of the broadcast nodes. To accurately capture the practical behaviors of the broadcast nodes and design effective incentive mechanisms, the blockchain network model that reflects real-world situations should be studied.

Third, the incentive mechanism of full nodes is seldom studied at present. Most people think that the incentives for full nodes are insignificant, so little literature studies this topic. However, it is necessary for full nodes to share historical block records to unify the blockchain ledger. Wang et al. [88] proposed that full nodes that deliver historical block data should be rewarded. However, there was no specific reward distribution scheme provided.

Forth, not all existing attacks are suppressed by incentive mechanisms, and existing incentive mechanisms are primarily proposed to solve only one type of attacks. Our survey shows that some incentive mechanisms have already been proposed to eliminate selfish mining attacks, 51% attacks, BWA, and DoS attacks. However, no consideration about defending other emerging attacks, such as whale attacks [56], uncle-block attacks [14], **Fork After Withholding (FAW)** attacks [51], and so on. By launching the whale attack, an attacker increases the chance of double-spending by bribing others through transactions with large fees. The uncle-block attack exploits uncle blocks for block withholding. FAW attack combines a BWA with intentional forks. Kwon et al. [51] only proposed a simple countermeasure against FAW attacks. Practically, various attacks exist in one blockchain system. How to suppress these attacks effectively in an integrated way still needs

further investigation. Mirkin et al. [63] proposed to set uncle block rewards as an incentive to mitigate Blockchain Denial of Service attacks; however, this incentive disappointedly increases the risk of selfish mining attacks.

Fifth, existing incentive mechanisms proposed for mining pools are simple. Although the competition between two mining pools has already been studied in Reference [7], a scenario that involves multiple mining pools has not been explored. Eyal et al. [25] assumed mining pools hold the same computational powers and applied game theory to analyze the attacks among multiple mining pools. Besides, since miners are not instantly rewarded by mining pools after a block is mined successfully, an effective incentive mechanism should further consider the effect of time on node utility.

Sixth, the fairness of incentives for miners in Blockchain 2.0 is scarcely investigated in the current literature. Aldweesh et al. [2] found that the execution motivation of miners in the Ethereum blockchain is not proportional to their operational costs, which could cause an incentive imbalance. Unfortunately, they did not propose how to address this problem.

Seventh, existing incentive mechanisms in Blockchain 3.0 rarely fulfill the requirement of IA. Specifically, most monetary incentive mechanisms in Blockchain 3.0 manually distribute rewards to system entities, thus facing the risk of being deceived in complicated processes.

7.1.2 Open Issues in Blockchain-based Incentive Mechanisms. First, according to Section 5, we discovered that the blockchain-based incentive mechanisms mostly focus on preventing dishonest behaviors and motivating nodes to participate. However, this research is still in an early stage and some requirements like IP and BC are seldom considered in the existing literature.

Second, it lacks study on motivating newly involved system entities like miners. These mechanisms introduce the blockchain to realize decentralization to eliminate the demand on a trusted centralized party. Existing literature shows the effectiveness of such a method. However, the introduction of blockchain also brings additional issues that do not exist in centralized incentive mechanisms, like the incentives to miners. Existing literature only focuses on how to replace the centralized party with the blockchain in the incentive mechanisms that motivate original system entities without considering miners. Although the authors in Reference [83] stated that the contribution of miners will be paid, they did not perform a concrete investigation on the payment.

7.1.3 Open Issues in Both Cases. First, existing incentive mechanisms seldom jointly apply all incentive forms. We can observe from Tables 2 and 3 that most incentive mechanisms are proposed based on only a single incentive form and the widely applied form is monetary incentives. However, monetary incentive mechanisms are not as sustainable as non-monetary ones, such as reputation-based incentive mechanisms [61]. Moreover, if only a non-monetary incentive mechanism is applied, then the incentive is indirect without detailed payment mechanisms and short-sighted system entities may be unable to perceive the incentives.

Second, none of the reviewed incentive mechanisms fulfill all requirements. Tables 2 and 3 illustrate that existing incentive mechanisms in blockchain and blockchain-based incentive mechanisms can only fulfill some basic requirements. Specifically, most of them consider IR, IT, and IC. However, they rarely consider SW and IS. The time cost (CC) of the incentive mechanisms in Blockchain 3.0 and the blockchain-based incentive mechanisms is ignored. The implementation cost (BC) of incentive mechanisms in Blockchain 1.0, 2.0, and 3.0 is also seldom studied. This implies that the blockchain-related incentive mechanisms have a big space to be further improved or optimized. Therefore, well-designed incentive mechanisms that satisfy more requirements for achieving high effectiveness and robustness are highly demanded.

7.2 Future Research Directions

Motivated by the above open issues, we conclude the following directions for future research.

First, we should comprehensively concern all involved entities' utilities when designing the rules of transaction fees. We should consider it not only from the perspective of miners for ensuring that their balanced income and expenditures and providing them incentives to actively participate in systems but also from the perspective of users who pay the transaction fees. Specifically, we should consider additional factors, such as their time costs of waiting and transaction processing speeds in the design of an incentive mechanism. Long-term interactions between users and miners are worth studying, e.g., by employing evolutionary game theory. By considering blockchain market development and combining actual costs, practical and effective fee rules can be designed.

Second, a close to practice network model should be based on proposing an effective incentive mechanism. For example, we should study how to provide motivations to broadcast nodes to make incentive mechanisms compatible with practical blockchain networks. We can adopt complex network theory to study the blockchain networks, consider the evolution of the networks, and examine the changes in network topologies. Furthermore, we can design the distribution of incentives to broadcast nodes to be proportional to their contributions for fairly motivating the participation and cooperation of the broadcast nodes, thus resulting in an effective incentive mechanism with fairness and sustainability.

Third, the incentives for full nodes should be carefully investigated. More detailed incentive mechanisms can be designed according to the coin lock strategy proposed in Reference [88]. For example, an elaborate payment mechanism that allows newly joined nodes to pay for the cooperation of full nodes should be studied. Further research should also emphasize how to employ the inner competition of full nodes for relieving the incentive costs of newly joined nodes.

Fourth, the incentive mechanisms to prevent each uninvestigated attack and combined attacks should also be further studied. Due to the diverse attacker types and attacking goals in different attacks, incentive measures for different attacks are also different. Moreover, when considering the incentive measures to prevent the combination of different attacks, we should pay attention to how to model the tradeoff of different attacks. A possible further direction is to propose an adjustable incentive mechanism that can suppress some attacks more effectively than the others based on the system designer's expectation. Hou et al. [38] applied deep reinforcement learning to conduct automatic attack analysis on incentive mechanisms in blockchain, which can greatly help the adjustment of the incentive mechanism to prevent various attacks in a positive way.

Fifth, rigorous incentive mechanisms should be proposed for motivating cooperation in mining pools. The optimal decisions and behaviors of miners in a mining pool dynamically change as time goes by. Therefore, the time factor should be considered in future research for achieving accurate investigation of mining pools. Zolotavkin et al. [104] mentioned that a cross-time utility model should be adopted when considering the rewards or incentives of miners in the mining pool. Furthermore, the competition among multiple mining pools, which is scarcely studied, can be modeled as a game model. By designing suitable utility functions for mining pools with different strategies, we can regulate the Nash equilibrium of this game to an expected state where all mining pools behave honestly without attacking each other. To generalize the incentive mechanism, the computational powers of mining pools should be assumed to be diverse.

Sixth, further effective incentive mechanisms for the miners of the Ethereum blockchain should be proposed. Existing incentives normally come from the Ether rewards obtained by generating blocks. Inspired by Reference [22], research should be conducted to further improve the block reward-based incentive by considering the value of smart contracts. Specifically, we could consider employing the token transaction volume of a smart contract as its value, which is further designed to be positively related to block rewards.

Seventh, smart contracts can be introduced into the incentive mechanisms in Blockchain 3.0 for achieving the requirement of IA. An incentive mechanism can integrate smart contracts to implement bidding or game process. Such combination can not only avoid dishonest behavior or unintentional faults caused by human intervention but also simplify the implementation of incentive mechanisms regarding incentive design and distribution. Last, a well-designed smart contract can help the incentive mechanisms to achieve fairness easily.

Eighth, incentive mechanisms combining both monetary and non-monetary incentives will become a hot research topic in the future. The reason is that such a hybrid incentive mechanism can motivate system entities with direct rewards and increase system sustainability. Existing literature has already attempted to incorporate credit-based incentives into monetary incentives and achieved desirable performance and satisfying properties. We can further investigate how to combine monetary incentives, gamified incentives, lotteries-based incentives, contract theory-based incentives, and so on. Whether involving multiple kinds of non-monetary incentives can be more effective and how to allocate the weight of different forms of incentives are also interesting to be investigated.

Ninth, privacy preservation and the incentives for miners in blockchain-based incentive mechanisms should be carefully researched. Privacy preservation can be achieved by either introducing complicated cryptographic algorithms into incentive mechanisms or increasing the costs to violate privacy through incentive design. The appearance of miners complicates system models, the interactions among system entities, and the interest relationships between system entities. Borrowing the ideas of motivating miners in Blockchain 1.0, 2.0, and 3.0 could help; however, the effectiveness still needs to be seriously explored.

Finally, more requirements should be holistically considered when designing incentive mechanisms in blockchain and blockchain-based incentive mechanisms. We should pay attention to sustainability while focusing on social welfare maximization for increasing the contribution enthusiasm of all system nodes and maintaining long-term system operation. The requirements related to incentive costs should also be considered, which are highly needed in cost-sensitive application scenarios. Specifically, sustainability can be achieved by considering effective non-monetary incentives and designing repeated games. By taking the social welfare maximization as the general goal of incentive design instead of maximizing the incentive designer's utility, we can treat the maximization problem as an optimization problem and employ some efficient algorithms to output solutions. Gradient-based algorithms are commonly applied to yield near-optimal solutions when the optimization problem is NP-hard. It is worth investigating whether there are other efficient algorithms with low computational complexity in the future.

8 CONCLUSION

Incentive mechanism, as the driving force for maintaining the long-term system operation, is an indispensable element of blockchain systems. Furthermore, the advanced properties of blockchain can also contribute to designing effective and efficient incentive mechanisms. However, there still lacks a comprehensive survey on how incentive mechanisms and blockchain technology can make each other better. In this article, we broadly reviewed academic papers related to the incentive mechanisms in blockchain and blockchain-based incentive mechanisms. To systematically evaluate these papers, we proposed a set of requirements based on incentive properties and costs. In both incentive mechanisms in blockchain and blockchain-based incentive mechanisms, we reviewed the existing literature according to incentive forms, incentive goals, and application scenarios. Through our evaluation on their pros and cons, we discussed how incentive mechanisms and blockchain benefit with each other and further concluded some unsolved issues and proposed future research directions to guide further investigation in this field.

REFERENCES

[1] Ittai Abraham, Dahlia Malkhi, Kartik Nayak, Ling Ren, and Alexander Spiegelman. 2016. Solidus: An incentive-compatible cryptocurrency based on permissionless byzantine consensus. CoRR abs/1612.02916.

[2] Amjad Aldweesh, Maher Alharby, Ellis Solaiman, and Aad van Moorsel. 2018. Performance benchmarking of smart contracts to assess miner incentives in ethereum. In *Proceedings of the 14th European Dependable Computing Conference (EDCC'18)*. IEEE, 144–149.

[3] Turki Ali Alghamdi, Ishtiaq Ali, Nadeem Javaid, and Muhammad Shafiq. 2019. Secure service provisioning scheme for lightweight IoT devices with a fair payment system and an incentive mechanism based on blockchain. *IEEE Access* 8 (2019), 1048–1061.

[4] Naif Alzahrani and Nirupama Bulusu. 2018. Towards true decentralization: A blockchain consensus protocol based on game theory and randomness. In *Proceedings of the International Conference on Decision and Game Theory for Security*, Vol. 11199. Springer, 465–485.

[5] N. Anita and M. Vijayalakshmi. 2019. Blockchain security attack: A brief survey. In *Proceedings of the 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT'19)*. IEEE, 1–6.

[6] Moshe Babaioff, Shahar Dobzinski, Sigal Oren, and Aviv Zohar. 2012. On bitcoin and red balloons. In *Proceedings of the 13th ACM Conference on Electronic Commerce*. 56–73.

[7] Samiran Bag and Kouichi Sakurai. 2016. Yet another note on block withholding attack on bitcoin mining pools. In *International Conference on Information Security*. Springer, 167–180.

[8] Roman Beck, Christoph Müller-Bloch, and John Leslie King. 2018. Governance in the blockchain economy: A framework and research agenda. *J. Assoc. Inf. Syst.* 19, 10 (2018), 1.

[9] Ethan Buchman. 2016. *Tendermint: Byzantine Fault Tolerance in the Age of Blockchains*. Ph.D. Dissertation.

[10] Vitalik Buterin et al. 2014. Ethereum: A Next-generation Smart Contract and Decentralized Application Platform. *White Paper* 3, 37 (2014), 1–36. Retrieved from https://github.com/ethereum/wiki/wiki/%5BEnglish%5D-White-Paper 7.

[11] Glenn Carl, George Kesidis, Richard R. Brooks, and Suresh Rai. 2006. Denial-of-service attack-detection techniques. *IEEE Internet Comput.* 10, 1 (2006), 82–89.

[12] Miles Carlsten, Harry Kalodner, S. Matthew Weinberg, and Arvind Narayanan. 2016. On the instability of bitcoin without the block reward. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*. 154–167.

[13] Chandrima Chakrabarti and Souvik Basu. 2019. A blockchain based incentive scheme for post disaster opportunistic communication over DTN. In *Proceedings of the 20th International Conference on Distributed Computing and Networking*. 385–388.

[14] Sang-Yoon Chang, Younghee Park, Simeon Wuthier, and Chang-Wu Chen. 2019. Uncle-block attack: Blockchain mining threat beyond block withholding for rational and uncooperative miners. In *International Conference on Applied Cryptography and Network Security*, Vol. 11464. Springer, 241–258.

[15] Chen Chen, Tingting Xiao, Tie Qiu, Ning Lv, and Qingqi Pei. 2019. Smart-contract-based economical platooning in blockchain-enabled urban internet of vehicles. *IEEE Trans. Industr. Inf.* 16, 6 (2019), 4122–4133.

[16] Huan Chen and Yijie Wang. 2019. SSChain: A full sharding protocol for public blockchain without data migration overhead. *Perv. Mobile Comput.* 59 (2019), 101055.

[17] Wuhui Chen, Yufei Chen, Xu Chen, and Zibin Zheng. 2019. Toward secure data sharing for the IoV: A quality-driven incentive mechanism with on-chain and off-chain guarantees. *IEEE IoT J.* 7, 3 (2019), 1625–1640.

[18] Xiaofeng Chen and Xiaohong Zhang. 2019. Secure electricity trading and incentive contract model for electric vehicle based on energy blockchain. *IEEE Access* 7 (2019), 178763–178778.

[19] Sunghyun Cho and Sejong Lee. 2019. Survey on the application of BlockChain to IoT. In *Proceedings of the International Conference on Electronics, Information, and Communication (ICEIC'19)*. IEEE, 1–2.

[20] Peter B. Clark and James Q. Wilson. 1961. Incentive systems: A theory of organizations. *Admin. Sci. Quart.* (1961), 129–166.

[21] Huan Cui, Zhiyong Chen, Ning Liu, and Bin Xia. 2019. Blockchain-driven contents sharing strategy for wireless cache-enabled D2D networks. In *Proceedings of the IEEE International Conference on Communications Workshops (ICC Workshops'19)*. IEEE, 1–5.

[22] Weiqi Dai, Deshan Xiao, Hai Jin, and Xia Xie. 2019. A concurrent optimization consensus system based on blockchain. In *Proceeedings of the 26th International Conference on Telecommunications (ICT'19)*. IEEE, 244–248.

[23] Changyu Dong, Yilei Wang, Amjad Aldweesh, Patrick McCorry, and Aad van Moorsel. 2017. Betrayal, distrust, and rationality: Smart counter-collusion contracts for verifiable cloud computing. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*. 211–227.

[24] Oğuzhan Ersoy, Zhijie Ren, Zekeriya Erkin, and Reginald L. Lagendijk. 2018. Transaction propagation on permissionless blockchains: Incentive and routing mechanisms. In *Proceedings of the Crypto Valley Conference on Blockchain Technology (CVCBT'18)*. IEEE, 20–30.

[25] Ittay Eyal. 2015. The miner's dilemma. In *Proceedings of the IEEE Symposium on Security and Privacy*. IEEE, 89–103.
[26] Ittay Eyal, Adem Efe Gencer, Emin Gün Sirer, and Robbert Van Renesse. 2016. Bitcoin-ng: A scalable blockchain protocol. In *Proceedings of the 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI'16)*. 45–59.
[27] Ittay Eyal and Emin Gün Sirer. 2014. Majority is not enough: Bitcoin mining is vulnerable. In *International Conference on Financial Cryptography and Data Security*, Vol. 8437. Springer, 436–454.
[28] Wei Feng, Yafeng Li, Xuetao Yang, Zheng Yan, and Liang Chen. 2021. Blockchain-based data transmission control for tactical data link. *Digit. Commun. Netw.* 3 (2021), 285–294.
[29] Wei Feng and Zheng Yan. 2019. MCS-Chain: Decentralized and trustworthy mobile crowdsourcing based on blockchain. *Fut. Gener. Comput. Syst.* 95 (2019), 649–666.
[30] Wei Feng, Zheng Yan, Laurence T. Yang, and Qinghua Zheng. 2020. Anonymous authentication on trust in blockchain-based mobile crowdsourcing. *IEEE IoT J.* (2020).
[31] Keke Gai, Jinnan Guo, Liehuang Zhu, and Shui Yu. 2020. Blockchain meets cloud computing: A survey. *IEEE Commun. Surv. Tutor.* 22, 3 (2020), 2009–2030.
[32] Ziye Geng, Yunhua He, Tong Niu, Hong Li, Limin Sun, Wei Cheng, and Xu Li. 2017. Poster: Smart-contract based incentive mechanism for K-anonymity privacy protection in LBSs. In *Proceedings of the IEEE Symposium on Privacy-Aware Computing (PAC'17)*. IEEE, 200–201.
[33] Arthur Gervais, Ghassan O. Karame, Karl Wüst, Vasileios Glykantzis, Hubert Ritzdorf, and Srdjan Capkun. 2016. On the security and performance of proof of work blockchains. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*. 3–16.
[34] Xuan Han, Yong Yuan, and Fei-Yue Wang. 2019. A fair blockchain based on proof of credit. *IEEE Trans. Comput. Soc. Syst.* 6, 5 (2019), 922–931.
[35] Garrett Hardin. 2009. The tragedy of the commons. *J. Nat. Resourc. Policy Res.* 1, 3 (2009), 243–253.
[36] Justin D. Harris and Bo Waggoner. 2019. Decentralized and collaborative AI on blockchain. In *Proceedings of the IEEE International Conference on Blockchain (Blockchain'19)*. IEEE, 368–375.
[37] Yejun He, Man Chen, Baohong Ge, and Mohsen Guizani. 2016. On WiFi offloading in heterogeneous networks: Various incentives and trade-off strategies. *IEEE Commun. Surv. Tutor.* 18, 4 (2016), 2345–2385.
[38] Charlie Hou, Mingxun Zhou, Yan Ji, Phil Daian, Florian Tramer, Giulia Fanti, and Ari Juels. 2019. SquirRL: Automating attack analysis on blockchain incentive mechanisms with deep reinforcement learning. In *Proceedings of Network and Distributed System Security Symposium*. ISOC, 1–18.
[39] Bowen Hu, Chunjie Zhou, Yu-Chu Tian, Yuanqing Qin, and Xinjue Junping. 2019. A collaborative intrusion detection approach using blockchain for multimicrogrid systems. *IEEE Trans. Syst. Man Cybernet.: Syst.* 49, 8 (2019), 1720–1730.
[40] Jiejun Hu, Kun Yang, Kezhi Wang, and Kai Zhang. 2020. A blockchain-based reward mechanism for mobile crowdsensing. *IEEE Trans. Comput. Soc. Syst.* 7, 1 (2020), 178–191.
[41] Jiyue Huang, Kai Lei, Maoyu Du, Hongting Zhao, Huafang Liu, Jin Liu, and Zhuyun Qi. 2019. Survey on blockchain incentive mechanism. In *International Conference of Pioneering Computer Scientists, Engineers and Educators*, Vol. 1058. Springer, 386–395.
[42] Tam T. Huynh, Thuc D. Nguyen, and Hanh Tan. 2019. A survey on security and privacy issues of blockchain technology. In *Proceedings of the International Conference on System Science and Engineering (ICSSE'19)*. IEEE, 362–367.
[43] Luis G. Jaimes, Idalides J. Vergara-Laurens, and Andrew Raij. 2015. A survey of incentive techniques for mobile crowd sensing. *IEEE IoT J.* 2, 5 (2015), 370–380.
[44] Suhan Jiang and Jie Wu. 2019. Bitcoin mining with transaction fees: A game on the block size. In *Proceedings of the IEEE International Conference on Blockchain (Blockchain'19)*. IEEE, 107–115.
[45] Xin Jiang and Xiang-Yu Bai. 2013. A survey on incentive mechanism of delay tolerant networks. In *Proceedings of the 10th International Computer Conference on Wavelet Active Media Technology and Information Processing (ICCWAMTIP'13)*. IEEE, 191–197.
[46] Maha Kadadha, Hadi Otrok, Rabeb Mizouni, Shakti Singh, and Anis Ouali. 2020. Sensechain: A blockchain-based crowdsensing framework for multiple requesters and multiple workers. *Fut. Gener. Comput. Syst.* 105 (2020), 650–664.
[47] Yuki Kano and Tatsuo Nakajima. 2017. A new approach to mining work in blockchain technologies. In *Proceedings of the 15th International Conference on Advances in Mobile Computing & Multimedia*. 107–114.
[48] Fazlullah Khan, Ateeq Ur Rehman, Jiangbin Zheng, Mian Ahmad Jan, and Muhammad Alam. 2019. Mobile crowdsensing: A survey on privacy-preservation, task management, assignment models, and incentives mechanisms. *Fut. Gener. Comput. Syst.* 100 (2019), 456–472.
[49] Moon Soo Kim and Jee Yong Chung. 2019. Sustainable growth and token economy design: The case of steemit. *Sustainability* 11, 1 (2019), 167.

[50] Elias Koutsoupias, Philip Lazos, Foluso Ogunlana, and Paolo Serafino. 2019. Blockchain mining games with pay forward. In *Proceedings of the World Wide Web Conference*. 917–927.
[51] Yujin Kwon, Dohyun Kim, Yunmok Son, Eugene Vasserman, and Yongdae Kim. 2017. Be selfish and avoid dilemmas: Fork after withholding (faw) attacks on bitcoin. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*. 195–209.
[52] Brian Ledbetter, Samuel Wehunt, Mohammad Ashiqur Rahman, and Mohammad Hossein Manshaei. 2019. LIPs: A protocol for leadership incentives for heterogeneous and dynamic platoons. In *Proceedings of the IEEE 43rd Annual Computer Software and Applications Conference (COMPSAC'19)*, Vol. 1. IEEE, 535–544.
[53] Kai Lei, Maoyu Du, Jiyue Huang, and Tong Jin. 2020. Groupchain: Towards a scalable public blockchain in fog computing of IoT services computing. *IEEE Trans. Serv. Comput.* 13, 2 (2020), 252–262.
[54] Yoad Lewenberg, Yonatan Sompolinsky, and Aviv Zohar. 2015. Inclusive block chain protocols. In *International Conference on Financial Cryptography and Data Security*, Vol. 8975. Springer, 528–547.
[55] Lun Li, Jiqiang Liu, Lichen Cheng, Shuo Qiu, Wei Wang, Xiangliang Zhang, and Zonghua Zhang. 2018. Creditcoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles. *IEEE Trans. Intell. Transport. Syst.* 19, 7 (2018), 2204–2220.
[56] Kevin Liao and Jonathan Katz. 2017. Incentivizing blockchain forks via whale transactions. In *International Conference on Financial Cryptography and Data Security*, Vol. 10323. Springer, 264–279.
[57] Li Lin. 2019. *Deconstruction of Blockchain* (1st ed.). Beijing: Tsinghua University Press, Tsinghua University, China.
[58] Gao Liu, Huidong Dong, Zheng Yan, Xiaokang Zhou, and Shohei Shimizu. 2020. B4SDC: A blockchain system for security data collection in MANETs. *IEEE Trans. Big Data* (2020).
[59] Gao Liu, Zheng Yan, Wei Feng, Xuyang Jing, Yaxing Chen, and Mohammed Atiquzzaman. 2021. SeDID: An SGX-enabled decentralized intrusion detection framework for network trust evaluation *Information Fusion* 70 (2021), 100–114.
[60] Ziyao Liu, Nguyen Cong Luong, Wenbo Wang, Dusit Niyato, Ping Wang, Ying-Chang Liang, and Dong In Kim. 2019. A survey on blockchain: A game theoretical perspective. *IEEE Access* 7 (2019), 47615–47643.
[61] Tie Luo, Salil S. Kanhere, Jianwei Huang, Sajal K. Das, and Fan Wu. 2017. Sustainable incentives for mobile crowdsensing: Auctions, lotteries, and trust and reputation systems. *IEEE Commun. Mag.* 55, 3 (2017), 68–74.
[62] Du Mingxiao, Ma Xiaofeng, Zhang Zhe, Wang Xiangwei, and Chen Qijun. 2017. A review on consensus algorithm of blockchain. In *Proceedings of the IEEE International Conference on Systems, Man, and Cybernetics (SMC'17)*. IEEE, 2567–2572.
[63] Michael Mirkin, Yan Ji, Jonathan Pang, Ariah Klages-Mundt, Ittay Eyal, and Ari Juels. 2020. BDoS: Blockchain denial-of-service. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*. 601–619.
[64] Malte Möser and Rainer Böhme. 2015. Trends, tips, tolls: A longitudinal study of bitcoin transaction fees. In *International Conference on Financial Cryptography and Data Security*, Vol. 8976. Springer, 19–33.
[65] Satoshi Nakamoto. 2008. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review* (2008), 21260.
[66] Mehrdad Nojoumian, Arash Golchubian, Laurent Njilla, Kevin Kwiat, and Charles Kamhoua. 2018. Incentivizing blockchain miners to avoid dishonest mining strategies by a reputation-based paradigm. In *Science and Information Conference*, Vol. 857. Springer, 1118–1134.
[67] S. Pavithra, S. Ramya, and Soma Prathibha. 2019. A survey on cloud security issues and blockchain. In *Proceedings of the 3rd International Conference on Computing and Communications Technologies (ICCCT'19)*. IEEE, 136–140.
[68] Dan Peng, Fan Wu, and Guihai Chen. 2015. Pay as how well you do: A quality based incentive mechanism for crowdsensing. In *Proceedings of the 16th ACM International Symposium on Mobile Ad Hoc Networking and Computing*. 177–186.
[69] Li Peng, Wei Feng, Zheng Yan, Yafeng Li, Xiaokang Zhou, and Shohei Shimizu. 2021. Privacy preservation in permissionless blockchain: A survey. *Digit. Commun. Netw.* 7, 3 (2021), 295–307.
[70] Rui Qin, Yong Yuan, and Fei-Yue Wang. 2018. Research on the selection strategies of blockchain mining pools. *IEEE Trans. Comput. Soc. Syst.* 5, 3 (2018), 748–757.
[71] N. Ramkumar, G. Sudhasadasivam, and K. G. Saranya. 2020. A survey on different consensus mechanisms for the blockchain technology. In *Proceedings of the International Conference on Communication and Signal Processing (ICCSP'20)*. IEEE, 0458–0464.
[72] Meni Rosenfeld. 2011. Analysis of bitcoin pooled mining reward systems. arXiv:1112.4980. Retrieved from https://arxiv.org/abs/1112.4980.
[73] Sarwar Sayeed and Hector Marco-Gisbert. 2019. Assessing blockchain consensus and security mechanisms against the 51% attack. *Appl. Sci.* 9, 9 (2019), 1788.
[74] Okke Schrijvers, Joseph Bonneau, Dan Boneh, and Tim Roughgarden. 2016. Incentive compatibility of bitcoin mining pool reward functions. In *International Conference on Financial Cryptography and Data Security*, Vol. 9603. Springer, 477–498.

[75] RuYi She. 2020. Survey on incentive strategies for mobile crowdsensing system. In *Proceedings of the IEEE 11th International Conference on Software Engineering and Service Science (ICSESS'20)*. IEEE, 511–514.
[76] Meng Shen, Junxian Duan, Liehuang Zhu, Jie Zhang, Xiaojiang Du, and Mohsen Guizani. 2020. Blockchain-based incentives for secure and collaborative data sharing in multiple clouds. *IEEE J. Select. Areas Commun.* 38, 6 (2020), 1229–1241.
[77] Yonatan Sompolinsky and Aviv Zohar. 2018. Bitcoin's underlying incentives. *Commun. ACM* 61, 3 (2018), 46–53.
[78] P. Swathi, Chirag Modi, and Dhiren Patel. 2019. Preventing sybil attack in blockchain using distributed behavior monitoring of miners. In *Proceedings of the 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT'19)*. IEEE, 1–6.
[79] Pawel Szalachowski, Daniël Reijsbergen, Ivan Homoliak, and Siwei Sun. 2019. Strongchain: Transparent and collaborative proof-of-work consensus. In *Proceedings of the 28th USENIX Security Symposium (USENIX Security'19)*. 819–836.
[80] Itay Tsabary and Ittay Eyal. 2018. The gap game. In *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security*. 713–728.
[81] Eric Ke Wang, Zuodong Liang, Chien-Ming Chen, Saru Kumari, and Muhammad Khurram Khan. 2020. PoRX: A reputation incentive scheme for blockchain consensus of IIoT. *Fut. Gener. Comput. Syst.* 102 (2020), 140–151.
[82] Eric Ke Wang, RuiPei Sun, Chien-Ming Chen, Zuodong Liang, Saru Kumari, and Muhammad Khurram Khan. 2020. Proof of X-repute blockchain consensus protocol for IoT systems. *Comput. Secur.* 95 (2020), 101871.
[83] Jingzhong Wang, Mengru Li, Yunhua He, Hong Li, Ke Xiao, and Chao Wang. 2018. A blockchain based privacy-preserving incentive mechanism in crowdsensing applications. *IEEE Access* 6 (2018), 17545–17556.
[84] Wenbo Wang, Dinh Thai Hoang, Peizhao Hu, Zehui Xiong, Dusit Niyato, Ping Wang, Yonggang Wen, and Dong In Kim. 2019. A survey on consensus mechanisms and mining strategy management in blockchain networks. *IEEE Access* 7 (2019), 22328–22370.
[85] Yingjie Wang, Yang Gao, Yingshu Li, and Xiangrong Tong. 2020. A worker-selection incentive mechanism for optimizing platform-centric mobile crowdsourcing systems. *Comput. Netw.* 171 (2020), 107144.
[86] Yufeng Wang, Jie Huang, Qun Jin, and Jianhua Ma. 2017. ABT: An effective ability-balanced team based incentive mechanism in crowdsourcing system. In *Proceedings of the 5th International Conference on Advanced Cloud and Big Data (CBD'17)*. IEEE, 220–225.
[87] Yuntao Wang, Zhou Su, and Ning Zhang. 2019. BSIS: Blockchain-based secure incentive scheme for energy delivery in vehicular energy network. *IEEE Trans. Industr. Inf.* 15, 6 (2019), 3620–3631.
[88] Zhipeng Wang and Qianhong Wu. 2019. Incentive for historical block data sharing in blockchain. In *Proceedings of the IEEE 10th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON'19)*. IEEE, 0913–0919.
[89] Yangxin Wu, Peijia Zheng, Jianting Guo, Wei Zhang, and Jiwu Huang. 2018. A controllable efficient content distribution framework based on blockchain and ISODATA. In *Proceedings of the 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE'18)*. IEEE, 1698–1701.
[90] Yang Xiao, Ning Zhang, Wenjing Lou, and Y. Thomas Hou. 2020. A survey of distributed consensus protocols for blockchain networks. *IEEE Commun. Surv. Tutor.* 22, 2 (2020), 1432–1465.
[91] Hong Xie, John C. S. Lui, and Don Towsley. 2016. Design and analysis of incentive and reputation mechanisms for online crowdsourcing systems. *ACM Trans. Model. Perf. Eval. Comput. Syst.* 1, 3 (2016), 1–27.
[92] Chang Xu, Yayun Si, Liehuang Zhu, Chuan Zhang, Kashif Sharif, and Can Zhang. 2019. Pay as how you behave: A truthful incentive mechanism for mobile crowdsensing. *IEEE IoT J.* 6, 6 (2019), 10053–10063.
[93] Zheng Yan, Li Peng, Wei Feng, and Laurence T. Yang. 2021. Social-chain: Decentralized trust evaluation based on blockchain in pervasive social networking. *ACM Trans. Internet Technol.* 21, 1 (2021), 1–28.
[94] Dejun Yang, Xi Fang, and Guoliang Xue. 2013. Truthful incentive mechanisms for k-anonymity location privacy. In *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM'13)*. IEEE, 2994–3002.
[95] Bo Yin, Yulei Wu, Tianshi Hu, Jiaqing Dong, and Zexun Jiang. 2019. An efficient collaboration and incentive mechanism for internet of vehicles (iov) with secured information exchange based on blockchains. *IEEE IoT J.* 7, 3 (2019), 1582–1593.
[96] Jiayuan Yin, Changren Wang, Zongyang Zhang, and Jianwei Liu. 2018. Revisiting the incentive mechanism of bitcoin-NG. In *Australasian Conference on Information Security and Privacy*, Vol. 10946. Springer, 706–719.
[97] Zhaoyang Yu, XiaoGuang Liu, and Gang Wang. 2018. A survey of consensus and incentive mechanism in blockchain derived from P2P. In *Proceedings of the IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS'18)*. IEEE, 1010–1015.
[98] Xinglin Zhang, Zheng Yang, Wei Sun, Yunhao Liu, Shaohua Tang, Kai Xing, and Xufei Mao. 2015. Incentives for mobile crowd sensing: A survey. *IEEE Commun. Surv. Tutor.* 18, 1 (2015), 54–67.

[99] Jiawei Zheng, Xuewen Dong, Qihang Liu, Xinghui Zhu, and Wei Tong. 2019. Blockchain-based secure digital asset exchange scheme with QoS-aware incentive mechanism. In *Proceedings of the IEEE 20th International Conference on High Performance Switching and Routing (HPSR'19)*. IEEE, 1–6.

[100] Bowen Zhou, Satish Narayana Srirama, and Rajkumar Buyya. 2019. An auction-based incentive mechanism for heterogeneous mobile clouds. *J. Syst. Softw.* 152 (2019), 151–164.

[101] Huan Zhou, Xue Ouyang, Zhijie Ren, Jinshu Su, Cees de Laat, and Zhiming Zhao. 2019. A blockchain based witness model for trustworthy cloud service level agreement enforcement. In *Proceedings of the IEEE International Conference on Computer Communications (INFOCOM'19)*. IEEE, 1567–1575.

[102] Zhi Zhou, Fangming Liu, Shutong Chen, and Zongpeng Li. 2018. A truthful and efficient incentive mechanism for demand response in green datacenters. *IEEE Trans. Parallel Distrib. Syst.* 31, 1 (2018), 1–15.

[103] Liehuang Zhu, Hui Dong, Meng Shen, and Keke Gai. 2019. An incentive mechanism using shapley value for blockchain-based medical data sharing. In *Proceedings of the IEEE 5th International Conference on Big Data Security on Cloud (BigDataSecurity'19), IEEE International Conference on High Performance and Smart Computing (HPSC'19), and IEEE International Conference on Intelligent Data and Security (IDS'19)*. IEEE, 113–118.

[104] Yevhen Zolotavkin, Julian Garcia, and Joseph K. Liu. 2019. Time-dependent decision-making and decentralization in proof-of-work cryptocurrencies. In *Proceedings of the IEEE 32nd Computer Security Foundations Symposium (CSF'19)*. IEEE, 108–10813.

Received 15 March 2021; revised 8 April 2022; accepted 13 May 2022