Hindawi
Security and Communication Networks
Volume 2023, Article ID 6403686, 10 pages
https://doi.org/10.1155/2023/6403686

Research Article

Contract-Based Incentive Mechanism for Redactable Proof-of-Stake Blockchains

Yumei Wang, Yongdong Wu, and Junzuo Lai

Jinan University, Guangzhou 510632, China

Correspondence should be addressed to Yongdong Wu; wuyd007@qq.com

Received 21 October 2022; Revised 7 April 2023; Accepted 3 May 2023; Published 17 May 2023

Academic Editor: Andrea Michienzi

Blockchain has received a lot of attention due to its immutability. However, the immutability characteristic prohibits editing the blocks which need to be modified. Although the existing redactable blockchain enables to manipulate blocks in a controlled way, it may suffer from the security threats if the number of honest committee members (CMs) is insufficient. Thus, to attract honest CMs for validating and voting the editing blocks in permissionless blockchain, this paper presents a contract-based incentive mechanism between contract issuer and every CM. Firstly, it models the interaction between the contract issuer and each CM in the verifying and voting process. Secondly, it builds an incentive mechanism according to the contract issuer's cost and the committee size. Finally, it selects a sufficiently large number of CMs with an optimization method. The analysis shows that the present mechanism is secure against Sybil attack, and the simulations demonstrate that the proposed mechanism is effective.

1. Introduction

As the underlying technology of Bitcoin proposed in 2008 [1], blockchain has received widespread attention due to its immutability merits. Nevertheless, the immutability of blockchain has shown some side effects. For example, if a blockchain has been misused to store and distribute inappropriate content such as child pornography and material that infringes on intellectual property rights on the chain, the immutability of the blockchain prevents fulfilling the data regulations such as the "right to be forgotten" [2] and General Data Protection Regulation (GDPR) [3]. As a result, some chain participants may be reluctant to participate the blockchain for fear of being accused of possessing illegal information.

To overcome the shortcoming of the immutability, a redacting process is employed to rewrite the block data in a secure and controlled manner [4]. Usually, it varies with the consensus mechanisms in the blockchains. For the most popular POW blockchains and POS blockchains, cryptographic primitive based redacting and voting based redacting are preferable, respectively.

As a POS-like blockchain consumes much less energy than a POW counterpart and is deployed widely, this paper focuses on the POS blockchain, in particular to its redacting process. Generally speaking, a redacting process for POS blockchain composes of four main steps (e.g., [5]): (1) submitting an editing request from a user; (2) selecting a leader and Committee Members (CMs) in blockchain; (3) voting on the editing request from CMs; and (4) updating the block data. Specifically, at the beginning of each editing time slot, CMs are pseudo-randomly selected as volunteers according to their stakes by a verifiable random function (VRF) [6] and then verify the editing blocks before deciding whether to vote on them. However, if CMs spend resources to vote without reward, they may be reluctant to participate honestly in validating editing blocks and voting on candidate blocks over time. As a result, it increases the security risk that the data on the chain are maliciously tampered with.

In the editing process, it is critical to select as many honest CMs as possible to reduce security risks because rewriting old consensus blocks requires a stricter consensus approach. We believe that the higher the voting power, the more honest the CMs will be, because the larger the

percentage of stake in the blockchain, the less they want the blockchain to suffer from the security risk of tampering. To this end, this paper designs an incentive mechanism to motivate more CMs with higher voting rights to join in the validation and voting of rewriting blocks. Thus, it has to address two challenging problems. Firstly, the leader does not know in advance which stakeholder would become a CM and would be willing to participate in validation and voting. Secondly, he does not have an accurate value of the CMs' voting rights and does not know how the CMs would vote. Information asymmetry between the leader and CMs may lead to high costs for the leader to complete the editing process. Therefore, the best strategy for a leader is to design an incentive mechanism that reduces the impact of information asymmetry. In addition, the more CMs contribute, the more rewards they will receive. Accordingly, this paper presents a contract-based incentive mechanism. The addition of contracts allows the scheme to not only effectively motivate CMs to participate in redactable block validation and voting but also to maximise the utility of the leader. The contributions of this paper can be summarised as follows:

(1) Design an incentive mechanism to inspire more CMs with higher voting power to participate honestly in validating edit blocks and voting on candidate blocks. As long as a CM completes her validation and voting tasks, she will be rewarded with a portion of the transaction fee provided by the leader.

(2) Propose an enhanced redactable POS blockchain scheme for permissionless systems, so as to mitigate the security risk of tampering with data on the chain. The security analysis shows that the present scheme is secure against Sybil attack.

(3) Carry on abundant simulations to demonstrate that the present contract-based incentive mechanism achieves high performance in member utility compared to a contract with no information asymmetry. Thus, the present mechanism will have honest CMs enough to engage in voting.

The rest of the paper is organized as follows. Section 2 introduces the related work in redactable blockchain and incentive mechanism for blockchain. Then, in Section 3, we introduce the system model and the attack model. In Section 4, we introduce the overview of the enhanced Redactable POS Blockchain. The problem formulation and optimal contract designing for information asymmetry are elaborated in Section 5. Section 6 evaluates the performance of the designed contract. Finally, Section 7 concludes this paper and presents future work.

2. Related Work

Nowadays, the growing fusion of blockchain technology with other fields has been contributed by many scholars. Rathee et al. [7] proposed a blockchain framework that addresses the security problem of malicious intrusion on smart devices by adversaries in the Internet of Vehicles. Further, Rathee et al. [8] proposed a device-trustworthy management approach with the help of blockchain-based data transparency for the possible network adversaries in industrial Internet of things (IoT). Krishnamurthy et al. [9] proposed a voting layout based on blockchain and IoT devices in order to enhance the security of e-voting. In addition, Cai et al. [10] proposed an oracle protocol by utilizing alternative mechanisms to filter objective information from subjective data. The expanding applications of blockchain have also led to increased concerns about the security of data on the chain. Therefore, this section briefs the redactable scheme and incentive mechanism. The incentive mechanism is used to attract the CM so as to guarantee the security of the redactable scheme.

2.1. Redactable Scheme. To remove harmful data in the blockchain, redactable blockchain has been proposed. According to the authorization and modification method, the existing redactable schemes are mainly divided into two types: authorization-based chameleon hashing function and voting-based double hash chain.

In the redactable scheme with authorization-based chameleon hashing function, the trapdoor of the chameleon hash function is used to calculate hash collisions for arbitrary input data, thus enabling changes to block data without changing the original block connection. Ateniese et al. [4] first proposed a block-level redactable scheme based on chameleon hash functions, where authorized entities can obtain trapdoors and compute hash collisions for the corresponding blocks. Further, Derler et al. [11] proposed the policy-based chameleon hashes (PCH), which refers to the ability of anyone with all the permissions required by a policy to have the ability to compute arbitrary collisions for a given hash and hence enables fine-grained and controlled editing at the transaction level. Subsequently, accountability [12], revocation [13], supervision [14], and k-time [15] are embedded to make the editable scheme be more relevant to practical applications.

In the voting-based redactable scheme, anyone who harvests enough votes will be able to reach a consensus among the users on the chain to change the block. In order to eliminate a trusted central authority, Deuber et al. [16] proposed a block-level double hash chain scheme under nonauthorisation through consensus-based voting. This scheme extends the structure of adjacent blocks by preserving a copy of the Merkle root in its original state. In such a way, the integrity of the hash link among blocks is not broken, even if the hash value of the new block changes. To speed up voting for consensus, Li et al. [5] proposed an instantly editable blockchain protocol for POS and POW. The protocol pseudo-randomly selects the committee based on stake or computing power. That committee will validate edit blocks and voting on candidate blocks. Of these, completing a redaction requires only a time slot in the case of a synchronous network in POS blockchain.

In general, most editing schemes based on chameleon hash function require a trusted central entity to grant editing rights, and some schemes still require complex multiparty

computation (MPC) to manage chameleon hash traps, and the nondisclosure of traps makes it impossible for the public to verify the edited blocks. The voting-based consensus editing schemes achieve a decentralized, publicly verifiable editing process and do not require complex cryptographic primitives. However, the voting-based schemes demand a high level of honesty from the members involved in validating the editing blocks. In practical scenarios, often rational members are unwilling to spend extra computational resources and time to participate in the editing process. Therefore, this paper investigates an incentive mechanism to motivate members to honestly participate in the editable voting process.

2.2. Incentive Mechanism. As POS-type blockchain becomes more and more popular, Kang et al. [17] built a Stackelberg game to jointly maximise the utility of blockchain user and the profit of each miner on the POS-based consortium blockchain network. The game is designed to incentivize miners to participate in the verification and propagation of mined block, using the transaction fee of the blockchain user as a reward. However, it may be not practical because the game model assumes the information between leader and CMs is symmetrical. Later, Kang et al. [18] proposed a delegated proof of stake (DPoS) blockchain. The scheme is designed to allow highly reputable candidates to be selected as active miners and standby miners. Incentive is designed to motivate candidate miners to participate in block validation and prevent internal collusion among active miners. The designed mechanism is based on contract theory with asymmetric information. However, it is not applicable to secure data editing in the POS blockchain.

In summary, contract theory and other game theoretic approaches have been applied and developed in the blockchain domain. Nevertheless, there is a common problem with many of these works: the universality of the methods is not high. Consequently, in order to be able to effectively solve the incentive problem in the editable blockchain scenario, further research on secure and feasible contract theory schemes is necessary.

3. Preliminaries

In this section, we introduce the system model and the security model considered in this paper.

3.1. System Model. The current voting-based editable blockchain [5] retains the data structure of the block header and block body with a new replica of the Merkle root of the original data in the block header. This double hash chain model ensures the integrity of the blockchain after data modification. To the best of our knowledge, there is a lack of incentive measures for committee in existing voting-based editable blockchain, i.e., committees are not rewarded for their contribution. This greatly reduces the interest of CMs in participating in data editing. Therefore, in this paper, we propose an editable scheme with incentives that allows CMs to actively choose whether to complete voting and validation tasks based on workload and rewards.

At the high level, our system consists of three entities as shown in Figure 1: leader, user, and CM. When there is no user request to edit, the blockchain elects the leader via an underlying POS-based protocol, which generates the next block as usual. Otherwise, a committee is elected locally using the VRF to make pseudo-random decisions based on the stakeholder's stake. The committee needs to participate in the vote on the edit request. The output of VRF and a staked cryptographic sortition method will determine how many votes the member will get. The number of votes an edit block receives above a certain threshold is considered a consensus reached by the whole network. The specific design of the above process can be found in [5]. However, CM requires some computational resources and power to validate the edit block and complete the voting process. To encourage nodes to participate in the block editing process, our designed system rewards participating members in the form of transaction fees. More details about the scheme are given in Section 4. And we introduce the problem formulation, optimal contract in Section 5. For the convenience of the readers, we have listed the main notations used in the paper in Table 1.

3.2. Security Model. With reference to Figure 1, the participants jointly update a permissionless redactable blockchain. The blockchain stores the edited blocks and nonedited blocks including transactions submitted by the user, validated and voted by the CMs, and recorded by the leader. The committee that votes on the editable blocks is elected based on the stakes among stakeholders. A leader is supposed to be honest and rational in the present protocols.

A user is assumed to be malicious if he behaves in the following ways: (1) broadcasts a large number of meaningless edit requests and (2) publishes an edit request intended to add harmful data to the chain.

A CM can be honest, lazy, or malicious. In particular, (1) members are considered honest when they have truly validated the editable block and voted honestly based on the results of the validation; (2) they are assumed to be lazy when they skip the editable block validation or vote for it randomly; (3) malicious members vote in the opposite way in accordance with the validation results. The tolerance for malicious CMs is strictly less than $(T/2)$, where T is the expected committee size of stakes. A malicious vote by a CM could result in illegally tampering with the data on the chain.

4. Overview of the Enhanced Redactable POS Blockchain

In this section, a contract-based redactable POS Blockchain is described, where the contract is designed as an incentive mechanism to motivate higher voting rights committees to join the validation and voting of editable blockchain data. In other words, in order to ensure the consistence among all the nodes in the blockchain after editing, the number of honest CMs shall be sufficiently high in the validation and voting of

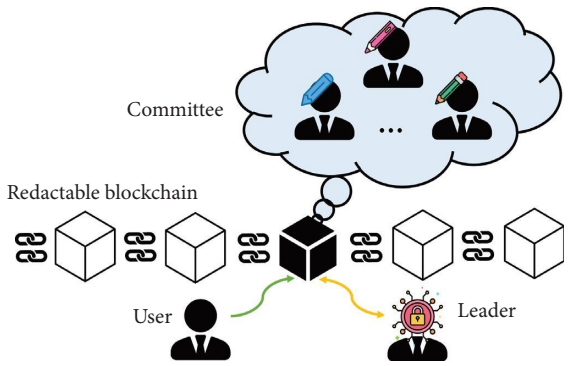

Figure 1: The system model.

Table 1: List of main notations.

Notations	Description
$\mathcal{U}$, G	Set of CMs, types of CMs be classified
θ_g	g-type
R_g, F_g	g-type CMs' incentives, g-type CMs' resources
U_l, U_m	Utility of leader, utility of CM
$c^{'}$	Unit value of resources for leader
c	Unit cost of computing resources spent by a CM
P_g	Prior probability of a g-type CM
$v(\bullet)$	A monotonically increasing valuation function
$R_{\max}$	Total editable transactions' fee
UC	Utility of a CM for launching the Sybil attack

editing block. Hence, it is in desire to develop an incentive mechanism to attract CMs.

As illustrated in Figure 2, we present an overview of the scheme to enhance the security of the redactable blockchain by embedding a contract-based incentive mechanism. A detailed design of the mechanism will be described in Section 5. The present redactable POS blockchain has three entities: (1) blockchain users, (2) leader, and (3) CMs. If a user wants to make an edit request and after broadcasting that request to the network, the mechanism allows for the editing of blocks by performing the following main steps:

① The leader develops the contract set based on the information he can gather about the committee and then broadcasts the set of contracts to the blockchain network.

② Each CM selects a corresponding contract and signs it and then carries out the tasks in accordance with the provisions of the contract.

③ The CM returns a proof including the voting outputs (i.e., edited blocks' verification and voting results) to the leader.

④ The leader gathers the proofs to verify the eligibility of voters and the vote results. When the number of the proofs associated with the editing blocks is higher than the vote threshold, the proofs are compressed and packed into a new block. Afterwards, a fee is paid to the corresponding CMs in accordance with the terms of the contract.

Finally, similar to [5], blockchain users check that whether the edit blocks meet the policy, i.e., whether the votes exceed the threshold and whether the blocks embedded in the votes satisfy the requirements of the blockchain. If yes, blockchain users will update the data locally.

5. Contract-Based Incentive Mechanism

Section 4 describes the overview of the enhanced redactable blockchain which includes an important incentive mechanism for attracting CMs. This section will elaborate the mechanism.

5.1. Problem Formulation. In each time slot, a monopoly market consists of a leader as task issuer and a set of CMs $\mathcal{U}$. In order to attract more CMs with high voting rights in validation and voting, we use the level of votes as a classification criterion for the type of CMs, i.e., CMs can be classified according to their votes: $\theta_1 < \ldots < \theta_g < \ldots < \theta_G$, $g \in \{1, \cdots, G\}$, where θ_g denotes a CM with a number of votes within a certain range. In this paper, assume that all CMs are rational. That is to say, a CM with more votes pays more attention to take part in the voting process.

The leader must overcome the resulting economic loss due to the information asymmetry caused by the leader not knowing the specific types of CMs. The leader offers CMs of different types contracts containing a series of reward-performance packages $(R_g(F_g), F_g)$. In this case, F_g is the validation and voting performance requirement for a CM of θ_g, and $R_g(F_g)$ is the corresponding reward to a CM of θ_g. If a CM completes a validation and voting task to a higher quality, i.e., the more computing resources invested, the more rewards the member will receive.

(1) Utility of the Leader: Depending on the contract (R_g, F_g) between a CM of type g and the leader, the utility function of the leader can be expressed as follows:

$$U_l(\theta_g) = c^{'} F_g - R_g, \tag{1}$$

where $c^{'} > 0$ is the unit value of computing resources for the leader, F_g is the required computing resources provided to the leader by a CM of type g, and R_g is the reward that leader must provide to a CM of type g under the contract (R_g, F_g) where the reward refers to the transaction fee provided by the blockchain users who make the edit requests. The utility of the leader is the benefit generated from the resources invested by the CMs minus the incentive to the CMs. For a validation and voting task with G types of CMs participating, the total utility available to the leader as task issuer is

$$U_l = \sum_{g=1}^{G} \left(|\mathcal{U}|P_g\right)\left(c^{'} F_g - R_g\right), \tag{2}$$

where P_g is the prior probability of a CM of type g, and $\sum_{g=1}^{G} P_g = 1$. According to reference [5], it is known that the ballot of a CM is broadcast to the entire blockchain network, where the ballot contains

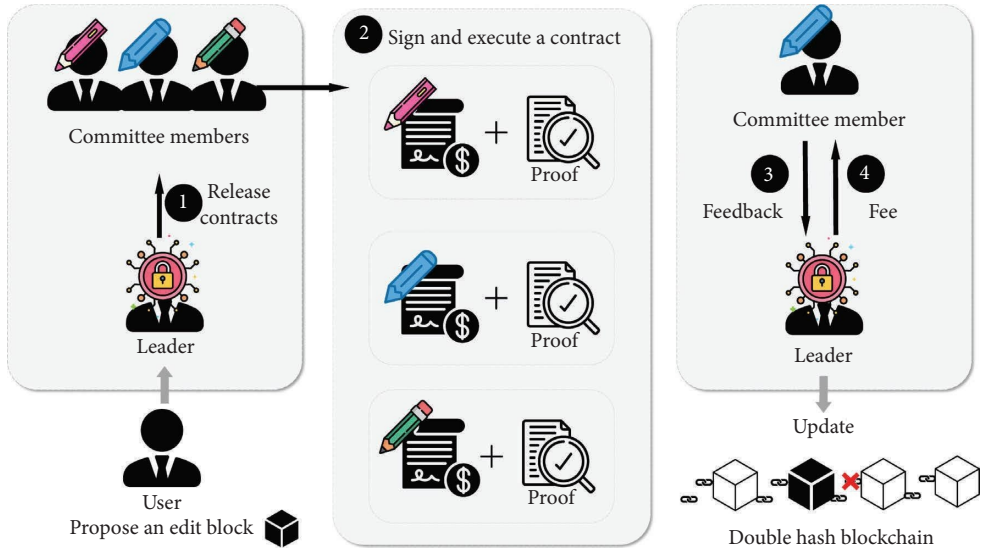

Figure 2: Diagram of the enhanced redactable POS blockchain scheme.

the specific number of votes that the member has. As a result, the leader has access to the voting information of all previous CMs for each slot. Based on the historical CMs' voting information obtained, the leader can statistically determine the historical probability distribution of members' types. Assuming that the stakes of blockchain users do not change over time, leader can infer the current probability distribution based on the historical distribution. The leader's goal is to maximise profits through the validating and voting process as follows:

$$\max_{(R_g,F_g)} U_l = \sum_{g=1}^{G} \left(|\mathcal{U}|P_g\right)\left(c^{'}F_g - R_g\right). \tag{3}$$

(2) Utility of CMs: For a CM of type g, based on the signed contract, the utility function is defined as follows:

$$U_m = \theta_g v\left(R_g\right) - cF_g, \tag{4}$$

where $v(R_g)$ is a monotonically increasing valuation function of the incentive R_g for a CM of type g, where $v(0) = 0$, $(\partial v/\partial R) > 0$, and $(\partial^2 v/\partial R^2) < 0$, and c is the unit cost of computing resources spent by a CM. The utility of CMs is the reward received from the leader minus the cost expended. However, CMs wish to maximise their utility by minimising the resource consumption in the validation and voting process. Specifically, the goal of a CM of type g is to maximise his utility, denoted as follows:

$$\max_{(R_g,F_g)} U_m = \theta_g v\left(R_g\right) - cF_g, \forall g \in \{1,\ldots,G\}. \tag{5}$$

(3) Contract Feasibility: Given that the utility function for a certain type CM is defined as equation (4), the contract theory suggests that each contract item for CMs must satisfy the following principles of individual reasonableness (IR) and incentive compatibility (IC) in order for a contract to be feasible. IR implies that a CM will join the block verification and voting when he receives a non-negative utility, i.e.,

$$\theta_g v\left(R_g\right) - cF_g \geq 0, \forall g \in \{1,\cdots,G\}. \tag{6}$$

IC is when a CM of type g, to maximise utility, will only choose the contract (R_g, F_g) over all other contracts (R_{g^-}, F_{g^-}).

$$\theta_g v\left(R_g\right) - cF_g \geq \theta_g v\left(R_{g^-}\right) - cF_{g^-}, \forall g, g^- \in \{1,\cdots,G\}, g \neq g^-. \tag{7}$$

Furthermore, all the rewards that a leader can offer will not exceed $R_{\max}$ which is the transaction fee given by blockchain users for editable transactions on the chain. Thus, we have [18]

$$\sum_{g=1}^{G} |\mathcal{U}|P_g R_g \leq R_{\max}, \forall g \in \{1,\cdots,G\}. \tag{8}$$

According to the constraints given above, the optimization problem can be expressed as

$$\begin{aligned} &\max_{(R_g,F_g)} U_l = \sum_{g=1}^{G}\left(|\mathcal{U}|P_g\right)\left(c^{'}F_g - R_g\right), \\ &\text{s.t.,} \\ &\theta_g v\left(R_g\right) - cF_g \geq 0, \forall g \in \{1,\ldots,G\}, \\ &\theta_g v\left(R_g\right) - cF_g \geq \theta_g v\left(R_{g^-}\right) - cF_{g^-}, \forall g, g^- \in \{1,\cdots,G\}, g \neq g^-, \\ &\sum_{g=1}^{G} |\mathcal{U}|P_g R_g \leq R_{\max}, \forall g \in \{1,\cdots,G\}. \end{aligned} \tag{9}$$

5.2. Optimal Contract for Handling Information Asymmetry. The problem represented equation (9) is not a convex optimization problem. The main difficulty in solving this problem is how to reduce the number of incentive constraints [19]. As the number of IR and IC constraints is N and $N(N-1)$, respectively, we need to simplify the constraints until they are easy to solve. Similar to [18, 20], the number of constraints can only be effectively reduced if the utility function of the CMs satisfies the Spence–Mirrlees property. Luckily, the designed utility function equation (4) satisfies the condition. Thus, equation (9) can be solved with the following steps:

Lemma 1 (Monotonicity Condition). *The incentive R must be monotonically increasing with respect to the type θ of a CM.*

Proof. According to the IC constraint (7), for CMs of type i and type j, where $\theta_i \neq \theta_j$, we can have

$$\begin{aligned} \theta_i v(R_i) - cF_i &\geq \theta_i v\left(R_j\right) - cF_j, \\ \theta_j v\left(R_j\right) - cF_j &\geq \theta_j v(R_i) - cF_i. \end{aligned} \tag{10}$$

Furthermore, we get

$$\left(\theta_i - \theta_j\right)\left[v(R_i) - v\left(R_j\right)\right] \geq 0. \tag{11}$$

Since $(\partial v/\partial R) \geq 0$, whenever $\theta_i > \theta_j$, there must be $R_i \geq R_j$.

Next, we consider three types, i.e., $\theta_{i-1} \leq \theta_i \leq \theta_{i+1}$, and the following constraints which can be called local downward incentive constraints (LDICs).

$$\theta_{i+1} v\left(R_{i+1}\right) - cF_{i+1} \geq \theta_{i+1} v(R_i) - cF_i, \tag{12}$$

$$\theta_i v(R_i) - cF_i \geq \theta_i v\left(R_{i-1}\right) - cF_{i-1}. \tag{13}$$

The equation (13) together with $R_i \geq R_{i-1}$ implies $\theta_{i+1} v(R_i) - cF_i \geq \theta_{i+1} v(R_{i-1}) - cF_{i-1}$. This in turn implies that for type θ_{i+1}, the downward incentive constraint and contract term (R_{i-1}, F_{i-1}) are also satisfied.

$$\theta_{i+1} v\left(R_{i+1}\right) - cF_{i+1} \geq \theta_{i+1} v\left(R_{i-1}\right) - cF_{i-1}. \tag{14}$$

Thus, we can reduce the set of downward incentive constraints to a set of LDICs and the monotonicity condition $R_i \geq R_{i-1}$. It is easy to show that the above approach also holds for the upward incentive constraint set. □

Lemma 2. *LDICs are tight at the optimum point when the monotonicity condition is satisfied.*

Proof. We start by ignoring the set of local upward incentive constraints and concentrate only on the monotonicity of incentive and the set of LDICs. According to the converse method, if the LDIC for some type θ_i is not tight, we have

$$\theta_i v(R_i) - cF_i > \theta_i v\left(R_{i-1}\right) - cF_{i-1}. \tag{15}$$

In this case, the leader can adjust the contract by raising F_i until $\theta_i v(R_i) - cF_i = \theta_i v(R_{i-1}) - cF_{i-1}$.

Based on the above inferences, we can transform equation (9) into

$$\begin{aligned} &\max_{\left(R_g, F_g\right)} U_l = \sum_{g=1}^{G}\left(|\mathcal{U}|P_g\right)\left(c^{'}F_g - R_g\right), \\ &\text{s.t.,} \\ &\theta_1 v(R_1) - cF_1 = 0, \\ &\theta_g v\left(R_g\right) - cF_g = \theta_g v\left(R_{g-1}\right) - cF_{g-1}, \forall g \in \{2, \cdots, G\}, \\ &0 \leq R_1 \leq \cdots \leq R_g \leq \cdots \leq R_G, \\ &\sum_{g=1}^{G} |\mathcal{U}|P_g R_g \leq R_{\max}, \forall g \in \{1, \cdots, G\}. \end{aligned} \tag{16}$$

The standard procedure for solving the equation (16) is to first solve this optimization problem without the monotonicity constraint and then check that the resulting solution satisfies the monotonicity condition [19]. By iterating over the IC and IR constraints, we can obtain

$$F_g = \frac{\left[\theta_1 v(R_1) + \sum_{i=1}^{g} \Delta_i\right]}{c}, \forall g \in \{1, \cdots, G\}. \tag{17}$$

Let $\Delta_i = \theta_i[v(R_i) - v(R_{i-1})]$, $\forall i \in \{2, \cdots, G\}$, $\Delta_1 = 0$. Therefore, equation (16) can be replaced by

$$\begin{aligned} &\max_{R_g, g \in \{1, \cdots, G\}} \sum_{g=1}^{G-1} \left\{ |\mathcal{U}| \frac{c^{'}}{c} v\left(R_g\right)\left[\theta_g \sum_{i=g}^{G} P_i - \theta_{g+1} \sum_{i=g+1}^{G} P_i\right] - |\mathcal{U}|P_g R_g \right\} + |\mathcal{U}| \frac{c^{'}}{c} P_G \theta_G v\left(R_G\right) - |\mathcal{U}|P_G R_G \\ &\text{s.t.,} \\ &\sum_{g=1}^{G} |\mathcal{U}|P_g R_g \leq R_{\max}, \forall g \in \{1, \cdots, G\}. \end{aligned} \tag{18}$$

To solve equation (18), we let $Z_g = |\mathcal{U}|(c^{'}/c) v(R_g)[\theta_g \sum_{i=g}^{G} P_i - \theta_{g+1} \sum_{i=g+1}^{G} P_i] - |\mathcal{U}|P_g R_g$. For each type $\theta_g, g \in \{1, \cdots, G-1\}$, we find an $\widetilde{R_g}$ to maximise the value of Z_g. While for type θ_G, we maximise $|\mathcal{U}|(c^{'}/c) P_G \theta_G v(R_G) - |\mathcal{U}|P_G R_G$ to find $\widetilde{R_G}$. As mentioned before, $(\partial^2 v/\partial R^2) < 0, Z_g$ is a concave function when $|\mathcal{U}|(c^{'}/c)[\theta_g \sum_{i=g}^{G} P_i - \theta_{g+1} \sum_{i=g+1}^{G} P_i] > 0$. Because the sum of concave functions is concave and the constraint is affine,

equation (18) is a convex optimization problem. We assume that the types of CMs obey a uniform distribution so that monotonicity is satisfied [19, 20]. Otherwise, we use the infeasible subsequence substitution algorithm to find the final tuple $(\tilde{R}, \tilde{F})$ [21]. □

5.3. Security against Sybil Attack. A malicious CM may spawn multiple nodes $N = \{n_1, n_2, \ldots, n_q\}$ under his control to participate in validation and voting. He distributes his own votes to these nodes in order to gain lager utility. We can describe the type of CM and the type of these nodes as θ_{g^*} and $\{\theta_{g_1^*}, \ldots, \theta_{g_q^*}\}$ where $\theta_{g^*} = \theta_{g_1^*} + \ldots + \theta_{g_q^*}$.

Theorem 3. *A contract (R_{g^*}, F_{g^*}) according to equation (5) is resistant to Sybil attack.*

Proof. Substituting the left and right sides of the above inequality back into the committee's utility function equation (4), the collation gives

$$\begin{aligned} UC &= U_m(g^*) - \sum_{k=1}^{q} U_m(g_k^*) \\ &= \theta_{g^*} v_{g^*} - \sum_{k=1}^{q} \left(\theta_{g_k^*} v_{g_k^*}\right) - c\left(F_{g^*} - \sum_{k=1}^{q} F_{g_k^*}\right). \end{aligned} \tag{19}$$

For convenience, we abbreviate $v(R_g)$ as v_g. Furthermore, we take equation (17) into equation (19) to get

$$c\left(F_{g^*} - \sum_{k=1}^{q} F_{g_k^*}\right) = \sum_{i=1}^{g^*} \theta_i (v_i - v_{i-1}) - (q-1)\theta_1 v_1 - \sum_{k=1}^{q}\sum_{i=1}^{k} \theta_i (v_i - v_{i-1}). \tag{20}$$

Since $\sum_{i=1}^{g^*} \theta_i (v_i - v_{i-1}) < \sum_{i=1}^{g^*} \theta_i v_i - \sum_{i=1}^{g^*} \theta_{i-1} v_{i-1}$, we have

$$UC > (q-1)\theta_1 v_1 - \sum_{k=1}^{q} \theta_{g_k^*} v_{g_k^*} + \sum_{k=1}^{q}\sum_{i=1}^{k} \theta_i (v_i - v_{i-1}). \tag{21}$$

Since $\sum_{k=1}^{q}\sum_{i=1}^{k} \theta_i (v_i - v_{i-1}) > 0$, a rational CM's UC must be a positive utility when $(q-1)\theta_1 v_1 - \sum_{k=1}^{q} \theta_{g_k^*} v_{g_k^*} > 0$. As a result, we have designed the contract to be well protected against Sybil attack under certain conditions. □

6. Simulation Results

Firstly, this section evaluates the proposed incentive mechanism based on contract theory through simulation. Then, the characteristics of this paper are compared with those of the schemes mentioned in the paper.

All of our experiment is run on desktop with AMD Ryzen 7 5800H with Radeon Graphics 3.20 GHz CPU and 16.0 GB RAM on Windows 10. For comparison purposes, we compare the present incentive mechanism under information asymmetry with another incentive mechanism without information asymmetry, which refers to the leader knowing the specific type of each CM. Obviously, optimal design without information asymmetry is the best result we can achieve.

It is assumed that there are 500 CMs and a leader. The type of each CM follows a uniform distribution. They are classified into 20 different types according to the votes, so the probability of each member being a certain type is 0.05. Parameter $c' = 5$ or $c = 1$. As a contract publisher, a leader generates contract items based on the information that has been obtained and sends them to each CM. Each stakeholder chooses to sign a contract and then acts as voter and verifier to execute the contract. Every CM completes his task honestly will receive a reward from the leader.

6.1. Contract Feasibility. Figures 3(a) and 3(b) show that incentive and resource improve with node type, which reflects the monotonicity of our system. The difference is that the incentive for our contract is a concave function with respect to the node type, whereas the incentive without information asymmetry is a linear function. We can see that under no information asymmetry, when the miner knows the specific type of node, it can obtain higher resources with lower rewards.

The utility of the node with different types ranging from 17 to 19 is presented in Figure 3(c). The results show that utility is only maximised when a node chooses a contract item designed for his type and the utility of node is non-negative. The former accounts for the IC constraint, and the latter verifies the IR constraint.

6.2. Contract Performance. Figure 4 reveals that different types of nodes bring different utilities to miner. The higher the node type, the higher utility it can bring. Figure 4(a) presents that the utility under no information asymmetry is an upper bound on the utility under information symmetry. This is because the miner knows all the information about the node in the former condition. Figure 4(b) displays that the optimization utility of our mechanism is higher than the utility without information asymmetry and that this utility remains zero. The reason for this has already been explained in the previous chart. Thus, the incentive of information asymmetry protects nodes from being over utilized. Figures 4(a) and 4(c) show the same performance that is because the utility is still highest with no information asymmetry, but we strive for some reward for the nodes.

6.3. Comparison of Solutions. In order to better reflect the innovation and necessity of the enhanced redactable POS blockchain solution proposed in this paper, we compare this

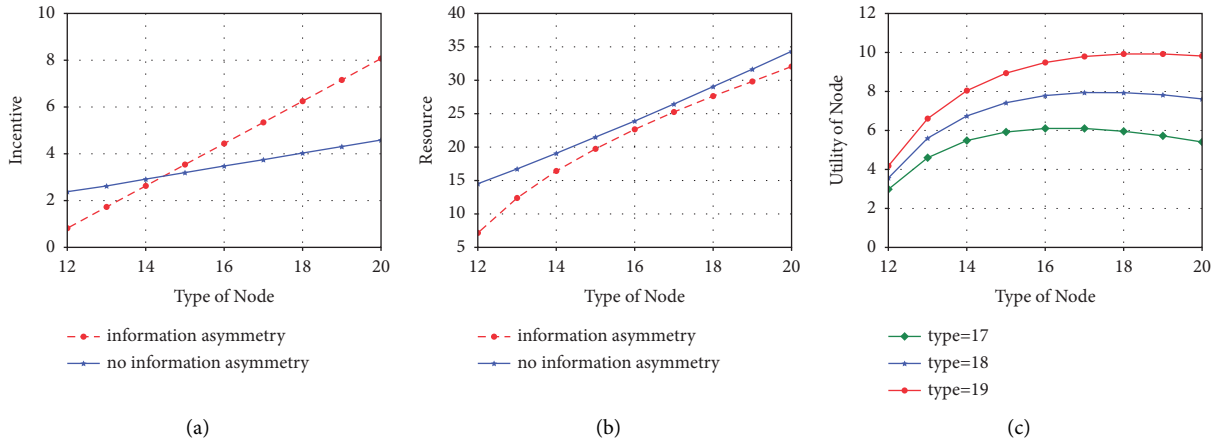

Figure 3: Contract feasibility: (a) incentive, (b) reward, and (c) utility of node.

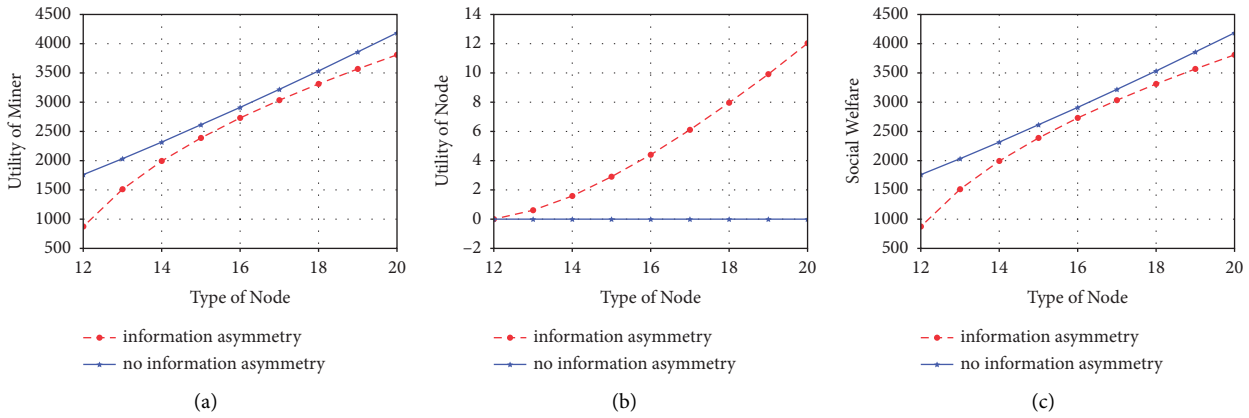

Figure 4: Contract performance of different type node: (a) utility of miner, (b) utility of node, and (c) social welfare.

Table 2: Comparison of editable blockchain solutions.

Features	Works					Ours
	Ateniese et al. EuroS&P′17 [4]	Derler et al. NDSS'19 [11]	Deuber et al. S&P′19 [16]	Xu et al. TIFS'21 [15]	Li et al. TDSC'22 [5]	
Decentralization	✗	✗	✓	✗	✓	✓
Without MPC	✗	✗	✓	✓	✓	✓
Public verifiability	✗	✗	✓	✓	✓	✓
Incentive mechanism	✗	✗	✗	✓	✗	✓

Scheme characteristics: ✓ means fully realized, ✗ means not realized.

paper with the existing research works in terms of the following four features: decentralization, without MPC, public verifiability, and incentive mechanism. The results are shown in Table 2.

As can be seen from the above table, this paper makes an innovative design to add incentives based on the literature [5]. In terms of decentralization and without MPC, existing works [4, 11] and [15] require a central entity for the issuance of editing rights, and some of them also require MPC for trapdoor management, while this paper is a decentralized scheme based on voting to reach consensus. In terms of public verifiability, the disclosure or nondisclosure of the chameleon hash trapdoor determines whether the edited block satisfies public verifiability. Overall, a voting-based editable blockchain solution can achieve decentralization, without MPC, public verifiability, and this paper adds an incentive mechanism to effectively engage enough CMs to honestly participate in verifying and voting on editable blocks. As a result, the research work in this paper further improves the security of the block editing process compared to existing studies.

7. Conclusions

This paper proposes a contract theory-based incentive mechanism on voting-based redactable POS blockchains to deal with the issue of insufficient committee incentives. To

demonstrate the effectiveness of the mechanism, we compare the feasibility and performance with a contract design that does not consider information asymmetry. The experimental results show that the incentive mechanism can effectively attract enough high-stakes CMs to honestly join the validation and voting of editable blocks. In addition, the mechanism can defend against Sybil attack. Therefore, the present incentive for CMs with high stake in the voting-based editing POS blockchain solution is practical, as it allows these members to receive the rewards they deserve. In the future, we will investigate incentive mechanisms with broader incentive coverage so that CMs with lower voting weights can also receive the rewards they deserve.

Data Availability

The related data used to support the findings of this study have been deposited in the incentive-mechanism repository (https://github.com/hippo212/incentive-mechanism).

Conflicts of Interest

The authors declare that they have no conflicts of interest.

Acknowledgments

This work was in part supported by the Guangdong Key R&D Plan 2020 (Grant no. 2020B0101090002), National Natural Science Foundation of China (Grant no. 61932011), Guangdong Basic and Applied Basic Research Foundation (Grant no. 2019B1515120010), Guangdong Key Laboratory of Data Security and Privacy Preserving (Grant no. 2017B030301004), National Key R&D Plan 2020 (Grant no. 2020YFB1005600), National Joint Engineering Research Center of Network Security Detection and Protection Technology (Grant no. 2016B010124009), and Guangdong Provincial Special Funds for Applied Technology Research and Development and Transformation of Important Scientific and Technological Achieve (Grant no. 2017B010124002).

References

[1] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," *Decentralized Business Review*, Article ID 21260, 2008.

[2] J. M. L. Alfonsín, "Argentina: the right to be forgotten," *The Right to Be Forgotten*, pp. 239–248, Springer, Berlin, Germany, 2020.

[3] P. Voigt and A. Von dem Bussche, "The Eu General Data protection Regulation," *A practical guide*, Springer International Publishing, vol. 103152676, pp. 10–5555, New York, NY, USA, 1 edition, 2017.

[4] G. Ateniese, B. Magri, D. Venturi, and E. Andrade, "Redactable blockchain–or–rewriting history in bitcoin and friends," in *Proceedings of the 2017 IEEE European Symposium on Security and Privacy (EuroS&P)*, pp. 111–126, IEEE, Paris, France, April 2017.

[5] X. Li, J. Xu, L Y. Yin et al., "Escaping from Escaping From Consensus: Instantly Redactable Blockchain Protocols in Permissionless Settingonsensus: Instantly Redactable Blockchain Protocols in Permissionless setting," *IEEE Transactions on Dependable and Secure Computing*, pp. 1–20, 2022.

[6] S. Micali, M. Rabin, and S. Vadhan, "Verifiable random functions," in *Proceedings of the 40th Annual Symposium on Foundations of Computer Science*, pp. 120–130, IEEE, New York, NY, USA, October 1999.

[7] G. Rathee, A. Sharma, R. Iqbal, M. Aloqaily, N. Jaglan, and R. Kumar, "A blockchain framework for securing connected and autonomous vehicles," *Sensors*, vol. 19, no. 14, p. 3165, 2019.

[8] G. Rathee, F. Ahmad, N. Jaglan, and C. Konstantinou, "A secure and trusted mechanism for industrial IoT network using blockchain," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 2, pp. 1894–1902, 2023.

[9] R. Krishnamurthy, G. Rathee, and N. Jaglan, "An enhanced security mechanism through blockchain for E-polling/counting process using IoT devices," *Wireless Networks*, vol. 26, no. 4, pp. 2391–2402, 2020.

[10] Y. Cai, G. Fragkos, E. E. Tsiropoulou, and A. Veneris, "A truth-inducing sybil resistant decentralized blockchain oracle," *IEEE*, in *Proceedings of the 2020 2nd conference on blockchain research & applications for innovative networks and services (BRAINS)*, pp. 128–135, Paris, France, September 2020.

[11] D. Derler, S. Kai, and D. Slamanig, "Fine-grained and controlled rewriting in blockchains: chameleon-hashing gone attribute-based," in *Proceedings of the 26th Annual Network and Distributed System Security Symposium (NDSS)*, Diego, CA, USA, February 2019.

[12] Y. Tian, N. Li, Y. Li, P. Szalachowski, and J. Zhou, "Policy-based chameleon hash for blockchain rewriting with black-box accountability," in *Proceedings of the Annual Computer Security Applications Conference*, pp. 813–828, Austin, TX, USA, December 2020.

[13] G. Panwar, R. Vishwanathan, and S. Misra, "Retrace: revocable and traceable blockchain rewrites using attribute-based cryptosystems," in *Proceedings of the 26th ACM Symposium on Access Control Models and Technologies*, pp. 103–114, Spain, June 2021.

[14] Y. Jia, S.-F. Sun, Y. Zhang, Z. Liu, and D. Gu, "Redactable blockchain supporting supervision and self-management," in *Proceedings of the 2021 ACM Asia Conference on Computer and Communications Security*, pp. 844–858, Hong Kong, May 2021.

[15] S. Xu, J. Ning, J. Ma, X. Huang, and R. H. Deng, "K-time modifiable and epoch-based redactable blockchain," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 4507–4520, 2021.

[16] D. Deuber, B. Magri, and S. A. K. Thyagarajan, "Redactable blockchain in the permissionless setting," in *Proceedings of the 2019 IEEE Symposium on Security and Privacy (SP)*, pp. 124–138, IEEE, San Francisco, CA, USA, May 2019.

[17] J. Kang, Z. Xiong, D. Niyato, P. Wang, D. Ye, and D. I. Kim, "Incentivizing consensus propagation in proof-of-stake based consortium blockchain networks," *IEEE Wireless Communications Letters*, vol. 8, no. 1, pp. 157–160, 2019.

[18] J. Kang, Z. Xiong, D. Niyato, D. Ye, D. I. Kim, and J. Zhao, "Toward secure blockchain-enabled internet of vehicles:

optimizing consensus management using reputation and contract theory," *IEEE Transactions on Vehicular Technology*, vol. 68, no. 3, pp. 2906–2920, 2019.

[19] P. Bolton and M. Dewatripont, *Contract Theory*, MIT press, Cambridge, MA, USA, 2004.

[20] Y. Zhang, L. Song, W. Saad, Z. Dawy, and Z. Han, "Contract-based incentive mechanisms for device-to-device communications in cellular networks," *IEEE Journal on Selected Areas in Communications*, vol. 33, no. 10, pp. 2144–2155, 2015.

[21] L. Gao, X. Wang, Y. Xu, and Q. Zhang, "Spectrum trading in cognitive radio networks: a contract-theoretic modeling approach," *IEEE Journal on Selected Areas in Communications*, vol. 29, no. 4, pp. 843–855, 2011.