Research on Blockchain-Based Distributed Incentive Mechanisms (Postprint)

Authors: He Yunhua, Liu Zhaoyang, Hu Yan, Li Hong, Sun Limin, Xiao Ke

Date: 2020-09-28T00:00:00+00:00

Abstract

Incentive mechanisms are widely applied in scenarios such as crowdsensing, P2P video-on-demand, and opportunistic networks, and represent a key factor in enhancing the quality of service and efficiency of information networks. Existing incentive mechanisms typically rely on bank-like trusted centers; however, such centers suffer from systemic trust deficits and privacy leakage issues due to characteristics including opaque governance and vulnerability to attacks. Blockchain-based incentive mechanisms can serve as a solution to these problems. Blockchain features decentralization, openness, immutability, and anonymity, enabling the establishment of reliable trust relationships among mutually unfamiliar parties. Moreover, blockchain-based cryptocurrencies have garnered widespread attention and recognition in the real world. This paper first introduces blockchain technology and the differences among cryptocurrencies, then summarizes the current research status of blockchain-based incentive mechanisms, including transaction forms, classification, and evaluation criteria for such mechanisms. Finally, it provides a summary and outlook on existing incentive mechanism research.

Full Text

Abstract

Incentive mechanisms are widely employed in crowdsensing, P2P video-on-demand streaming, opportunistic networks, and other scenarios, serving as a key approach to improving the quality and efficiency of information network services. Existing incentive mechanisms typically rely on trusted central authorities such as banks. However, these trusted centers suffer from opaque management, vulnerability to attacks, and other issues that lead to systemic trust deficits and privacy leakage. Blockchain-based incentive mechanisms offer a solution to these problems. Blockchain features decentralization, openness, immutability, and anonymity, enabling reliable trust establishment among

mutually unfamiliar parties. Moreover, blockchain-based cryptocurrencies have gained widespread attention and acceptance in the real world. This paper first introduces blockchain technology and the differences among cryptocurrencies, then summarizes the current state of research on blockchain-based incentive mechanisms, including transaction forms, classification of incentive mechanisms, and evaluation criteria. Finally, we provide a summary and outlook for existing incentive mechanism research.

Keywords: incentive mechanism; blockchain; cryptocurrency; payment policy; incentive effect

0 Introduction

Incentive mechanisms have found extensive application in information networks. For instance, electronic currency incentivizes users to share real-time traffic information in intelligent transportation systems [**?**]; user ranking systems encourage active software usage in NetEase Cloud Music; lottery opportunities motivate users to report damaged vehicles in bike-sharing systems; reward points stimulate article and post publication on blogs and forums. Incentive mechanisms are also applicable to delay-tolerant networks [**?**], wireless spectrum allocation [**?**], and other domains. By designing reasonable remuneration forms along with behavioral norms and reward-penalty measures, incentive mechanisms encourage users to regulate their behavior—such as restraining node selfishness, promoting node cooperation, and enhancing node contributions—thereby serving as an effective guarantee for improving service quality and efficiency.

Electronic currency, as a widely adopted incentive method in information networks [**?**, **?**, **?**, **?**], is typically issued by authoritative institutions such as banks or government agencies. However, this approach presents numerous problems. Trusted centers wield absolute control over the entire system, including currency issuance and transaction data management. The opacity of their issuance, accounting, and maintenance processes, coupled with irregular operations and incomplete protection measures, creates trust deficits. Once attacked by malicious actors, the entire system' s operation is compromised. In reality, attacks on trusted centers and data leakage incidents occur frequently, such as the Pentagon' s violation in November 2017 that exposed 50 million users' information [**?**], and Turkey' s database security vulnerability in April 2016 that led to the leakage of 50 million users' information [**?**].

Blockchain technology can address these trust deficit issues. Blockchain features traceability, trustlessness, decentralization, immutability, and anonymity. Using consensus mechanisms, asymmetric encryption, and chained block structures, it establishes reliable trust relationships among mutually unfamiliar parties and enables information exchange between nodes. Blockchain-based distributed incentive methods can enhance system security and disaster recovery capabilities.

Current distributed incentive mechanism designs are basically scenario-specific.

For example, Xunlei launched "Wankebi," a blockchain-based incentive for users to convert idle resources into shared computing services, while Wang et al. [**?**] proposed a blockchain-based incentive mechanism for crowdsensing applications. Existing literature tends to design incentive mechanisms based on specific scenarios. This paper, however, analyzes the design differences across various scenarios and introduces research progress on blockchain-based incentive mechanisms, including methods, classification, and evaluation. Section 1 introduces blockchain technology and analyzes cryptocurrency differences. Section 2 discusses blockchain-based incentive mechanisms, including specific incentive transaction forms and classification. Section 3 elaborates on evaluation criteria for incentive mechanisms. Section 4 summarizes existing incentive mechanism work and provides an outlook on future blockchain-based incentive mechanisms.

1 Blockchain Technology and Cryptocurrency

Blockchain, as the underlying technology of Bitcoin, was first proposed by Satoshi Nakamoto in the whitepaper "Bitcoin: A Peer-to-Peer Electronic Cash System." Bitcoin, the pioneer of blockchain, uses distributed timestamping technology to solve the "double-spending" problem in electronic payments and has gained widespread attention and application due to its decentralization, openness, independence, security, and certain anonymity. In blockchain networks, technologies such as the PoW consensus algorithm, asymmetric encryption, and hash algorithms ensure blockchain security and reliability. Blockchain security relies on the participation of numerous miner nodes, and blockchain' s inherent incentive mechanism rewards nodes that follow the rules in bookkeeping while punishing those that do not, guiding the entire system toward a virtuous cycle. This paper focuses on using blockchain-based cryptocurrencies to design incentive mechanisms to enhance the security of related network applications and systems.

Blockchain-based cryptocurrencies, as electronic currencies created using blockchain and cryptographic principles to ensure transaction security, do not rely on monetary institutions for issuance. They are a form of P2P encrypted digital currency featuring decentralization, transaction security, and robustness. In recent years, with the widespread application of blockchain technology [**?**, **?**, **?**, **?**], the variety of cryptocurrencies has increased. Most existing cryptocurrencies such as Bitcoin, ETH, Litecoin, XRP, and Zerocoin share basic characteristics of stable value and good liquidity, while also possessing differentiated features, as shown in Table 1 .

Table 1 Comparative Analysis of Cryptocurrency

Cryptocurrency	Consensus Protocol	Block Generation Speed	Key Features
Bitcoin	PoW/PoS	10 minutes	Pioneer cryptocurrency, high recognition
Litecoin	Scrypt	2.5 minutes	Scrypt algorithm more secure than SHA256, better for preventing 51% attacks
Zerocoin	Zerocoin Protocol	2.5 minutes	Zero-knowledge proof protects user privacy
ETH	Smart contracts	15 seconds	Smart contract functionality, supports application building, easy to implement pricing strategies
XRP	Consensus nodes	3-5 seconds	Consensus nodes as trusted nodes, low cost, high scalability, poor security

Bitcoin, proposed by Satoshi Nakamoto [**?**], is a cryptocurrency based on blockchain technology. As the pioneer of blockchain, Bitcoin uses distributed timestamping technology to solve the "double-spending" problem in electronic payments and has gained widespread attention and application due to its decentralization, openness, independence, security, and certain anonymity. However, the Bitcoin network requires high maintenance costs, with computing consuming substantial electricity. Second, Bitcoin transactions are slow to

confirm, with the network generating a new block approximately every 10 minutes, requiring at least one hour for transaction confirmation. Bitcoin cannot guarantee complete user anonymity, as real identities may be traced through associated information. Bitcoin' s transaction syntax only supports transfers, and when directly used as an incentive method, it may lead to repudiation by either the incentivizer or the incentivized. Therefore, when used as an incentive method, Bitcoin' s transaction syntax should be expanded to support functional transfers to ensure the normal operation of the incentive mechanism.

ETH is a digital token based on Ethereum, enabling highly flexible ETH transactions through Ethereum' s programmable smart contracts and open-source system. Ethereum employs smart contract functionality based on Blockchain 2.0, which endows blockchain with highly flexible extended application capabilities, enabling complex operations to control digital assets on the blockchain. Smart contracts feature automatic execution, immutability, and traceability, allowing the writing of contract requirements and corresponding regulations for both parties, making it easy to implement pricing strategies in incentive mechanisms. ETH adopts the PoS consensus mechanism to incentivize rewards, achieving a transaction efficiency of one block every 15 seconds while reducing data processing costs. ETH has no fixed total supply, with an issuance cap of 18 million per year.

Litecoin improves upon Bitcoin in terms of proof-of-work algorithm, total supply cap, and block generation speed. Litecoin uses the Scrypt algorithm instead of SHA-256 in its proof-of-work mechanism, replacing the scenario in Bitcoin where computing power is determined solely by CPU processing speed with one determined by both CPU and memory. This change makes computing power difficult to concentrate, preventing the formation of large mining farms and pools as in Bitcoin, while making miners more dispersed and thus better preventing 51% attacks. The Litecoin network is suitable for incentive mechanisms with high security requirements. Litecoin' s fixed total supply is increased from Bitcoin' s 21 million to 84 million, with a block speed of 2.5 minutes per block, completing a transaction in about 20 minutes. Currently, Litecoin is the digital currency with the highest attention and recognition after Bitcoin.

XRP implements transactions based on the Ripple network, which supports instant, low-cost international payments between different ledgers and networks worldwide, with transaction fees nearly zero. XRP is the base currency in the Ripple network, with a total quantity of 100 billion, decreasing as transactions increase. Each initiated transfer requires paying a 微量 (tiny amount) of Ripple coins to the network for destruction. Based on the consensus and verification mechanisms in the Ripple protocol, XRP is faster than Bitcoin in transaction data packaging and record confirmation. Its consensus mechanism is protocol consensus, dividing network nodes into ordinary nodes and verification nodes, where transaction verification and confirmation only require votes from verification nodes, so XRP does not need mining. Incentive mechanism scenarios

require transaction systems with low delay and high-efficiency payment methods. Therefore, when considering transfer costs, efficiency, and cross-border remittance issues, XRP can ensure these requirements are met.

Zerocoin, as a branch of Bitcoin, retains its original model with a total supply of 21 million and uses the Equihash algorithm for proof-of-work, which relies more on GPU. Compared to Bitcoin, Zcash remains a niche digital currency, but Zerocoin solves the problem of insufficient anonymity in Bitcoin. Zerocoin has two types of funds: transparent funds and private funds. Transparent funds are similar to Bitcoin, with Zerocoin providing completely public addresses where transaction records are queryable. Private funds aim to protect user privacy, using zk-SNARKS encryption technology to achieve anonymity, completely hiding transaction records and amounts. Transaction records are not publicly disclosed but can be viewed through private keys, solving the "pseudo-anonymity"problem present in Bitcoin. Therefore, when Zerocoin is used as an incentive method, its transaction rules can hide the identity information and transaction records of both parties in the incentive mechanism, making it suitable for scenarios requiring more comprehensive privacy protection.

2 Blockchain-Based Incentive Mechanisms

Incentive mechanisms employ various motivational methods to encourage organizers and participants to collaborate efficiently, achieve objectives, and maximize benefits. Blockchain-based incentive mechanisms use blockchain-based cryptocurrencies as the incentive method, featuring decentralization, transaction security, and robustness. Organizers and participants can collaborate under conditions of mutual distrust and without third-party supervision, using cryptocurrencies as task remuneration. Different cryptocurrencies' inherent attributes provide transaction privacy protection, low latency, and low cost, while technologies such as micropayment channels and off-chain transactions ensure high throughput and trusted security.

Incentive mechanism design should consider different application scenarios. Under different scenarios, the relationships between roles and interests vary, leading to different settings for transaction verification and remuneration flow. For example, in the incentive mechanism for road condition crowdsensing systems [**?**], the system includes three roles: task initiators, participants, and verifiers. The task initiator issues a traffic condition query request for a geographic location and delivers remuneration to the server. Nearby participants collaboratively perform the sensing task. After verifiers validate the participants' tasks, they obtain remuneration from the server delivered by the initiator in proportion with the participants, thereby enhancing users' enthusiasm for secure transactions and information sharing. In video-on-demand applications based on P2P network streaming distribution incentive mechanisms [**?**], the system includes video-on-demand servers and bandwidth-contributing nodes. The video-on-demand server provides better video service quality to high-contributing nodes while isolating low-contribution nodes to avoid the free-riding problem in P2P networks.

In incentive mechanisms for caching and forwarding files in delay-tolerant networks [**?**], the system includes source nodes, destinations, and relay nodes. The source node provides reward remuneration to relay nodes to incentivize them to cache files, carry and forward file data, and ultimately deliver the data to the destination.

2.1 Incentive Mechanism Transaction Forms

On the Internet, incentive mechanisms mostly use electronic currency as the incentive method to encourage organizers and participants to collaborate and achieve objectives. The incentive process can be viewed as a remuneration transaction process. Blockchain-based incentive mechanisms can provide security guarantees for the transaction process through their inherent cryptographic technologies. The blockchain' s native transaction model prevents double-spending and tampering. Blockchain technology timestamps each transaction and publishes it to the entire network, ensuring that once a currency is spent, it cannot be used for other payments. Once information on the blockchain is verified and added to the chain, it is permanently stored. Unless more than 51% of nodes in the system are simultaneously controlled, modifications to the database by a single node are invalid, thereby ensuring data cannot be illegally tampered with.

However, incentive mechanisms must consider not only double-spending and tampering prevention but also transaction efficiency, security, and privacy. The transaction process should reduce latency. Time-limited commitment mechanisms can ensure the timeliness of transaction payments. Time-limited commitment mechanisms ensure effectiveness through time constraints and penalty deposits, requiring transaction payments to be completed within a specified valid time after legitimacy is determined. Andrychowicz et al. [**?**] designed a "timed commitment" mechanism based on Bitcoin, where tasks must be completed within a limited time; otherwise, a penalty is paid. The transaction process with timed commitment mechanism is shown in Figure 1 [Figure 1: see original paper].

The transaction process should ensure minimal information transmission and low management and storage requirements—that is, high speed and efficiency—while frequently generating small-amount currency payment transactions. Poon et al. [**?**] proposed using micropayment channel networks for trusted transactions between two nodes with long-term cooperation. Transactions are not published on the public chain; only the total Bitcoin amount of the two nodes in the micropayment channel is recorded. The micropayment network reduces block size, lowers miners' computational workload, improves Bitcoin scalability, and achieves near-instantaneous transaction efficiency. The designed micropayment channel network model is shown in Figure 2 [Figure 2: see original paper].

In the channel establishment phase, A and B each transfer X BTC to a multisignature address jointly controlled by both parties, thereby opening a payment

channel that is written into the Bitcoin network. In the off-chain transaction phase, A and B can conduct off-chain transactions in the payment channel without broadcasting or recording, with zero fees. In the channel closure phase, after multiple transactions are completed and there is no further transaction demand, A and B can close the channel. When closing the channel, a transaction is initiated and broadcast to the main network, and miners record it to complete the process. Off-chain transactions in micropayment channels occur only among local nodes, making security difficult to guarantee.

When cryptocurrency is used as an incentive mechanism, without corresponding measures to limit nodes' transfer amounts, nodes may not transfer according to the specified pricing strategy. Moreover, miner nodes may launch deception attacks or collusion attacks, causing insecurity in the incentive mechanism. Trusted hardware approaches require replacing existing equipment at high cost. Recording commitments on the blockchain can prevent tampering and is a relatively feasible approach. Kumaresan et al. [**?**] proposed a functional transfer model based on Bitcoin, constructing a formal model through Bitcoin to support functions such as time-limited transfers, commitment refunds, and deposit compensation. Through these functional transfer models, they implemented provable computation, secure computation, fair computation, and non-interactive bounty tasks. Matsumoto et al. [**?**] proposed a blockchain-based PKI certification authority (CA) security incentive mechanism, defining CA dishonest behaviors and establishing reward-penalty measures to incentivize honest CA behavior. They used Ethereum smart contracts to store CA registration information, dishonest behaviors, reward-penalty transactions, and supervisor records, thereby ensuring the security and trustworthiness of the incentive mechanism.

The transaction process should guarantee that information is not leaked. Even in the Bitcoin network, transaction correlation problems exist, where user real information can be obtained through transaction records and de-anonymization methods. Enhancing transaction correlation has become key to achieving privacy protection in transaction processes. Liu et al. [**?**] proposed an unlinkable coin mixing scheme that allows users to mix their Bitcoins without trusting third parties. This mixing scheme uses a ring signature primitive and employs the Elliptic Curve Digital Signature Algorithm (ECDSA) to hide traces of coin transfer operations between addresses. This method is similar to the CoinJoin technology used by Dash, where user transactions are randomly routed through multiple master nodes and mixed sequentially, increasing the difficulty for attackers to guess transaction correlations. Unless attackers control many nodes, it is nearly impossible to correlate specified transactions, thereby ensuring user transaction privacy. Sasson et al. used non-interactive zero-knowledge proofs (zk-SNARKs) to construct the Zerocash payment framework, achieving strong privacy protection for payment destinations and amounts.

2.2 Classification of Incentive Mechanisms

Cryptocurrency-based incentive mechanisms use cryptocurrencies as remuneration to reward participants who achieve task objectives. Existing classifications include intrinsic and extrinsic incentives [**?**], where intrinsic incentives include self-actualization and entertainment incentives, and extrinsic incentives include material and electronic currency incentives. Incentive mechanisms are also categorized as entertainment incentives, service incentives, and monetary incentives [**?**, **?**, **?**]. On the Internet, electronic currency often serves as incentive remuneration. Pricing strategies determine remuneration amounts and affect the rationality and fairness of incentive mechanisms. Therefore, incentive mechanisms are classified into three categories based on pricing strategy:

1) **Reputation-Based Incentive Mechanisms**
   Reputation-based incentive mechanisms quantify reputation and trust as primary parameters. Based on factors under different conditions, various parameters are calculated through responsive computation methods to ultimately determine eligible remuneration prices. The reputation systems underlying such pricing strategies can be centralized or distributed. Centralized reputation systems have central authorities record, collect, and publish users' historical transaction information and reputation feedback, but they have high operating costs and suffer from central trust deficits. Distributed reputation systems store node reputation information dispersedly among nodes that have transacted, with transaction nodes responding to broadcast queries and feeding back corresponding reputation values. Wang et al. [**?**] proposed a reputation- and trust-based incentive mechanism for mobile users with selfish nodes. The incentive mechanism model consists of a user selection module and a reward implementation module. It comprehensively calculates pricing for service providers through three pricing factors to inhibit selfish behavior. The model comprises service requesters, service platforms, and service providers. In the user selection module, the platform selects winners based on service providers' reputation and trust values. In the reward execution module, the pricing strategy is comprehensively calculated by service quality Q, link strength S, and the probability z that service providers will be accessed within a limited time:

$$P = \theta Q + \delta S + \zeta z$$

where θ, δ, and ζ are weights of the three pricing factors and $\theta+\delta+\zeta = 1$. These three factors represent forwarding quality—the higher the quality, the higher the price. After task execution, the reputation and trust values of requesters and providers are updated respectively. Bogliolo et al. [**?**] proposed a joint incentive method using virtual currency and reputation in specific environments to avoid selfish free-riding nodes damaging the entire system through cooperative incentives. This method includes four stages: discovery and request, negotiation, transaction, evaluation, and feedback. Task pricing uses a reputation-based

piecewise linear function:

$$T = \begin{cases} C_{\min} + \frac{C_{\max} - C_{\min}}{T_{\text{th}}} \cdot T & \text{if } T < T_{\text{th}} \\ C_{\max} & \text{if } T \geq T_{\text{th}} \end{cases}$$

where C is the task intensity, T is the requester' s trust value, $C_{\min}$ is the minimum remuneration (cost) requested by the requester without considering their own reputation, $C_{\max}$ is the maximum remuneration provided for untrusted users, and T_{th} is the reputation threshold at minimum cost.

However, the rationality of reputation quantification is difficult to recognize, such as the rationality of pricing factor proportion allocation and threshold setting, while also facing whitewashing attacks and Sybil attacks [**?**].

2) **Auction-Based Incentive Mechanisms**
Auction-based incentive mechanisms execute task allocation through auction forms, optimizing the interests of task requesters and participants through bidding. Auction-based pricing strategies can be categorized as Myerson auctions, VCG auctions, double auctions, multi-attribute auctions, and reverse auctions.

In bidding mechanisms, the seller' s core problem is how to maximize revenue based on auction rules and buyers' bids. In 1983, Myerson proposed the Myerson Lemma [**?**] to solve the "optimal auction problem" for selling single items in bidding mechanisms. When a task initiator publishes an information transmission task, participants and the publisher report their acceptable real remuneration to reach a transaction at the cost of certain transaction efficiency. However, Myerson' s Lemma cannot solve the optimal problem for selling multiple items.

In combinatorial auction scenarios, achieving optimal revenue from allocating and selling multiple goods becomes a key challenge. The VCG (Vickrey-Clark-Groves) mechanism solves this problem. The VCG auction mechanism is based on dynamic pricing, where the pricing strategy is determined by the loss of benefits the bidder causes to other bidders. As shown in Figure 3 [Figure 3: see original paper], under the VCG mechanism, the pricing for the m-th task in a bidding task is determined by its ranking result in the bidding. For the n-th task ($n \leq m$), pricing is not affected by m; when $n > m$, the pricing for task m is equivalent to the sum of benefit losses for tasks ranked after m in the bidding due to m' s existence.

The VCG auction mechanism is a global optimization strategy that guides participating nodes to honestly upload their actual quotes through incentive mechanism design and reasonable payment functions, providing a more stable transaction environment. David et al. [**?**] analyzed asymmetric scenarios between buyers and sellers, proposing a weighted bilateral VCG auction mechanism that achieves suboptimal allocation by sacrificing allocation optimality without increasing the complexity of optimization problems. Shajaiah et al. [**?**] designed

an energy trading auction mechanism based on the VCG mechanism, using Paillier cryptography for homomorphic encryption to ensure user privacy protection and the value of bidding items, avoiding dishonest behavior by auctioneers.

The double auction mechanism incentive structure involves a platform (auctioneer) purchasing data from mobile users (one bidder) and selling data to sensing task owners (the other bidder). In this auction, the platform first announces allocation rules (task selection and user scheduling) and payment rules (payment prices for scheduled users and prices charged for selected tasks). Then, each task submits a value (bid), and each user submits a sensing cost vector (bid) to the platform, which may differ from the true task value or cost vector. Finally, the platform calculates allocation and payments based on all tasks' and users' bids and other public information. This paper mainly considers designing truthful auction mechanisms where tasks and users submit their private information truthfully. Yong et al. [**?**] designed a double auction mechanism between multi-source users and idle users in cellular networks, solving the optimal allocation problem of source users purchasing relay services from other idle users under energy shortage through double auctions.

Multi-attribute auction mechanisms differ from most single auctions, as this auction competition typically involves many aspects beyond price, such as performance and quality. The platform delivers contracts to participants with the highest total score after evaluating technical features, delivery dates, management performance, and cost information through a complex scoring system. Che et al. [**?**] established a two-dimensional bidding model based on quality and price in government procurement bidding contexts, using three auction schemes: first-score, second-score, and second-preferred bidding. This scheme achieves optimal results by utilizing the buyer' s scoring rule committed to their own maximum benefit. Kang et al. [**?**] studied an online reverse multi-attribute auction mechanism in digital product auction scenarios, introducing multi-attributes into traditional online reverse auction mechanisms to achieve buyer revenue maximization strategies under seller uncertainty.

Reverse auction mechanisms involve one buyer and many potential sellers, where the buyer publishes task requirements and suppliers conduct real-time bidding through specialized network platforms within a valid time. The final quotes at the end of bidding are the suppliers' ultimate offers, and the buyer determines the winning supplier through a comprehensive evaluation model. Chen et al. [**?**] studied the impact of four attributes on supplier bidding strategies in reverse auctions, optimizing the information inequality between buyers and sellers. Zhang et al. [**?**] proposed a two-stage reverse auction mechanism that obtains optimal combinations by mining implicit relationships between price and quality attributes, enabling suppliers to provide private information and buyers to obtain high-quality tasks through information acquisition.

3) **Quality-Contribution-Based Incentive Mechanisms**
   Quality-contribution-based incentive mechanisms assign tasks to participants and calculate task quality cost levels through quality calculation

models after task completion, paying participants corresponding remuneration based on task quality.

Gao et al. [**?**] proposed a quality-aware incentive mechanism for crowdsensing to address low incentive and contribution quality issues, creating utility functions to optimize data quality and setting additional remuneration rewards to make task remuneration more accurate with contribution quality. Selected participants can obtain remuneration p_i, where c_i is the base reward and f_i is the additional reward.

Jin et al. [**?**] proposed an incentive mechanism based on participant information quality to motivate mobile crowdsensing participation, obtaining high-quality data at low cost through quality metrics. Their pricing function is:

$$p_i = \begin{cases} c_i + u & \text{if } i \in S^* \\ 0 & \text{otherwise} \end{cases}$$

where p_i is the task remuneration, c_i is the participant' s cost, and u is the participant' s work effectiveness in the task winner set S^*.

Yu et al. [**?**] proposed a reputation-based incentive mechanism for poor data quality in crowdsensing, quantifying participants' perceived data quality through reputation and providing virtual coupons based on reputation values, giving high-quality contributors priority in pricing rankings. Virtual coupons compensate participants who previously failed to obtain tasks, increasing their chances of winning in the next round. The virtual coupon for participant i in round j is defined as:

$$b_i^j = \frac{r_i^j}{n}$$

where b_i^j is participant i' s virtual coupon in round j, n represents the number of virtual coupons, and r_i^j represents participant i' s reputation quantification value. This virtual coupon is used to improve pricing rankings and increase winning probability. The pricing ranking is defined as:

$$\text{rank}_i = a_i - b_i$$

where a_i represents participant i' s actual bid and b_i represents participant i' s virtual coupon. Each auction selects participants with higher pricing rankings as winners.

Quality-contribution-based incentive mechanisms are limited to scenarios where quality can be quantified and also face issues such as unfriendliness to low-quality participants and low participant engagement.

3 Evaluation Criteria for Incentive Mechanisms

Evaluation criteria for incentive mechanisms are means to measure the security, privacy protection, and performance of incentive mechanisms under specific scenarios and payment methods. They mainly include: (a) security and trustworthiness, aiming to solve selfish node problems in incentive mechanisms and scenarios where miners launch impersonation attacks or collude with participating nodes; (b) privacy protection, considering node information privacy in incentive mechanism design; (c) scalability, addressing transaction bottlenecks in cryptocurrency-based incentive mechanisms in dynamic networks like crowdsensing and DTN; (d) cost overhead, considering the expenses required to implement incentive mechanisms; and (e) sustainability, considering how to maintain user participation sustainably.

3.1 Security and Trustworthiness

Incentive mechanisms face problems where selfish nodes exhibit illegal behaviors in transactions for their own benefit maximization. Security and trustworthiness refer to adopting corresponding measures to ensure user transaction security and mutual trust. Strategies to prevent illegal behaviors typically use identity authentication mechanisms, providing valid proof of node behavior through signatures during transactions. He et al. [**?**] constructed a game model to analyze incentive mechanism security. For security and trustworthiness issues of nodes in distributed opportunistic transmission, they established a remuneration pricing game model. The optimal response strategies for participants under different pricing strategies are:

$$p_i = \begin{cases} \alpha - \frac{1}{2}c_i & \text{if } i \in P \text{ and } c_i > \beta \\ \alpha - \frac{1}{2}c_i & \text{if } i \in E \text{ and } c_i > \beta \\ 0 & \text{if } \frac{2}{n} < \alpha - \beta \end{cases}$$

where p_i is node i' s final payment remuneration, α and β are remuneration-related parameters, P is the set of intermediate nodes, E is the receiver, c_i is the receiver' s communication cost, $c_{\max}$ is the intermediate node' s maximum communication cost, and q is the encounter probability between two nodes. The authors also formally proved that under the condition $\alpha - \frac{1}{2}c_i > \beta$, the mechanism can resist deception attacks from intermediate nodes or miner nodes; under $\frac{2}{n} < \alpha - \beta$, it can resist collusion attacks between receivers and miner nodes; and under $\frac{2}{n} < \alpha - \beta$, it can resist collusion attacks between intermediate nodes and miner nodes. As shown in Figure 4 [Figure 4: see original paper], given relevant parameters, the mechanism can resist the aforementioned deception and collusion attacks when the number of intermediate node hops does not exceed 5.

Security and trustworthiness can be achieved through the inherent security of cryptographic technologies. For instance, Li et al. [**?**] analyzed traffic condi-

tion systems and proposed a reputation-based incentive mechanism to motivate users to share real-time traffic information, using cryptographic technologies such as ring signatures and elliptic curves to solve selfish node and fraud attack problems in the claim process. Cheng et al. [**?**] proposed a secure incentive mechanism for delay-tolerant networks, using signature and verification technologies to incentivize intermediate node forwarding behavior and solve selfish node problems.

Threshold signatures, as a cryptographic technology, can be used to solve collusion attack problems in security and trustworthiness. A threshold signature means a task is shared by n members with a group key. When the number of participating signers is greater than or equal to the specified threshold value t, they can represent the group to generate signatures, and any verifier can verify signature validity with the group public key. Its security is reduced to the Computational Diffie-Hellman problem—if no probabilistic polynomial-time algorithm A can solve the CDH problem on cyclic groups within time t with probability at least ε, then the threshold signature scheme is secure. In 2006, Yang et al. [**?**] proposed a fuzzy identity-based signature scheme. In 2007, Khader [**?**, **?**] proposed attribute-based group signature schemes and attribute-based group signature schemes with anonymous revocation functions. Chen et al. [**?**] analyzed existing attribute-based threshold signature schemes and introduced secret random factors to prevent collusion attackers from forging signatures by combining private keys. Qin et al. [**?**] proposed a secure identity threshold signature scheme based on access structures, reducing the design complexity of (t, n) threshold structures based on Lagrange interpolation, making system applications more widespread and providing security proofs under adaptive chosen-message attacks to ensure system security and trustworthiness.

3.2 Privacy Protection

Incentive mechanism design should also consider not leaking personal privacy information, but the openness of blockchain often exposes incentive relationships between users, user identities, or user behaviors. Wang et al. [**?**] achieved privacy protection in incentive mechanisms through K-anonymity methods. For blockchain-based cryptocurrencies as incentive methods, miners are responsible for quantifying and verifying sensing quality to obtain node privacy. The k-anonymity approach distributes part of the verification work to nodes in the task to protect privacy. Single-node verification significantly increases storage, computation, and communication overhead and can be easily tracked through IP addresses, while node group collaboration is more efficient in transaction verification. As shown in Figure 5 [Figure 5: see original paper], during verification, the system assigns part of the miner' s work to node groups, where server S transacts with user group G consisting of k users. Users desensitize privacy data through node groups, causing attackers attacking any data record in the group to be associated with $k-1$ records in the group, making it impossible to determine associated information and reducing privacy leakage from linking

attacks.

Kim [**?**] proposed an on-demand incentive method using group signature technology to protect user location and privacy. Zhuo [**?**] proposed a privacy-preserving framework for crowdsourcing using differential privacy technology to protect miners' data privacy.

3.3 Scalability

Scalability refers to ensuring information network service quality and efficiency while achieving system scalability and high efficiency without sacrificing security, trustworthiness, privacy protection, or communication overhead. Incentive mechanisms need to consider miner verification efficiency, transaction efficiency, and transaction bottlenecks in cryptocurrency-based incentive mechanisms in dynamic networks such as crowdsensing and DTN networks. For example, Luu et al. [**?**] proposed a scalable public blockchain distributed consensus protocol that randomly divides system nodes into groups to verify different transactions in parallel, achieving group consensus through Byzantine protocols to enhance transaction throughput, making computing power increase almost linearly with the number of transactions per unit time. However, the Byzantine protocol used within groups has large latency. Figure 6 [Figure 6: see original paper] shows network delay based on Byzantine protocols. Even with a Byzantine network scale of 100, delay grows quadratically with network scale, and when malicious nodes exist, delay further increases.

Bitcoin-NG [**?**] is a scalable blockchain protocol based on the Bitcoin trust model, dividing traditional Bitcoin mining into keyblocks and microblocks. Keyblocks are used for leader election, maintaining the traditional ten-minute interval to ensure security. Microblocks record transactions without containing proof-of-work, with a block time of 10 seconds, improving transaction speed. Bitcoin-NG, as a serialized transaction blockchain protocol, optimizes latency and bandwidth without sacrificing other conditions. Figure 7 [Figure 7: see original paper] shows Bitcoin-NG latency under different numbers of microblocks. As network node numbers increase and intra-group block numbers increase, system performance decreases. Bitcoin-NG protocol requires nodes to broadcast all blocks to the entire network as it is necessary for serialized transactions, so as the network scales, increased block throughput requires longer time.

Sompolinsky et al. [**?**] improved upon Bitcoin' s original protocol by using DAG graph structures instead of chain structures, optimizing transaction processing waiting time and increasing transaction processing rate while ensuring security, raising block generation rate to 600 times the previous rate.

4 Conclusion

This paper surveys and reviews recent research on incentive mechanisms related to blockchain technology. We first overview blockchain concepts and comparatively analyze cryptocurrency attributes. We then analyze blockchain-based

incentive mechanism transaction methods, classify incentive mechanisms according to pricing strategies, and summarize evaluation criteria such as security/trustworthiness, privacy protection, and scalability. We discuss the advantages and disadvantages of incentive mechanisms under blockchain technology. The literature review shows that research on blockchain-based incentive mechanisms is still in its infancy. Future work needs to improve upon the requirements and objectives of blockchain-based incentive mechanisms, exploring more combinations of incentive mechanisms with blockchain advantages. When specifically designing incentive mechanisms, blockchain incentive architectures cannot yet achieve precise adaptation, and some strategy details remain incomplete. Future blockchain-based incentive mechanisms need to expand research in the following aspects:

a) **Compatibility and adaptation of relevant incentive strategies**: Different cryptocurrencies, pricing strategies, and payment forms have corresponding requirements for hardware performance and systems. Whether they can be implemented or improved for applicability in corresponding application scenarios is worth studying. For example, how to use lightweight cryptocurrencies to incentivize IoT devices in IoT application scenarios, how to apply privacy-preserving cryptocurrencies in cloud computing scenarios to ensure data security, and how to use pricing strategies to achieve fairness and trustworthiness in big data platform transactions.

b) **Performance improvement of incentive effects**: As an emerging technology, blockchain still has many optimization issues in privacy protection and scalability. Qualitative breakthroughs are needed in certain incentive effect aspects, such as using zero-knowledge proof technology to enhance privacy protection effects and implementing encrypted search and access control on this basis, and using parallel processing, batch processing, and batch authentication technologies to enhance transaction verification speed and improve incentive mechanism scalability.

c) **Multi-objective joint optimization**: Incentive mechanisms are often more complex in practical applications, requiring joint consideration and optimization of multiple incentive effects, some of which conflict with each other, such as privacy protection vs. efficiency, security/trustworthiness vs. usability, and cost overhead vs. security.

d) **Organic integration with centralized incentive mechanisms**: Centralized incentive mechanisms currently exist widely, and completely replacing them may be unrealistic. How to make blockchain-based incentive mechanisms coexist and organically integrate with centralized incentive mechanisms is an urgent problem to be solved.

References

[1] Li L, Liu J, Cheng L, Qiu S, Wang W. CreditCoin: A Privacy-Preserving Blockchain-Based Incentive Announcement Network Communications of Smart

Vehicles [J]. IEEE Transactions on Intelligent Transportation Systems, 2018, 19 (7): 2204-2220.

[2] Zhang Y Q, Bai X Y, Liu Q. Incentive mechanisms in mobile delay tolerant network [C]// 2017 7th IEEE International Conference on Electronics Information and Emergency Communication, 2017: 184-188.

[3] Yang C G, Xiao J, Li J D, Shao X Q, Anpalagan A, Ni Q, Guizani M. DISCO: Interference-Aware Distributed Cooperation with Incentive Mechanism for 5G Heterogeneous Ultra-Dense Networks [J]. IEEE Communications Magazine, 2018, 56 (7): 198-204.

[4] Zhan Y, Xia Y, Zhang J, Wang Y. Incentive Mechanism Design in Mobile Opportunistic Data Collection With Time Sensitivity [J]. IEEE Internet of Things Journal, 2018, 5 (1): 246-256.

[5] Islam M A, Mahmud H, Ren S, Wang X. A Carbon-Aware Incentive Mechanism for Greening Colocation Data Centers [C]// IEEE Transactions on Cloud Computing, 2017: 1-17.

[6] Zhai Y, Bai X, Liu Q. Incentive mechanisms in mobile delay tolerant network [C]// IEEE International Conference on Electronics Information and Emergency Communication, 2017: 184-188.

[7] Rezai A A, Torki L. The impact of the electronic money development in the profitability of DBS banks of Singapore [C]// International Conference on E-commerce in Developing Countries: with Focus on E-trust, 2014: 1-9.

[8] Huicong Security Network. The top ten data breaches in 2017, [OL]. [2018-10-01]

[9] Sohu News Website. Sohu, The top ten data breaches in 2016, [OL]. [2018-10-01] http://www.sohu.com/a/122021640_{526642}

[10] Wang J Z, Li M R, He Y H, Li H, Xiao K. A Blockchain Based Privacy-Preserving Incentive Mechanism in Crowdsensing Applications [J]. IEEE Access, 2018, 6 (3): 17545-17556.

[11] Kuzuno H, Karam C. Blockchain explorer: An analytical process and investigation environment for bitcoin [C]// Electronic Crime Research, 2017: 9-16.

[12] Urien P. Towards secure Bitcoin fast trading: Designing secure elements for digital currency [C]// International Conference on Mobile & Secure Services, 2017: 1-5.

[13] Neudecker T, Andelfinger P, Hartenstein H. Timing Analysis for Inferring the Topology of the Bitcoin Peer-to-Peer Network [C]// Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People, & Smart World Congress, 2017.

[14] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system, [OL]. [2018-10-01] http://www.bitcoin.org/bitcoins.pdf

[15] Gobel J, Krzesinski A E. Increased block size and Bitcoin blockchain dynamics [C]// Telecommunication Networks & Applications Conference, 2017: 1-6.

[16] Li L, Liu J, Cheng L, Qiu S, Wang W. CreditCoin: A Privacy-Preserving Blockchain-Based Incentive Announcement Network Communications of Smart Vehicles [J]. IEEE Transactions on Intelligent Transportation Systems, 2018, PP (99): 1-17.

[17] Sheshjavani A G, Akbari B, Ghaeini H R. A free-riding resiliency incentive mechanism for VoD streaming over hybrid CDN-P2P networks [C]// International Symposium on Telecommunications, 2017: 771-776.

[18] Ezzahidi S A, Sabir E, Kamili M E, Bouyakhf E H. A non-cooperative file caching for delay tolerant networks: A reward-based incentive mechanism [C]// Wireless Communications & Networking Conference, 2018.

[19] Andrychowicz M, Dziembowski S, Malinowski D, Mazurek L. Secure Multiparty Computations on Bitcoin [C]// IEEE Symposium on Security and Privacy, 2014: 443-458.

[20] Poon J, Dryja T. The bitcoin lightning network: Scalable off-chain instant payments [OL]. [2018-10-01] http://lighting:network-network-paper:pdf, 2016

[21] Kumaresan R, Iddo B. How to Use Bitcoin to Incentivize Correct Computations [C]// 21st ACM Conference on Computer and Communications Security (CCS 2014), November 3-7, 2014.

[22] Stephanos Matsumoto, and Raphael M. Reischuk. IKP: Turning a PKI Around with Decentralized Automated Incentives [C]// The 38th IEEE Symposium on Security and Privacy (S&P 2017), May 22-24, 2017, San Jose, CA, USA

[23] Liu Y, Liu X T, Tang C J, Wang J, Zhang L. Unlinkable Coin Mixing Scheme For Transaction Privacy Enhancement of Bitcoin [J]. IEEE Early Access Articles, 2018, 6 (4): 23261-23270.

[24] 王娟, 王丽清, 马文倩, 徐永跃. 群智协同激励机制研究综述 [J]. 计算机工程与应用, 2020: 1-12.

[25] Jaimes Luis G, Vergara-Laurens Idalides J, Raij Andrew. A Survey of Incentive Techniques for Mobile Crowd Sensing [J]. IEEE INTERNET OF THINGS JOURNAL, 2015 (2): 370-380.

[26] Hui Gao, Chi Harold Liu, Wendong Wang, Jiaxin Zhao, Zheng Song, Xin Su. A Survey of Incentive Mechanisms for Participatory Sensing [C]// IEEE Communications Surveys & Tutorials, 2015, 17 (2): 918-943.

[27] Xinglin Zhang, Zheng Yang, Wei Sun, Yunhao Liu, Shaohua Tang, Kai Xing, Xufei Mao. Incentives for Mobile Crowd Sensing: A Survey [C]// IEEE Communications Surveys & Tutorials, 2016, 18 (1): 54-67.

[28] Huilin Wang, Chunxiao Liu, Yanfeng Wang, Dawei Sun. A Novel Incentive Mechanism Based on Reputation and Trust for Mobile Crowd Sensing Network [C]// 5th International Conference on Cross-Cultural Decision Making, 2016.

[29] A Bogliolo, P. Polidori, A Aldini, Virtual Currency and Reputation-Based Cooperation Incentives in User-Centric Networks [C]// 2012 8th International Wireless Communications and Mobile Computing Conference (IWCMC), Aug. 2012.

[30] Xuewen Dong; Qiao Kang; Yang Xu; Zhuo Ma, Teng Li. Poster Abstract: A Practical Sybil-Proof Incentive Mechanism for Multichannel Allocation [C]// IEEE Conference on Computer Communications Workshops (INFOCOM WKSHPS), 2019.

[31] Myerson R, MA Satterthwaite. Effient mechanism for bilateral trading [J]. Journal of Economic Theory, 1983, 29 (2): 265-281.

[32] David E, Azoulay R. It Does Matter Who I sell to and Whom I Buy From: Weighted Bilateral VCG [C]// IEEE/WIC/ACM International Conference on Web Intelligence and Intelligent Agent Technology, 2015.

[33] Shajaiah H, Abdelhadi A. Clancy C. Secure power scheduling auction for smart grids using homomorphic encryption [C]// IEEE International Conference on Big Data, 2017: 4507-4512.

[34] Wang Yong, Yun Li, Liao Chao, Chong gang Wang, Xiaolong Yang. Double-Auction-Based Optimal User Assignment for Multisource–Multirelay Cellular Networks [J]. IEEE Transactions on Vehicular Technology, 2015, 64 (6): 2627-2636.

[35] Yeon-Koo Che. Design competition through multidimensional auctions [J]. The Rand Journal of Economics, 1993, 24 (4): 668-680.

[36] Wanglin Kang, Lei Wang, Yanan Jiang. A Multi-attribute Auction Model for Online Digital Goods [C]// Proceedings of the 25th China control and decision-making conference, 2013.

[37] Chen Guowei. Reverse auction format choice decision based on supplier attributes [C]// International Conference on Service Systems & Service Management, 2015.

[38] Lufang Zhang. Reverse Auction Mechanism Design with Quality Preference [C]// International Conference on Service Systems & Service Management, 2015.

[39] Gao, Hui, Liu, Chi Harold, Tang, Jian. Online Quality-Aware Incentive Mechanism for Mobile Crowd Sensing with Extra Bonus [C]// IEEE Transactions on Mobile Computing, 2018.

[40] Haiming Jin, Lu Su, Danyang Chen, Hongpeng Guo, Klara Nahrstedt, Jinhui Xu. Thanos: Incentive Mechanism with Quality Awareness for Mobile Crowd Sensing [J]. IEEE Transactions on Mobile Computing, 2018, 18 (8): 1951-1964.

[41] Ruiyun Yu, Jiannong Cao, Rui Liu, Wenyu Gao, Xingwei Wang, Junbin Liang. Participant Incentive Mechanism Toward Quality-Oriented Early Sensing: Understanding and Application [C]// Transactions on Sensor Networks 15 (2): 1-25.

[42] He Y H, Li H, Cheng X Z, Liu Y, Yang C, Sun L. A Blockchain based Truthful Incentive Mechanism for Distributed P2P Applications [C]// IEEE Access, 2018: 1-11.

[43] Cheng Gong; Wang Bo; Zhao Faru, SIS: Secure Incentive Scheme for Delay Tolerant Networks [C]// 2012 11th International Symposium on Distributed Computing and Applications to Business, Engineering & Science, 2012.

[44] Yang P, Cao Z, Dong X. Fuzzy identity based signature with applications to biometric authentication [J]. Compute and Electrical Engineering, 2011, 37 (4): 532-540.

[45] KHADER D. Attrebute based group signatures [OL]. [2018-10-02]. https://eprint.iacr.org/2007/159.pdf.

[46] KHADER D. Attribute based group signature with revocation [OL]. [2018-10-01]. http://eprint.iacr.org/2007/241.

[47] 陈桢, 张文芳, 王小敏. 基于属性的抗合谋攻击可变门限环签名方案 [J]. 通信学报, 2015, 36 (12): 212-222.

[48] Qin H W, Zhu X H, Dai Y W. Provably Secure Identity-Based Threshold Decryption on Access Structure [C]// Tenth International Conference on Computational Intelligence & Security, 2014: 464-468.

[49] Kim M. Incentive mechanism with privacy-preservation on intelligent parking system utilizing mobile crowdsourcing [C]// 2017 4th International Conference on Computer Applications and Information Processing Technology, 2017: 1-4.

[50] Zhuo G Q. Privacy-preserving and fine-grained data aggregation framework for crowdsourcing [C]// Tenth International Conference on Mobile Computing and Ubiquitous Network, 2017: 1-6.

[51] Luu L, Narayanan V, Zheng C, Baweja K, Gilbert S. A Secure Sharding Protocol For Open Blockchains [C]// Acm Sigsac Conference on Computer & Communications Security, 2016: 17-30.

[52] Eyal I, Gencer A E, Sirer E G, et al. Bitcoin-ng: A scalable blockchain protocol [C]// 13th USENIX Symposium on Networked Systems Design and Implementation (NSDI 16). USENIX Association, 2016: 45-59.

[53] Sompolinsky Y, Zohar A. Accelerating bitcoin' s transaction processing fast money grows on trees, not chain [OL]. [2018-11-01]. https://eprint.iacr.org/2013/881.pdf

Note: Figure translations are in progress. See original paper for figures.