# *Enhancing the Delegated Proof of Stake consensus mechanism for secure and efficient data storage in the Industrial Internet of Things*

Article

Accepted Version

# Enhancing the Delegated Proof of Stake Consensus Mechanism for Secure and Efficient Data Storage in the Industrial Internet of Things

Wencheng Chen, *Graduate Student Member, IEEE*, Jun Wang, *Senior Member, IEEE*, Jeng-Shyang Pan, *Senior Member, IEEE*, R. Simon Sherratt, *Fellow, IEEE*, and Jin Wang, *Senior Member, IEEE*

***Abstract*—The rapid advancement of Industry 5.0 has accelerated the adoption of the Industrial Internet of Things (IIoT). However, challenges such as data privacy breaches, malicious attacks, and the absence of trustworthy mechanisms continue to hinder its secure and efficient operation. To overcome these issues, this paper proposes an enhanced blockchain-based data storage framework and systematically improves the Delegated Proof of Stake (DPoS) consensus mechanism. A four-party evolutionary game model is developed, involving agent nodes, voting nodes, malicious nodes, and supervisory nodes, to comprehensively analyze the dynamic effects of key factors—including bribery intensity, malicious costs, supervision, and reputation mechanisms—on system stability. Furthermore, novel incentive and punishment strategies are introduced to foster node collaboration and suppress malicious behaviors. The simulation results show that the improved DPoS mechanism achieves significant enhancements across multiple performance dimensions. Under high-load conditions, the system increases transaction throughput by approximately 5%, reduces consensus latency, and maintains stable operation even as the network scale expands. In adversarial scenarios, the double-spending attack success rate decreases to about 2.6%, indicating strengthened security resilience. In addition, the convergence of strategy evolution is notably accelerated, enabling the system to reach cooperative and stable states more efficiently. These results demonstrate that the proposed mechanism effectively improves the efficiency, security, and dynamic stability of IIoT data storage systems, providing strong support for reliable operation in complex industrial environments.**

***Index Terms*—Industrial Internet of Things(IIoT), Blockchain, Data storage, Delegated Proof of Stake (DPoS), Consensus mechanism.**

## I. Introduction

THE rapid development of Industry 5.0 is driving the industrial sector towards higher levels of intelligence, personalization, and human-machine collaboration [1]. As a crucial pillar of Industry 5.0, the Industrial Internet of Things (IIoT) significantly enhances productivity and resource utilization through large-scale device connectivity and data interaction [2]. However, the widespread adoption of IIoT has revealed critical challenges, including inadequate data privacy protection, frequent malicious attacks, and the absence of trust mechanisms [3]. A single point of failure in the traditional centralized IIoT system can result in system paralysis, extensive sensitive data leakage, or data tampering [4]. These issues not only hinder the broader adoption of IIoT technologies but also impede the realization of Industry 5.0's vision.

In recent years, blockchain technology has gained substantial attention from both academia and industry due to its decentralization, data immutability, and traceability features. It is widely regarded as a revolutionary solution to the data security issues in IIoT [5]–[7]. By integrating distributed ledger and smart contracts, blockchain effectively mitigates the security risks of centralized architectures and offers a transparent, efficient, and trustworthy data storage environment for IIoT systems [8]. Despite its potential, the application of blockchain in IIoT faces several challenges, including low consensus efficiency, complex interactions among nodes, and the threat posed by malicious nodes [9], [10]. Specifically, the widely used Delegated Proof of Stake (DPoS) consensus algorithm is prone to inefficiencies and security risks, such as bribery-induced vote manipulation and attacks from malicious nodes [11]. These challenges compromise the fairness and security of blockchain systems, posing significant obstacles to their large-scale deployment in IIoT scenarios.

To address these challenges, this paper presents an innovative optimization framework based on a four-party evolutionary game model, which comprehensively considers the interactions among agent nodes, voting nodes, malicious nodes, and supervisory nodes. Unlike traditional two-party or three-party game models, the four-party model simulates multi-agent behavior in real-world applications, providing deeper insights into the dynamic impacts of strategic choices on system stability. Furthermore, this study examines the effects of key factors such as bribery intensity, costs associated with malicious behavior, reputation value, and punitive measures on system performance. By exploring the evolutionary dynamics of malicious node behavior, this research enriches the theoretical framework of blockchain game theory and provides practical guidance for optimizing the DPoS consensus mechanism. The primary contributions of this paper are as follows:

(i) A blockchain-based IIoT data storage framework is proposed, integrating a game model to analyze node interactions and their impact on system stability and efficiency.

(ii) The impact of bribery intensity, punishment mecha-

This work was supported in part by the Natural Science Foundation of China under Grant No. 6247314 and No. U25A20426, the Industry-Academia Collaboration Program of Fujian Universities under Grant No. 2024H6026, the Fujian Province Special Funding Projects for Promoting High-Quality Development of Marine and Fishery Industry under Grant No. FJHYF ZH-2023-06, and the Key Project of Natural Science Foundation of Hunan Province under Grant No. 2024JJ3017. (Corresponding author: Jin Wang).

Wencheng Chen and Jun Wang are with the College of Electrical Engineering and Automation, Fuzhou University, Fuzhou 350116, China (e-mail: 220110006@fzu.edu.cn; wangjun_online@hotmail.com).

Jeng-Shyang Pan is with the School of Artificial Intelligence, Nanjing University of Information Science & Technology, Nanjing 210000, China (e-mail: jspan@ieee.org).

R. Simon Sherratt is with the School of Biomedical Engineering, the University of Reading, RG6 6AY, United Kingdom (e-mail: sherratt@ieee.org).

Jin Wang is with the Sanya Institute of Hunan University of Science & Technology, Sanya 572024, China (e-mail: jinwang@hnust.edu.cn).

nisms, and reputation mechanisms on the system's evolutionary stability is systematically analyzed.

(iii) A comparative analysis with two-party and three-party game models demonstrates the proposed model's superiority in accelerating strategy convergence and enhancing system stability.

(iv) Building on the research findings, policy recommendations are proposed to optimize the DPoS consensus mechanism, strengthening blockchain's secure storage capabilities in IIoT and offering guidance for complex application scenarios.

The rest of the paper is organized as follows: Section II reviews related work. Section III analyzes the core challenges of IIoT and proposes a blockchain-based storage framework. Section IV details the proposed four-party evolutionary game model. Section V presents simulation and comparative analysis. Section VI discusses the research results and outlines future research directions. Section VII concludes the paper.

## II. Related Works

### A. Blockchain Integration with IIoT

As a subset of IoT, IIoT promotes industrial transformation through data interaction among smart devices [12], enhancing efficiency and reducing costs. However, traditional centralized architectures struggle with privacy risks, single points of failure, and weak security. Blockchain, with its decentralized, tamperproof, and traceable features, offers a promising solution for secure IIoT data management.

In recent years, blockchain applications in IIoT have attracted widespread attention across various domains. For example, in supply chain management, Dutta et al. [13] proposed a blockchain-based parametric transportation insurance to improve efficiency and transparency. In smart manufacturing, Lin et al. [14] developed a blockchain-enabled knowledge sharing platform to safeguard private knowledge while supporting edge intelligence. In the energy sector, Abegaz et al. [15] designed a blockchain-based resource transaction framework with deep reinforcement learning to ensure security and privacy. In the context of smart cities, Wang et al. [16] introduced a blockchain-based electronic toll collection system to reduce evasion and enhance transparency.

Blockchain technology offers innovative solutions for IIoT, yet faces two key challenges in practical applications: efficiency bottlenecks and security risks. The consensus mechanism, as the core of blockchain, directly impacts system security, scalability, and decentralization. Specifically, the DPoS mechanism encounters issues like node strategy conflicts and vulnerabilities to malicious attacks, affecting both consensus efficiency and blockchain's industrial applicability. Thus, exploring the evolution and dynamic optimization of node behaviors is crucial for both theoretical and practical advancements.

### B. Application of Game Theory in Blockchain DPoS Consensus Mechanism

Game theory serves as a powerful tool for analyzing the behavior of blockchain nodes, particularly in the design of incentive structures, the distribution of benefits, and the defense against attacks within consensus mechanisms. This approach plays a pivotal role in enhancing system efficiency and security. Recent studies have therefore explored the DPoS consensus mechanism through the lens of game theory.

From the perspective of incentive and efficiency optimization, Wang et al. [17] developed a DPoS consensus mechanism based on the Stackelberg game, leveraging a reputation model to enhance the utility and efficiency of validation nodes. Focusing on behavioral supervision, Ren et al. [18] proposed a monitoring mechanism with a reward–punishment system and constructed a three-party evolutionary game model involving agent nodes, voting nodes, and supervisory nodes to analyze strategic changes before and after consensus scheme improvements. In terms of energy efficiency, Liu et al. [19] formulated a cooperative game model that balances the interests of block nodes and the system, achieving dual optimization through Nash equilibrium.

Overall, existing research on the DPoS consensus mechanism often employs two- or three-party game models, which cannot fully capture the complexity of real-world applications and the dynamic interactions among multiple stakeholders. Malicious actors can severely compromise system security and stability. Therefore, the introduction of a multi-party game model is essential to better represent these interactions and further optimize the DPoS consensus mechanism.

### C. Research on Preferential Delegated Proof of Stake (PDPoS)

To address the shortcomings of traditional DPoS in terms of fairness in node selection, decentralization tendencies, and resistance to attacks, many scholars proposed improved mechanisms based on the concept of priority delegation. In terms of PDPoS mechanisms optimized for reputation, Wang et al. [20] quantified node battery levels, computational resources, and trust levels to construct a multi-dimensional reputation score, granting nodes with higher reputation a higher priority for selection as validators. Zhu et al. [21] introduced a reputation adjustment factor to modify voting weights, making it easier for high-reputation nodes to be selected into the candidate miner set. Li et al. [11] calculated base station reputation values based on historical performance, enabling high-reputation base stations to prioritize becoming core nodes in the blockchain for block production and validation. In terms of PDPoS mechanisms based on weight and voting optimization, You et al. [22] improved the fuzzy set conversion formula to allocate voting weights, enhancing the influence of high-weight nodes in the consensus process. Lin et al. [23] employed the SP-DEWOA algorithm to optimize witness node elections, making the results more consistent with the preference rankings of the majority of stakeholders.

In existing PDPoS studies, incentive, punishment, and reputation mechanisms are typically designed as independent components. Reputation mainly serves for node prioritization or voting-weight adjustment and does not interact with bribery incentives, behavioral deviations, or reputation backlash. Furthermore, malicious nodes are often treated as exogenous

disturbances without strategic evolution, limiting the ability to capture dynamic coupling among malicious behavior, supervisory strength, and incentives. These characteristics hinder PDPoS models from characterizing stability evolution under multi-mechanism coupling in complex IIoT scenarios.

### D. Study of Malicious Nodes in DPoS Consensus Mechanism

Malicious nodes pose severe threats to the security and stability of the DPoS consensus mechanism. As blockchain technology evolves, mitigating their impact has become a central research focus, with existing studies exploring diverse defense strategies such as voting optimization, credit scoring, and enhanced consensus protocols.

To address these challenges, scholars have proposed a series of methods with increasing sophistication. Xu et al. [24] first improved the voting process by designing a fuzzy set-based method to enhance fairness and efficiency, thereby reducing the likelihood of malicious nodes being elected. Building on system-level security, Wang et al. [25] introduced a credit scoring and malicious behavior disclosure mechanism in a blockchain-based carpooling scheme to strengthen reliability. To further resist sophisticated attacks, Li et al. [26] developed an enhanced DPoS algorithm resistant to long-range attacks, which addressed centralization risks through node sharding and reporting mechanisms for witness nodes. Extending to intelligent detection, Misic et al. [27] proposed a DL-DPoS mechanism that employs credit scoring and responsibility reassignment to identify and manage malicious nodes effectively.

Most defense strategies rely on single-dimensional penalties or isolation and lack mechanisms that link malicious behavior with reputation recovery or compliance incentives. Malicious nodes are rarely incorporated as strategic agents in a multi-party evolutionary framework, resulting in insufficient representation of mechanism coupling and cross-party feedback effects.

### E. Comparative Analysis of Existing Methods

To systematically review the advances and limitations of optimization studies on DPoS and PDPoS consensus mechanisms, this paper presents a comparative analysis of representative methods, as summarized in Table I.

The existing methods suffer from three main shortcomings: the game models are oversimplified and fail to systematically capture malicious behaviors; most mechanisms are static and cannot adapt to dynamic strategy evolution; and incentive, punishment, and reputation schemes are often studied in isolation without coordinated optimization. To overcome these limitations, this paper proposes a four-party evolutionary game model involving agent nodes, voting nodes, malicious nodes, and supervisory nodes. It integrates incentive, punishment, and reputation mechanisms that dynamically adjust to evolving strategies, and employs replicator dynamics to quantify strategy evolution, thereby offering a more practical foundation for enhancing the security and efficiency of DPoS in IIoT scenarios.

## III. Core Challenges of IIoT and Blockchain Storage Framework

### A. Core Challenges of the IIoT

The rapid development of Industry 5.0 has brought about transformative technological advancements, establishing intelligent production systems where humans and machines collaborate as the new standard in the industrial sector [1]. However, this intelligent transformation is inevitably accompanied by significant challenges related to data security and system reliability, as illustrated in Figure 1.

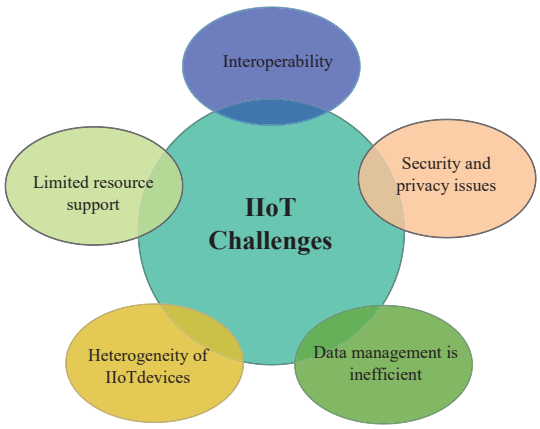


Fig. 1. IIoT challenges

First, the lack of trust remains a core issue hindering the advancement of IIoT. IIoT systems require seamless sharing of critical data across multiple devices and organizations, but the absence of a robust trust mechanism often results in risks of data leakage or misuse. This not only compromises data authenticity but also reduces the efficiency of inter-organizational collaboration.

Second, the risk of data tampering adds complexity to industrial operations. If an attacker manipulates critical parameters or production data, it can disrupt industrial processes and potentially trigger serious security incidents.

Moreover, the limitations of centralized storage present a major bottleneck for current systems. A single point of failure can compromise the entire network, and centralized server-based models lack the resilience needed to adapt to dynamic network changes. Additionally, interoperability issues among IIoT devices from different vendors and protocols create data silos, thereby restricting broader adoption.

Lastly, the challenge of balancing data privacy and sharing remains unresolved. Industrial data often contains sensitive information, and traditional data-sharing mechanisms lack comprehensive consideration of privacy and compliance, limiting system efficiency.

Addressing these challenges requires designing an innovative technological framework that ensures data security, system reliability, and efficient sharing—a critical step toward the comprehensive upgrade of IIoT.

### B. Blockchain-based IIoT Data Storage Framework

*1) Storage framework:* To address the core challenges faced by IIoT, this paper proposes a blockchain-based data storage

TABLE I
COMPARATIVE ANALYSIS OF REPRESENTATIVE STUDIES ON DPOS AND PDPOS OPTIMIZATION

| Research focus | Representative literature | Research objects / game model | Malicious nodes considered | Core mechanism | Main advantages | Main limitations | Relevance to this work |
|---|---|---|---|---|---|---|---|
| Incentive mechanism | Wang et al. [17] | Validator nodes; Stackelberg game based on reputation | No | Reputation + incentive mechanism | Optimizes validator utility and efficiency | Mechanisms analyzed independently; no dynamic co-evolution; no malicious-node interaction | Extended to four-party dynamic game with coupled mechanisms and malicious-node strategies |
| Behavioral strategy | Ren et al. [18] | Delegate/voter/supervisor nodes; three-party evolutionary game | No | Incentive + punishment mechanism | Constructs a three-party interaction model, clarifying reward–punishment constraints | No malicious nodes; no multi-mechanism coupling | Adds malicious-node evolution and incentive–punishment–reputation coupling |
| Reputation mechanism (PDPoS) | Zhu et al. [21] | Node reputation and voting weights; preferential delegation | No | Reputation adjustment factor modifies voting weights | High-reputation nodes are more likely to be selected, improving fairness and reliability | Static reputation; no penalty integration; no stability analysis | Couples reputation loss with penalties within replicator dynamics |
| Weight Optimization (PDPoS) | You et al. [22] | Node voting weights; fuzzy set optimization | No | Improved voting weight allocation formula | Enhances the influence of high-weight nodes in consensus | Ignores bribery and malicious behavior; isolated mechanisms | Integrates weight and incentives into dynamic evolutionary framework |
| Voting Optimization (PDPoS) | Lin et al. [23] | Witness node election; SP-DEWOA algorithm | No | Preference-consistency optimization | Improves alignment of election outcomes with stakeholder preferences | No dynamic defense; no mechanism coupling | Introduces malicious-node dynamics and cross-mechanism interaction |
| Malicious node defense | Li et al. [26] | Witness/malicious nodes; enhanced DPoS | Yes | Sharding + reporting mechanism | Resists long-range attacks, reduces centralization risk | Penalty static; no four-party evolution | Includes dynamic supervisory cost–benefit balance |
| Integrated mechanism | Misic et al. [27] | Multiple nodes; credit scoring and liability redistribution | Yes | Credit and responsibility redistribution | Strengthens system security | No dynamic coupling; penalty not adaptive | Uses adaptive penalty in coupled evolutionary system |
| This work | | agent/voter/malicious/ supervisor nodes; four-party evolutionary game | Yes | Dynamic incentives + dynamic penalties + reputation mechanism | High integrity of participants, dynamic mechanism coupling, quantified evolutionary path, accelerated convergence | Higher model complexity, requires parameter calibration | Provides fundamentally new equilibrium and stability via fully coupled dynamic mechanisms |

framework that leverages the DPoS consensus mechanism as its core and integrates distributed storage and smart contracts to ensure data security, reliability, and efficient sharing.

As shown in Figure 2, the proposed framework integrates a distributed ledger, smart contracts, and the DPoS consensus mechanism to achieve secure data storage and efficient management through the following functional modules:

Data Collection and Encryption: Sensors and devices in IIoT collect multidimensional data (e.g., temperature, humidity, pressure, energy consumption, etc.) in real time. After data collection, the raw data is encrypted, and a unique data identifier is generated using a hash algorithm to ensure data integrity and prevent tampering.

Data Block Construction and Signature: The encrypted data and its corresponding hash value are encapsulated into a data block. Each block contains a timestamp, device identifier, hash value of the data content, and a digital signature. The device uses its private key to sign the data block, enhancing trustworthiness and traceability.

Data Broadcasting and Validation: Data blocks are broadcast to distributed nodes through the blockchain network. Under the DPoS consensus mechanism, agent nodes validate the

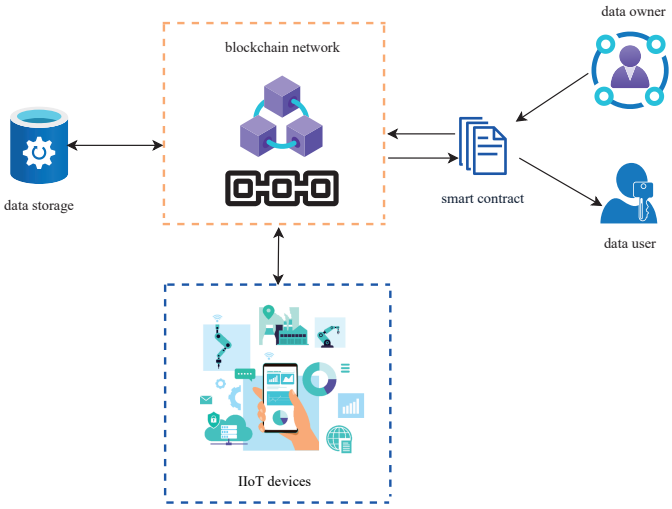


Fig. 2. Blockchain-based IIoT data storage framework

data blocks by checking their signatures and data integrity. This verification process is efficient and mitigates the risks associated with centralization.

DPoS Consensus mechanism and Block Generation: The DPoS consensus mechanism elects a set of agent nodes through voting. These nodes reach consensus on the data block and generate a new block. The agent nodes verify the legitimacy of the data block and record it onto the blockchain, ensuring secure and consistent distributed data storage. Reward tokens are issued to the block-generating nodes, incentivizing active participation.

Smart Contract Driven Data Sharing: During data storage, smart contracts define strict access rules and conditions. For instance, data requestors must meet specific permissions to access sensitive information. When conditions are satisfied, the smart contract automatically verifies identity and permissions, authorizing access to ensure secure and efficient data sharing.

Data Access and Feedback: Data owners dynamically manage access requests through smart contracts. These contracts not only execute permission verification, but also adjust access conditions based on the behavior and authority of the requesting party, ensuring compliance and data usage security.

*2) Technical Advantages of the Framework:* Decentralization Enhances Reliability: By utilizing the DPoS consensus mechanism and distributed storage architecture, the framework eliminates the risk of single-point failure in traditional centralized storage, significantly enhancing system reliability.

Efficient Consensus Mechanism: The low latency and high throughput of the DPoS consensus mechanism enable the blockchain to handle large-scale IIoT data storage requirements while maintaining low energy consumption.

Anti-tampering and Traceability: The combination of data hash values, digital signatures, and distributed ledgers ensures data integrity, anti-tampering capabilities, and traceability, providing robust security for industrial applications.

Smart Contracts Optimize Data Sharing: The automated execution of smart contracts improves data-sharing efficiency and protects sensitive data privacy through strict access control rules.

Flexibility and Scalability: The framework is adaptable to various IIoT application scenarios, including smart manufacturing, supply chain management, energy monitoring, and other fields, supporting in-depth applications across multiple industries.

## IV. Modeling of the Four-Party Game

Although blockchain technology has been widely adopted in IIoT, its core consensus mechanism continues to face dual challenges of security and efficiency. Under the DPoS consensus mechanism, the presence of malicious nodes not only threatens system security but also jeopardizes the fairness and effectiveness of the consensus process through methods such as bribery. Therefore, this section focuses on the DpoS consensus mechanism and introduces a four-party game model based on evolutionary game theory. The objective is to quantify and optimize the behavioral strategy choices among agent nodes, voting nodes, malicious nodes, and supervisory nodes.

### A. Description of the Game Problem

In the DPoS consensus mechanism, different types of nodes interact with one another through complex strategies that influence consensus efficiency and system security:

Agent Nodes: To secure more votes, an agent node may enhance its likelihood of being selected as a representative node through either legitimate or illegitimate means (e.g., bribing voting nodes).

Voting Nodes: Voting nodes decide to support specific agent nodes based on their own interests and may accept bribes or engage in malicious activities.

Malicious Nodes: Malicious nodes seek to attack other nodes or manipulate data to gain undue advantages, disrupting the normal functioning of the system.

Supervisory Nodes: Supervisory nodes are tasked with monitoring system behavior and maintaining network security by punishing bribery or malicious actions; however, these supervisory activities incur costs.

The behavioral strategies adopted by these subjects directly impact the stability and consensus efficiency of the system. To analyze these interactions, this paper constructs a four-party game model, as illustrated in Figure 3, to depict the dynamic relationships among the participants.

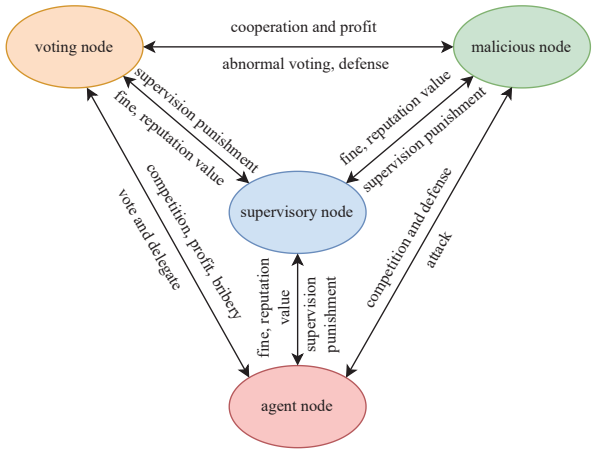


Fig. 3. Subject game relationships

### B. Underlying Assumptions

In the DPoS consensus mechanism, the behavioral decisions of participating subjects are diverse and complex. Interactions and strategic games occur between agent nodes, voting nodes, malicious nodes, and supervisory nodes. These interactions influence not only the system's consensus efficiency but also its security and stability. Due to the real-time nature of data circulation and the system's scale complexity in IIoT scenarios, agents cannot make fully rational decisions. Instead, they optimize their gains and adjust strategies based on limited information. This bounded rationality aligns with the assumptions of evolutionary game theory, providing a theoretical foundation for studying the dynamic evolution of node behavior.

To construct a game model, analyze the stability of equilibrium points for each party's strategy, and evaluate the impact

of various factors on participants' benefits, this paper builds upon the fundamentals of the DPoS consensus mechanism [28], the theoretical framework of evolutionary game theory [29], and insights from prior studies [18], [30]. By considering key factors influencing the strategic choices of agent nodes, voting nodes, malicious nodes, and supervisory nodes, the following assumptions are proposed. These assumptions aim to explore the impact of strategy evolution on system stability and efficiency, providing theoretical support for optimizing the DPoS consensus mechanism.

(1) Bounded Rationality and Evolutionary Strategy Optimization: Evolutionary game theory posits that participants are not fully rational in decision-making but gradually adjust their behavior based on limited information to optimize gains. In the complex IIoT environment, agent nodes, voting nodes, malicious nodes, and supervisory nodes adopt an evolutionary strategy optimization process. This assumption underpins the evolutionary game models commonly used to analyze dynamic interactions in complex systems.

(2) Competitive Behavior of Agent Nodes: In the DPoS consensus mechanism, agent nodes aim to maximize their chances of being selected as representative nodes by securing more votes. These nodes perform critical tasks such as verifying transactions, generating blocks, and maintaining blockchain network functionality. However, due to intense competition, agent nodes may resort to illegal means (e.g., bribing voting nodes) to improve their election prospects. Malicious nodes may further exacerbate this competition by colluding with agent nodes to manipulate election outcomes.

For the agent node, obtaining the block bookkeeping right through normal voting and completing the block generation task is profitable as $P_1$, obtaining the block bookkeeping right through bribing the voting node requires bribery cost $C_1$, and the bribery strength is $a_1$; and obtaining the block bookkeeping right through bribing the malicious node requires bribery cost $C_2$, and the bribery strength is $a_2$. Bribing the voting node is successful and profitable $P_2$, and bribing the malicious node is successful and profitable $P_3$. In the case of regulation by supervisory nodes, both bribery behavior and bribery intention of agent nodes will be punished with fines $F_1$, $F_2$, and reputation loss $L_1$, $L_2$; in case of non-supervisory by supervisory nodes, agent nodes collude to profit $P_2$, $P_3$.

(3) Economic Interests of Voting Nodes: Voting nodes play a pivotal role in the DPoS consensus mechanism, with their voting behavior directly influencing the selection of agent nodes. Typically, voting nodes allocate votes based on the contributions and reputation of agent nodes. However, economic incentives may drive voting nodes to accept bribes from agent or malicious nodes, leading to abnormal voting behavior. Such actions undermine blockchain fairness and could allow unqualified nodes to gain representation, threatening system security. The costs (e.g., computational overhead) and potential benefits associated with voting also significantly influence voting nodes' decisions.

When malevolent nodes operate evilly, voting nodes' normal voting profits $P_4$, bribed participation in voting earnings $P_5$, abnormal voting profits $P_6$, and voting nodes' voting expenses are all $C_3$. Voting nodes that accept agent nodes' bribed voting behaviors will be penalized with fines $F_3$ and reputational losses $L_3$; voting nodes that accept malicious nodes' bribes in voting behaviors will be penalized with fines $F_4$ and reputational losses $L_4$; and voting nodes that do not have supervisory nodes monitoring will benefit from bribed voting $P_5$ and $P_6$.

(4) Strategies and Impact of Malicious Nodes: Malicious nodes pose a significant threat to the DPoS consensus mechanism, interfering with the consensus process through various means, such as network attacks, data manipulation, or bribery. These nodes may target agent and voting nodes, influencing the election process through coercion or bribery. The behavior of malicious nodes is constrained by costs and benefits, such as resource consumption for attacks or penalties for detected violations. Understanding the strategies of malicious nodes and their systemic impact is crucial for improving security.

For the malicious node, the malicious node profits $P_7$ when it acts maliciously against the agent node, which requires evil cost $C_4$ and evil intensity $m_1$; the malicious node profits $P_8$ when it acts maliciously against the voting node, which requires evil cost $C_5$ and evil intensity $m_2$; and its profits by adopting the cooperative strategy $P_9$. In the case of supervision by the supervisory node, the malicious node's evil behavior and evil intention will be punished by the fines $F_5$, $F_6$, and reputation loss $L_5$, $L_6$; when the supervisory node does not supervise, the malicious node profits $P_7$, $P_8$. reputation loss $L_5$, $L_6$; when the supervisory node does not supervise, the malicious node profits from doing evil $P_7$, $P_8$.

(5) Cost-Benefit Trade-Off for Supervisory Nodes: Supervisory nodes monitor and penalize improper behavior in the DPoS mechanism, ensuring system functionality and maintaining blockchain network security. However, regulatory actions involve a trade-off between benefits and costs. Excessive supervision may increase system burden, while insufficient supervision could permit malicious behavior. Supervisory nodes derive benefits from penalizing violations but face supervisory costs (e.g., data analysis and decision-making overhead), which may limit their efforts. Inactive supervisory nodes risk reputational damage or external penalties for tolerating bribery or malicious behavior.

For the supervisory node, the cost of supervision is $C_6$, the profit of supervision is $P_{10}$, and the supervisory node profits $F_1$, $F_2$, $F_3$, $F_4$, $F_5$, $F_6$ when it discovers bribery, passive bribery and malpractice; $b$ is the penalty for the inaction of the supervisory node, and the supervisory node is not supervised by a fine of $F_7$ when it fails to supervise bribery, passive bribery and malpractice and a fine of $bF_7$ when it turns a blind eye to bribery, passive bribery, and malpractice. $bF_7$ is the penalty for failure to supervise. Profit $P_{11}$ when not supervised.

Based on the above assumptions, the strategy set of each agent is as follows:

The four parties of the game are agent nodes, voting nodes, malicious nodes, and supervisory nodes. And all four subjects are finite rationality. The strategy set $A = \{non\text{-}briberyA_1, briberyA_2\}$ of agent nodes, the strategy set $V = \{normal\ voting\ V_1,\ abnormal\ votingV_2\}$ of voting nodes, the strategy set $M = \{cooperateM_1, doevilM_2\}$ of malicious nodes, and

TABLE II
SYMBOL SETTING AND MEANING OF FOUR-PARTY GAME MODELS

| Symbol | Implication | Symbol | Implication |
|---|---|---|---|
| $A_1$ | Agent nodes adopt a non-bribery strategy | $P_9$ | Malicious nodes profit from cooperative strategies |
| $A_2$ | Agent nodes adopt a bribery strategy | $P_{10}$ | Supervisory nodes supervisory profitability |
| $V_1$ | Voting nodes adopt a normal voting strategy | $C_1$ | Bribery cost of bribing voting nodes by agent nodes |
| $V_2$ | Voting nodes adopt abnormal voting strategies | $P_{11}$ | Profit when supervisory nodes are non-supervisory |
| $M_1$ | Malicious nodes adopt cooperative strategies | $C_2$ | Cost of bribing malicious nodes by agent nodes |
| $M_2$ | Malicious nodes adopt evil strategy | $C_3$ | Voting node voting costs |
| $S_1$ | Supervisory nodes adopt supervisory strategies | $C_4$ | Cost of malicious node's evil against agent node |
| $S_2$ | Supervisory nodes adopt a non-supervisory strategy | $C_5$ | Cost of malicious node's evil against voting node |
| $P_1$ | Agent nodes gain block bookkeeping rights through normal voting and profit from completing block-generation tasks | $C_6$ | Supervisory nodes supervisory costs |
| $P_2$ | Agent nodes successfully bribe voting nodes for profits | $F_1$ | Bribery fines for agent nodes |
| $a_1$ | Bribery strength of agent nodes to bribe voting nodes | $F_2$ | Intent to bribe fines for agent nodes |
| $a_2$ | Bribery effort of agent nodes to bribe malicious nodes | $F_3$ | Fine for voting nodes accepting bribes from agent nodes for voting behavior |
| $m_1$ | Evil strength when malicious nodes behave maliciously towards agent nodes | $F_4$ | Voting nodes accepting bribes from malicious nodes for malicious behavior voting behavior fines |
| $m_2$ | Evil strength when malicious nodes behave maliciously towards voting nodes | $F_5$ | Fines for malicious node misdeeds |
| $P_8$ | Malicious nodes profit when they behave maliciously towards voting nodes | $F_6$ | Malicious nodes with evil intent fine |
| $bF_7$ | Fines for turning a blind eye to bribery, passive bribery and nefarious acts | $F_7$ | Failure of supervisory nodes to supervise fines for bribery, passive bribery and misdemeanors |
| $P_3$ | Agent nodes successfully bribe malicious nodes for profit | $L_1$ | Loss of reputation for bribery of agent nodes |
| $P_4$ | Voting nodes profit from normal voting | $L_2$ | Loss of reputation of agent node for intent to bribe |
| $P_5$ | Voting nodes are bribed to participate in voting for profit | $L_3$ | Voting nodes accept bribes from agent nodes for voting behavior reputation loss |
| $P_6$ | Voting nodes are abnormally involved in voting for profit | $L_4$ | Voting nodes accept bribes from malicious nodes for malicious behavior Voting behavior reputation loss |
| $P_7$ | Malicious nodes profit when they behave maliciously towards agent nodes | $L_5$ | Reputational damage from malicious node misdeeds |
| $b$ | Penalties for inaction at supervisory nodes | $L_6$ | Reputational damage from malicious nodes with evil intent |
| $x$ | Probability of the agent node to choose the bribery strategy | $E_{V2}$ | Expected revenue of voting nodes selecting an anomalous voting strategy. |
| $y$ | Probability of voting nodes selecting a normal voting strategy | $\overline{E_V}$ | Average expected revenue from voting node strategy selection |
| $m$ | Probability of malicious nodes choosing a cooperative strategy | $E_{M1}$ | Expected revenue from malicious node selection cooperation strategies |
| $z$ | Probability of supervisory node selection of supervisory strategy | $E_{M2}$ | Expected revenue of malicious nodes choosing an evil strategy. |
| $E_{A1}$ | Expected revenue when selecting agent nodes for non-bribery strategies | $\overline{E_M}$ | Average expected revenue from malicious node strategy selection |
| $E_{A2}$ | Expected revenue from agent node selection bribery strategy | $E_{S1}$ | Expected revenue of supervisory nodes choosing a supervisory strategy. |
| $\overline{E_A}$ | Average expected revenue from agent node strategy selection | $E_{S2}$ | Expected revenue of supervisory nodes choosing a non-supervisory strategy. |
| $E_{V1}$ | Expected revenue of voting node selection normal voting strategy | $\overline{E_S}$ | Average expected revenue of supervisory nodes' strategy selection. |

the strategy set $S = \{supervisoryS_1, non\text{-}supervisoryS_2\}$ of supervisory nodes.

Based on the above analysis, the symbol settings and their meanings in this section are shown in Table II.

### C. Benefits Matrix Construction

In the four-party evolutionary game model, the four parties make strategic choices according to their wishes. Suppose the probability of the agent node to choose the bribery strategy is $x$, $x \in [0,1]$, and the probability of the non-bribery strategy is $1-x$; The probability that a voting node selects a normal voting strategy is $y$, $y \in [0,1]$, and the probability of an abnormal voting strategy is $1-y$; The probability that the malicious node chooses the cooperation strategy is $m$, $m \in [0,1]$, and The probability of the evil strategy is $1-m$; the probability of the supervisory node to choose the supervisory strategy is $z$, $z \in [0,1]$, and the probability of the non-supervisory strategy is $1-z$. Based on the above assumptions and analysis, the four-party game benefit matrix of the DPoS consensus mechanism can be obtained as shown in Table III.

### D. Four-party Evolutionary Game Model Analysis

Through the four-party game revenue matrix [31] and related analysis, it is evident that the expected revenue for an agent node choosing the non-bribery strategy during the game is:

$$\begin{aligned} E_{A1} = {} & zmyP_1 + zm(1-y)P_1 + z(1-m)yP_1 \\ & + z(1-m)(1-y)P_1 + (1-z)myP_1 \\ & + (1-z)m(1-y)P_1 + (1-z)(1-m)yP_1 \\ & + (1-z)(1-m)(1-y)P_1 \end{aligned} \tag{1}$$

The expected revenue for an agent node adopting a bribery strategy is:

$$E_{A2} = zmy(P_1 - a_1C_1 - a_2C_2 - a_1F_1 - a_1L_1$$

TABLE III
THE PAYOFF MATRIX FOR THE FOUR-PARTY EVOLUTIONARY GAME

| | | | Agent Node, Voting Node | | | |
|---|---|---|---|---|---|---|
| | | | Non-bribery $x$ | | Bribery $1-x$ | |
| | | | Normal voting $y$ | Abnormal voting $1-y$ | Normal voting $y$ | Abnormal voting $1-y$ |
| Supervisory nodes, Malicious nodes | Supervisory $z$ | Cooperative $m$ | $P_{10}-C_6$<br>$P_9$ | $P_{10}-C_6+F_3+F_4$<br>$P_9$ | $P_{10}-C_6+a_1F_1+a_2F_2$<br>$P_9$ | $P_{10}-C_6+a_1F_1+F_3$<br>$P_9$ |
| | | | $P_1$ | $P_1$ | $P_1-a_1C_1-a_2C_2$<br>$-a_1F_1-a_1L_1-$<br>$a_2F_2-a_2L_2$ | $a_1P_2-a_1C_1-$<br>$a_1F_1-a_1L_1$ |
| | | | $P_4-C_3$ | $P_4-F_3-F_4-$<br>$L_3-L_4-2C_3$ | $P_4-C_3$ | $P_5-C_3-F_3-L_3$ |
| | | Evil $m$ | $P_{10}-C_6+m_1F_5$<br>$+m_2$ | $P_{10}-C_6+F_4$<br>$+m_2F_6$ | $P_{10}-C_6+m_1F_5$<br>$+a_2F_2$ | $P_{10}-C_6+m_1F_5$<br>$+m_2F_6+a_1F_1+$<br>$a_2F_2+F_3+F_4$ |
| | | | $P_7-m_1C_4-m_2C_5$<br>$-m_1F_5-m_2F_6-$<br>$m_1L_5-m_2L_6$ | $m_2P_8-m_2C_5-$<br>$m_2F_6-m_2L_6$ | $m_1P_7-m_1C_4$<br>$-m_1F_5-m_1L_5$ | $m_1P_7-m_1C_4+m_2P_8$<br>$-m_2C_5-m_1F_5-$<br>$m_1L_5-m_2F_6-m_2L_6$ |
| | | | $P_1$ | $P_1$ | $a_2P_3-a_2C_2$<br>$-a_2F_2-a_2L_2$ | $a_1P_2-a_1C_1+a_2P_3$<br>$-a_2C_2-a_1F_1-$<br>$a_1L_1-a_2F_2-a_2L_2$ |
| | | | $P_4-C_3$ | $P_6-C_3-F_4$<br>$-L_4$ | $P_4-C_3$ | $P_5+P_6$<br>$-2C_3-F_3$<br>$-F_4-L_3-L_4$ |
| | Non-supervisory $1-z$ | Cooperative $m$ | $P_{11}$<br>$P_9$<br>$P_1$<br>$P_4-C_3$ | $P_{11}-bF_7$<br>$P_9$<br>$P_1$<br>$P_4-C_3$ | $P_{11}-bF_7$<br>$P_9$<br>$P_1$<br>$P_4-C_3$ | $P_{11}-bF_7$<br>$P_9$<br>$a_1P_2-a_1C_1$<br>$P_5-C_3$ |
| | | Evil $m$ | $P_{11}-bF_7$ | $P_{11}-bF_7$ | $P_{11}-bF_7$ | $P_{11}-bF_7$ |
| | | | $P_7$ | $m_2P_8-m_2C_5$ | $m_1P_7-m_1C_4$ | $m_1P_7-m_1C_4+m_2P_8$<br>$-m$ |
| | | | $P_1$ | $P_1$ | $a_2P_3-a_2C_2$ | $a_1P_2-a_1C_1+a_2P_3$<br>$-a_2C$ |
| | | | $P_4-C_3$ | $P_6-C_3$ | $P_4-C_3$ | $P_5+P_6-2C_3$ |

$$
\begin{aligned}
&- a_2F_2 - a_2L_2)\\
&+ zm(1-y)(a_1P_2 - a_1C_1 - a_1F_1 - a_1L_1)\\
&+ z(1-m)y(a_2P_3 - a_2C_2 - a_2F_2 - a_2L_2)\\
&+ z(1-m)(1-y)(a_1P_2 - a_1C_1 + a_2P_3 - a_2C_2\\
&- a_1F_1 - a_1L_1 - a_2F_2 - a_2L_2)\\
&+ (1-z)myP_1 + (1-z)m(1-y)(a_1P_2 - a_1C_1)\\
&+ (1-z)(1-m)y(a_2P_3 - a_2C_2)\\
&+ (1-z)(1-m)(1-y)(a_1P_2 - a_1C_1\\
&+ a_2P_3 - a_2C_2)
\end{aligned} \tag{2}
$$

The average revenue for the agent node's strategic choice is:

$$
\overline{E_A} = xE_{A1} + (1-x)E_{A2} \tag{3}
$$

Similarly, the expected revenues for voting nodes adopting normal and abnormal voting strategies can be determined as follows:

$$
\begin{aligned}
E_{V1} = {} & zmx(P_4 - C_3) + zm(1-x)(P_4 - C_3)\\
&+ z(1-m)x(P_4 - C_3) + z(1-m)(1-x)\\
&\times (P_4 - C_3) + (1-z)mx(P_4 - C_3)\\
&+ (1-z)m(1-x)(P_4 - C_3)\\
&+ (1-z)(1-m)x(P_4 - C_3)\\
&+ (1-z)(1-m)(1-x)(P_4 - C_3)
\end{aligned} \tag{4}
$$

$$
\begin{aligned}
E_{V2} = {} & zmx(P_4 - F_3 - F_4 - L_3 - L_4 - 2C_3)\\
&+ zm(1-x)(P_5 - C_3 - F_3 - L_3) + z(1-m)\\
&\times x(P_6 - C_3 - F_4 - L_4) + z(1-m)(1-x)\\
&\times (P_5 + P_6 - 2C_3 - F_3 - F_4 - L_3 - L_4)\\
&+ (1-z)mx(P_4 - C_3) + (1-z)m(1-x)\\
&\times (P_5 - C_3) + (1-z)(1-m)x(P_6 - C_3)\\
&+ (1-z)(1-m)(1-x)(P_5 + P_6 - 2C_3)
\end{aligned} \tag{5}
$$

$$
\overline{E_V} = yE_{V1} + (1-y)E_{V2} \tag{6}
$$

The expected revenues for malicious nodes choosing cooperative and evil strategies are respectively:

$$
\begin{aligned}
E_{M1} = {} & zxyP_9 + zx(1-y)P_9 + z(1-x)yP_9\\
&+ z(1-x)(1-y)P_9 + (1-z)xyP_9\\
&+ (1-z)x(1-y)P_9 + (1-z)(1-x)yP_9\\
&+ (1-z)(1-x)(1-y)P_9
\end{aligned} \tag{7}
$$

$$
\begin{aligned}
E_{M2} = {} & zxy(P_7 - m_1C_4 - m_2C_5 - m_1F_5 - m_2F_6\\
&- m_1L_5 - m_2L_6)\\
&+ zx(1-y)(m_2P_8 - m_2C_5 - m_2F_6 - m_2L_6)\\
&+ z(1-x)y(m_1P_7 - m_1C_4 - m_1F_5 - m_1L_5)\\
&+ z(1-x)(1-y)(m_1P_7 - m_1C_4 + m_2P_8\\
&- m_2C_5 - m_1F_5 - m_1L_5 - m_2F_6 - m_2L_6)
\end{aligned} \tag{8}
$$

$$
\begin{aligned}
&+(1-z)xyP_7+(1-z)x(1-y)(m_2P_8-m_2C_5)\\
&+(1-z)(1-x)y(m_1P_7-m_1C_4)\\
&+(1-z)(1-x)(1-y)(m_1P_7-m_1C_4\\
&\quad+m_2P_8-m_2C_5)
\end{aligned}
$$

$$
\overline{E_M}=mE_{M1}+(1-m)E_{M2} \tag{9}
$$

The expected revenues for supervisory nodes adopting supervisory and non-supervisory strategies are, respectively:

$$
\begin{aligned}
E_{S1}=&mxy(P_{10}-C_6)+mx(1-y)(P_{10}-C_6\\
&+F_3+F_4)\\
&+m(1-x)y(P_{10}-C_6+a_1F_1+a_2F_2)\\
&+m(1-x)(1-y)(P_{10}-C_6+a_1F_1+F_3)\\
&+(1-m)xy(P_{10}-C_6+m_1F_5+m_2F_6)\\
&+(1-m)x(1-y)(P_{10}-C_6+F_4+m_2F_6)\\
&+(1-m)(1-x)y(P_{10}-C_6+m_1F_5+a_2F_2)\\
&+(1-m)(1-x)(1-y)(P_{10}-C_6+m_1F_5\\
&\quad+m_2F_6+a_1F_1+a_2F_2+F_3+F_4)
\end{aligned} \tag{10}
$$

$$
\begin{aligned}
E_{S2}=&mxyP_{11}+mx(1-y)(P_{11}-bF_7)\\
&+m(1-x)y(P_{11}-bF_7)+m(1-x)(1-y)\\
&\times(P_{11}-bF_7)+(1-m)xy(P_{11}-bF_7)\\
&+(1-m)x(1-y)(P_{11}-bF_7)+(1-m)\\
&\times(1-x)y(P_{11}-bF_7)+(1-m)\\
&\times(1-x)(1-y)(P_{11}-bF_7)
\end{aligned} \tag{11}
$$

$$
\overline{E_S}=zE_{S1}+(1-z)E_{S2} \tag{12}
$$

### *E. Evolutionary Stabilization Strategy Solving*

To analyze the evolutionary stability of each subject's strategy, we derive the replicator dynamic equations for the four types of nodes under different strategy combinations, based on the four-party game payoff matrix presented in Table III.

The dynamic evolution of the agent node's choice of the "non-bribery" strategy is influenced by its expected revenue, and the replication dynamic equation is:

$$
\begin{aligned}
F(x)=\frac{\mathrm{d}x}{\mathrm{d}t}&=x(E_{A1}-\overline{E_A})=x(1-x)(E_{A1}-E_{A2})\\
&=-x(x-1)(P_1+a_1C_1+a_2C_2-a_1P_2\\
&\quad-a_2P_3-ma_2C_2-ya_1C_1+ma_2P_3+za_1F_1\\
&\quad+za_2F_2+za_1L_1+za_2L_2+ya_1P_2-myP_1\\
&\quad-mza_2F_2-mza_2L_2-yza_1F_1-yza_1L_1\\
&\quad+myza_1C_1+myza_2C_2+myza_1F_1\\
&\quad+myza_2F_2+myza_1L_1+myza_2L_2)
\end{aligned} \tag{13}
$$

The replication dynamics equation for a voting node choosing the "normal voting" strategy is:

$$
\begin{aligned}
F(y)=\frac{\mathrm{d}y}{\mathrm{d}t}&=y(E_{V1}-\overline{E_V})=y(1-y)(E_{V1}-E_{V2})\\
&=-y(y-1)(C_3+P_4-P_5-P_6-mC_3-xC_3\\
&\quad+mP_6+zF_3+zF_4+zL_3+zL_4+xP_5\\
&\quad+xmC_3-mzF_4-mzL_4-mxP_4-xzF_3\\
&\quad-xzL_3+xmzC_3+xmzF_3\\
&\quad+xmzF_4+xmzL_3+xmzL_4)
\end{aligned} \tag{14}
$$

The replication dynamics equation for a malicious node choosing a "cooperative" strategy is:

$$
\begin{aligned}
F(m)=\frac{\mathrm{d}m}{\mathrm{d}t}&=m(E_{M1}-\overline{E_M})\\
&=m(1-m)(E_{M1}-E_{M2})\\
&=-m(m-1)(P_9+m_1C_4+m_2C_5-m_1P_7\\
&\quad-m_2P_8-xm_1C_4-ym_2C_5+zm_1F_5\\
&\quad+zm_2F_6+zm_1L_5+zm_2L_6+xm_1P_7\\
&\quad+ym_2P_8-xyP_7-xzm_1F_5-yzm_2F_6\\
&\quad-xzm_1L_5-yzm_2L_6+xyzm_1C_4\\
&\quad+xyzm_2C_5+xyzm_1F_5+xyzm_2F_6\\
&\quad+xyzm_1L_5+xyzm_2L_6)
\end{aligned} \tag{15}
$$

The replication dynamics equation for the supervisory node choosing the "supervisory" strategy is:

$$
\begin{aligned}
F(z)=\frac{\mathrm{d}z}{\mathrm{d}t}&=z(E_{S1}-\overline{E_S})=z(1-z)(E_{S1}-E_{S2})\\
&=z(z-1)(C_6-F_3-F_4-P_{10}+P_{11}-a_1F_1\\
&\quad-a_2F_2-bF_7+mF_4-m_1F_5-m_2F_6+xF_3\\
&\quad+yF_3+yF_4+ma_2F_2+xa_1F_1+xa_2F_2\\
&\quad+ya_1F_1+mm_1F_5+mm_2F_6-mxF_3\\
&\quad-mxF_4+xm_1F_5-myF_4+ym_2F_6-xyF_3\\
&\quad+mxyF_3+mxyF_4-xym_1F_5-xym_2F_6\\
&\quad-mxa_2F_2-mya_1F_1-mya_2F_2-xya_1F_1\\
&\quad-xmm_1F_5-mym_2F_6+mxya_1F_1\\
&\quad+mxya_2F_2+mxybF_7+mxym_1F_5\\
&\quad+mxym_2F_6)
\end{aligned} \tag{16}
$$

In order to seek the system evolutionary stable equilibrium solution, the above four equations will be associated, according to the stability theorem of differential equations, so that $F(x)=F(y)=F(m)=F(z)=0$ can be obtained by the 16 pure strategy solution of the system: $E_1(0,0,0,0)$, $E_1(0,0,0,1)$, $E_1(0,0,1,0)$, $E_1(0,0,1,1)$, $E_1(0,1,0,0)$, $E_1(0,1,0,1)$, $E_1(0,1,1,0)$, $E_1(0,1,1,1)$, $E_1(1,0,0,0)$, $E_1(1,0,0,1)$, $E_1(1,0,1,0)$, $E_1(1,0,1,1)$, $E_1(1,1,0,0)$, $E_1(1,1,0,1)$, $E_1(1,1,1,0)$, $E_1(1,1,1,1)$.

In the asymmetric game, the evolutionary stable equilibrium must be the strict Nash equilibrium, and the strict Nash equilibrium must be the pure strategy equilibrium [32]. Therefore, we only discuss the stability of the pure strategy equilibrium point, and the analysis of the eigenvalues and equilibrium stability of the $E_1 \sim E_{16}$ eigenvalues and the equilibrium points are shown in Table IV.

### *F. Equilibrium Point Stability Analysis*

From Table IV, it can be seen that there are eigenvalues equal to or greater than zero in the Jacobi matrices of

TABLE IV
STABILITY ANALYSIS OF PURE STRATEGY EQUILIBRIUM POINTS

| Balance Point | Eigenvalue | Positive or Negative | Stability | Scene |
|---|---|---|---|---|
| (0,0,0,0) | $P_1 + a_1C_1 - a_1P_2 + a_2C_2 - a_2P_3, C_3 + P_4 - P_5 - P_6,$ $P_9 + m_1C_4 + m_2C_5 - m_1P_7 - m_2P_8,$ $-C_6 + F_3 + F_4 + P_{10} - P_{11} + a_1F_1 + a_2F_2 + bF_7 + m_1F_5 + m_2F_6$ | N,N,N,N | ESS | (1) |
| (0,0,0,1) | $P_1 + a_1C_1 - a_1P_2 - a_2P_3 + a_2C_2 + a_1F_1 + a_2F_2 + a_1L_1 + a_2L_2,$ $C_3 + P_4 - P_5 - P_6 + F_3 + F_4 + L_3 + L_4,$ $P_9 + m_1C_4 + m_2C_5 - m_1P_7 - m_2P_8 + m_1F_5 + m_2F_6 + m_1L_5 + m_2L_6,$ $C_6 - F_3 - F_4 - P_{10} + P_{11} - a_1F_1 - a_2F_2 - bF_7 - m_1F_5 - m_2F_6$ | N,N,N,N | ESS | (2) |
| (0,0,1,0) | $P_1 + a_1C_1 - a_1P_2, P_4 - P_5, - P_9 - m_1C_4 - m_2C_5 + m_1P_7 + m_2P_8$ , $-C_6 + F_3 + P_{10} - P_{11} + a_1F_1 + bF_7$ | N,N,N,N | ESS | (3) |
| (0,0,1,1) | $P_1 + a_1C_1 + a_1F_1 + a_1L_1 - a_1P_2, C_4 + P_4 - P_5 - C_3 + F_3 + L_3,$ $-P_9 - m_1C_4 - m_2C_5 + m_1P_7 + m_2P_8 - m_1F_5 - m_2F_6 - m_1L_5 - m_2L_6,$ $C_6 - F_3 - P_{10} + P_{11} - a_1F_1 - bF_7$ | N,N,N,N | ESS | (4) |
| (0,1,0,0) | $P_1 - a_2P_3 + a_2C_2, - C_3 - P_4 + P_5 + P_6, P_9 + m_1C_4 - m_1P_7$ , $-C_6 + P_{10} - P_{11} + a_2F_2 + bF_7 + m_1F_5$ | N,N,N,N | ESS | (5) |
| (0,1,0,1) | $P_1 - a_2P_3 + a_2C_2 + a_2F_2 + a_2L_2,$ $-C_6 - P_4 + P_5 + P_6 - F_3 - F_4 - L_3 - L_4,$ $P_9 + m_1C_4 - m_1P_7 + m_1F_5 + m_1L_5,$ $C_6 - P_{10} + P_{11} - a_2F_2 - bF_7 - m_1F_5$ | N,N,N,N | ESS | (6) |
| (0,1,1,0) | $0, - P_4 + P_5, - P_9 - m_1C_4 + m_1P_7$ , $-C_6 + P_{10} - P_{11} + a_1F_1 + a_2F_2 + bF_7$ | 0,N,N,N | Saddle Point | \ |
| (0,1,1,1) | $a_1F_1 + a_1L_1 + a_2L_2 + a_1C_1 + a_2C_2 + a_2F_2, - P_4 + P_5 - P_6 - L_3,$ $-P_9 - m_1C_4 + m_1P_7 - m_1F_5 - m_1L_5,$ $C_6 - P_{10} + P_{11} - a_1F_1 - a_2F_2 - bF_5$ | +,N,N,N | Unstable | \ |
| (1,0,0,0) | $-P_1 - a_1C_1 + a_1P_2 - a_2C_2 + a_2P_3, P_4 - P_6, P_9 + m_2C_5 - m_2P_8,$ $-C_6 + F_4 + P_{10} - P_{11} + bF_7 + m_1F_5$ | N,N,N,N | ESS | (7) |
| (1,0,0,1) | $-P_1 - a_1C_1 + a_1P_2 + a_2P_3 - a_2C_2 - a_1F_1 - a_2F_2 - a_1L_1 - a_2L_2,$ $P_4 - P_6 + F_4 + L_4, - P_9 - m_2C_5 + m_2P_8 - m_2F_6 - m_2L_6,$ $C_6 - F_4 - P_{10} + P_{11} - bF_7 - m_1F_5$ | N,N,N,N | ESS | (8) |
| (1,0,1,0) | $-P_1 - a_1C_1 + a_1P_2$ ,0, $P_9 + m_2C_5 - m_2P_8$ , $-C_6 + P_{10} - P_{11} + bF_7 - F_3 + F_4$ | N,0,N,N | Saddle Point | \ |
| (1,0,1,1) | $-P_1 - a_1C_1 + a_1P_2 - a_1F_1 - a_1L_1, C_3 + F_3 + F_4 + L_3 + L_4,$ $-P_9 - m_2C_5 + m_2P_8 - m_2F_6 - m_2L_6,$ $C_6 - F_3 - F_4 - P_{10} + P_{11} - bF_7$ | N,+,N,N | Unstable | \ |
| (1,1,0,0) | $-P_1 + a_2P_3 - a_2C_2, - P_4 + P_6, 0,$ $-C_6 + P_{10} - P_{11} + a_2F_2 + bF_7 + m_1F_5 + 2m_2F_6 - F_6$ | N,N,0,N | Saddle Point | \ |
| (1,1,0,1) | $-P_1 + a_2P_3 - a_2C_2 - a_2F_2 - a_2L_2, - P_4 + P_6 - F_4 - L_4,$ $m_1F_5 + m_2L_6 + m_1L_5 + m_1C_4 + m_2C_5 + m_2F_6,$ $C_6 - P_{10} + P_{11} - bF_7 - m_1F_5 - m_2F_6$ | N,N,+,N | Unstable | \ |
| (1,1,1,0) | $0, 0, 0, -C_6 + P_{10} - P_{11}$ | 0,0,0,N | Saddle Point | \ |
| (1,1,1,1) | $-(a_1C_1 + a_1L_1 + a_2L_2 + a_2C_2 + a_1F_1 + a_2F_2),$ $-(F_3 + L_3 + C_3 + F_4 + L_4),$ $-(m_1L_5 + m_1C_4 + m_2C_5 + m_1F_5 + m_2F_6 + m_2L_6), C_6 - P_{10} + P_{11}$ | -,-,-,N | ESS | (9) |

Note: N indicates that the positivity or negativity of the eigenvalue could not be determined; ESS indicates Evolutionary Stabilization Strategy.

the $E_1(0,1,1,0)$, $E_1(0,1,1,1)$, $E_1(1,0,1,0)$, $E_1(1,0,1,1)$, $E_1(1,1,0,0)$, $E_1(1,1,0,1)$, $E_1(1,1,1,0)$ equilibrium points, and the above equilibrium points are not evolutionary stable points. Evolutionary stabilization points may exist in the following scenarios (1)-(9):

(1) $E_1(0,0,0,0)$: $\lambda_1 = P_1 + a_1C_1 - a_1P_2 + a_2C_2 - a_2P_3$, $\lambda_2 = C_3 + P_4 - P_5 - P_6$, $\lambda_3 = P_9 + m_1C_4 + m_2C_5 - m_1P_7 - m_2P_8$, $\lambda_4 = -C_6 + F_3 + F_4 + P_{10} - P_{11} + a_1F_1 + a_2F_2 + bF_5 + m_1F_5 + m_2F_6$, Decide on the symbol of $\lambda_1$, $\lambda_2$, $\lambda_3$, $\lambda_4$.

If $P_1 < a_1P_2 - a_1C_1 + a_2P_3 - a_2C_2$, $P_4 < P_5 + P_6 - C_3$, $P_9 < m_1P_7 - m_1C_4 + m_2P_8 - m_2C_5$ and $P_{10} - C_6 + F_3 + F_4 + a_1F_1 + a_2F_2 + m_1F_5 + m_2F < P_{11} - bF_7$. Under these conditions, the revenue for an agent node obtaining block bookkeeping rights through normal voting is lower than the revenue from successful bribery. Similarly, the revenue for a voting node participating in normal voting is less than that from abnormal voting, the revenue for a malicious node adopting cooperative strategies is lower than that from engaging in malicious behavior, and the revenue for a supervisory node from supervision is less than that from non-supervision. Additionally, all eigenvalues of the corresponding Jacobian matrices are negative, indicating a stable evolutionary point. In this scenario, the stable evolutionary strategy is (bribery, abnormal voting, evil, non-supervision). Consequently, the presence of malicious behavior combined with the lack of supervision poses significant security risks for consensus nodes in the blockchain network, undermining secure and efficient consensus. This outcome clearly deviates from the intended improvement goals of the system.

To mitigate this issue, the system can escape this disadvantageous stable point by increasing penalties for agent node bribery and rewarding supervisory nodes for taking supervisory actions. These adjustments can drive the system toward a more secure and efficient operating state.

(2) $E_1(0,0,0,1)$: $\lambda_1 = P_1 + a_1C_1 - a_1P_2 - a_2P_3 + a_2C_2 + a_1F_1 + a_2F_2 + a_1L_1 + a_2L_2$, $\lambda_2 = C_3 + P_4 - P_5 - P_6 + F_3 + F_4 + L_3 + L_4$, $\lambda_3 = P_9 + m_1C_4 + m_2C_5 - m_1P_7 - m_2P_8 +$

$m_1F_5 + m_2F_6 + m_1L_5 + m_2L_6$, $\lambda_4 = C_6 - F_3 - F_4 - P_{10} + P_{11} - a_1F_1 - a_2F_2 - bF_7 - m_1F_5 - m_2F_6$, Decide on the symbol of $\lambda_1$, $\lambda_2$, $\lambda_3$, $\lambda_4$.

If $P_1 < a_1P_2 + a_2P_3 - a_2C_2 - a_1C_1 - a_1F_1 - a_2F_2 - a_1L_1 - a_2L_2$, $P_4 < P_5 + P_6 - C_3 - F_3 - F_4 - L_3 - L_4$, $P_9 < m_1P_7 + m_2P_8 - m_1C_4 - m_2C_5 - m_1F_5 - m_2F_6 - m_1L_5 - m_2L_6$ and $P_{11} < P_{10} - C_6 + F_3 + F_4 + \alpha_1F_1 + \alpha_2F_2 + bF_7 + m_1F_5 + m_2F_6$. If the agent node's revenue from normal voting is less than the difference between the revenue from successful bribery and the supervisory penalty; if the voting node's revenue from normal voting is less than the difference between the revenue from abnormal voting and the supervisory penalty; if the malicious node's revenue from a cooperative strategy is less than the difference between the revenue from malicious actions and the supervisory penalty; and if the supervisory node's revenue from failing to supervise is less than the gain from supervisory actions and imposing penalties, the system's eigenvalues remain negative, indicating a stable equilibrium point. The corresponding strategies are (bribery, abnormal voting, evil, supervisory). Although supervision is implemented, bribery and malicious behaviors persist, posing security risks.

To overcome this, the system should increase the incentives for positive behavior among agent nodes, voting nodes, and malicious nodes, while intensifying supervision and penalties to suppress bribery, abnormal voting, and malicious activities. These measures promote a more secure and efficient evolutionary stable point, ensuring robust blockchain network operation.

(3) $E_1(0, 0, 1, 0)$: $\lambda_1 = P_1 + a_1C_1 - a_1P_2$, $\lambda_2 = P_4 - P_5$, $\lambda_3 = -P_9 - m_1C_4 - m_2C_5 + m_1P_7 + m_2P_8$, $\lambda_4 = -C_6 + F_3 + P_{10} - P_{11} + a_1F_1 + bF_7$, Decide on the symbol of $\lambda_1$, $\lambda_2$, $\lambda_3$, $\lambda_4$.

If $P_1 < a_1P_2 - a_1C_1$, $P_4 < P_5$, $m_1P_7 + m_2P_8 - m_1C_4 - m_2C_5 < P_9$, $P_{10} - C_6 + a_1F_1 + F_3 < P_{11} - bF_7$. Under the above conditions, the revenue of an agent node in obtaining block bookkeeping rights through normal voting is less than the revenue obtained by successfully bribing a voting node; the revenue of a voting node through normal voting is less than its revenue from participating in abnormal voting due to bribery; the revenue of a malicious node from adopting a malicious behavior is more than its revenue from choosing a cooperative strategy; and the revenue of a supervisory node in enforcing supervision is less than its revenue in failing to enforce supervision, then the system The eigenvalues of the Jacobi matrix are all less than zero, indicating that the system reaches a stable equilibrium point at this time. The corresponding stable evolutionary strategies are (bribery, abnormal voting, cooperation, non-supervisory). At this stable point, bribery and abnormal voting exist in the system while the supervisory nodes choose not to supervise. This state poses a serious threat to the security and efficiency of the consensus nodes in the blockchain network, which is clearly contrary to the improvement goal of the design scheme.

To improve this disadvantageous situation, the following measures should be taken: appropriately increase the benefits of choosing positive behaviors by agent nodes and voting nodes in order to enhance their compliance incentives; at the same time, increase the supervisory efforts and elevate the penalties for improper behaviors, such as bribery and abnormal voting, so as to significantly increase the cost of non-compliance. These improvements will steer the system away from the current inferior stability point and towards a more secure and efficient equilibrium state, ensuring the robust operation of the blockchain network in complex environments.

(4) $E_1(0, 0, 1, 1)$: $\lambda_1 = P_1 + a_1C_1 + a_1F_1 + a_1L_1 - a_1P_2$, $\lambda_2 = C_4 + P_4 - P_5 - C_3 + F_3 + L_3$, $\lambda_3 = -P_9 - m_1C_4 - m_2C_5 + m_1P_7 + m_2P_8 - m_1F_5 - m_2F_6 - m_1L_5 - m_2L_6$, $\lambda_4 = C_6 - F_3 - P_{10} + P_{11} - a_1F_1 - bF_7$, Decide on the symbol of $\lambda_1$, $\lambda_2$, $\lambda_3$, $\lambda_4$.

If $P_1 < a_1P_2 - a_1C_1 - a_1F_1 - a_1L_1$, $P_4 - C_3 < P_5 - C_4 - F_3 - L_3$, $-m_1C_4 - m_2C_5 + m_1P_7 + m_2P_8 - m_1F_5 - m_2F_6 - m_1L_5 - m_2L_6 < P_9$ and $P_{11} - bF_7 < P_{10} - C_6 + a_1F_1 + F_3$. Under the above conditions, if the revenue of an agent node through normal voting is lower than the revenue from bribing a voting node; the revenue of a voting node from bribing a node to participate in anomalous voting plus the negative effect of supervisory penalties is greater than its revenue from voting through normal voting; the revenue of a malicious node from choosing a malicious behavior is lower than that of a cooperative strategy; and the revenue of a supervisory node for failing to implement supervision is lower than that of its taking supervisory action, the Jacobian matrix's eigenvalues are all negative and the system will reach an evolutionary stability point. The stable evolutionary strategies at this point are (bribery, abnormal voting, cooperation, supervisory). Despite the supervision implemented by the supervisory nodes, bribery and abnormal voting still exist in the system, which poses a serious threat to the security and efficiency of the consensus nodes in the blockchain network, and is clearly not in line with the improvement goal of the scheme.

In order to optimize the evolution path of the system, the punishment for bribery of agent nodes should be strengthened, and the punishment for abnormal voting behavior of voting nodes should be increased, so as to enhance the cost of violations and weaken their revenue advantage. These measures will help guide the system to jump out of the current unfavorable stability point and develop towards a more secure and efficient state, and ultimately achieve a robust guarantee for the consensus mechanism of the blockchain network.

(5) $E_1(0, 1, 0, 0)$: $\lambda_1 = P_1 - a_2P_3 + a_2C_2$, $\lambda_2 = -C_3 - P_4 + P_5 + P_6$, $\lambda_3 = P_9 + m_1C_4 - m_1P_7$, $\lambda_4 = -C_6 + P_{10} - P_{11} + a_2F_2 + bF_7 + m_1F_5$, Decide on the symbol of $\lambda_1$, $\lambda_2$, $\lambda_3$, $\lambda_4$.

If $P_1 < a_2P_3 - a_2C_2$, $P_5 + P_6 - C_3 < P_4$, $P_9 < m_1P_7 - m_1C_4$ and $P_{10} - C_6 + a_2F_2 + m_1F_5 < P_{11} - bF_7$. If an agent node's revenue from normal voting is less than from bribing a malicious node; if a voting node's revenue from abnormal voting is lower than from normal voting; if a malicious node's revenue from malicious behavior exceeds that of cooperation; and if a supervisory node's revenue from supervision is lower than from non-supervisory, the system stabilizes at (bribery, normal voting, evil, non-supervisory). This state, where both bribery and malicious behavior persist without supervision, undermines the security and efficiency of consensus nodes, violating the design scheme's goals.

To optimize the system's evolution, increase supervisory intensity and impose stricter penalties for bribery and malicious

behaviors to raise violation costs and reduce their advantages. These measures guide the system toward a secure and efficient evolutionary direction, achieving robust consensus mechanism operation in complex environments.

(6) $E_1(0,1,0,1)$: $\lambda_1 = P_1 - a_2P_3 + a_2C_2 + a_2F_2 + a_2L_2$, $\lambda_2 = -C_6 - P_4 + P_5 + P_6 - F_3 - F_4 - L_3 - L_4$, $\lambda_3 = P_9 + m_1C_4 - m_1P_7 + m_1F_5 + m_1L_5$, $\lambda_4 = C_6 - P_{10} + P_{11} - a_2F_2 - bF_7 - m_1F_5$, Decide on the symbol of $\lambda_1$, $\lambda_2$, $\lambda_3$, $\lambda_4$.

If $P_1 < a_2P_3 - a_2C_2 - a_2F_2 - a_2L_2$, $P_5 + P_6 - C_6 - F_3 - F_4 - L_3 - L_4 < P_4$, $P_9 < m_1P_7 - m_1C_4 - m_1F_5 - m_1L_5$ and $P_{11} - bF_7 < P_{10} - C_6 + a_2F_2 + m_1F_5$. If an agent node's revenue from normal voting is less than from bribing a malicious node adjusted for supervisory penalties; if a voting node's normal voting revenue exceeds abnormal voting minus penalties; if a malicious node's gain from cooperation is less than from malicious behavior adjusted for penalties; and if a supervisory node's revenue from supervision exceeds non-supervision, the system stabilizes at (bribery, normal voting, evil, supervisory). Despite supervision, bribery and malicious behavior persist, posing risks to consensus node security and efficiency.

To address this, strengthen penalties for bribery and abnormal voting to increase non-compliance costs and guide the system toward a secure and efficient equilibrium.

(7) $E_1(1,0,0,0)$: $\lambda_1 = -P_1 - a_1C_1 + a_1P_2 - a_2C_2 + a_2P_3$, $\lambda_2 = P_4 - P_6$, $\lambda_3 = P_9 + m_2C_5 - m_2P_8$, $\lambda_4 = -C_6 + F_4 + P_{10} - P_{11} + bF_7 + m_1F_5$, Decide on the symbol of $\lambda_1$, $\lambda_2$, $\lambda_3$, $\lambda_4$.

If $a_1P_2 - a_1C_1 + a_2P_3 - a_2C_2 < P_1$, $P_4 < P_6$, $P_9 < m_2P_8 - m_2C_5$ and $P_{10} - C_6 + F_4 + m_1F_5 < P_{11} - bF_7$. If an agent node's revenue from normal voting exceeds that of bribery, but a voting node's revenue from abnormal voting exceeds that of normal voting, and a malicious node's revenue from malicious behavior surpasses cooperation, while a supervisory node's gain from non-supervision exceeds that of supervision, the system stabilizes at (non-bribery, abnormal voting, evil, non-supervision). This state, despite the absence of bribery, retains abnormal voting and malicious behavior, undermining security and efficiency.

To improve, increase penalties for abnormal voting and reinforce supervisory incentives to ensure effective supervision. These measures steer the system toward secure and efficient operation.

(8) $E_1(1,0,0,1)$: $\lambda_1 = -P_1 - a_1C_1 + a_1P_2 + a_2P_3 - a_2C_2 - a_1F_1 - a_2F_2 - a_1L_1 - a_2L_2$, $\lambda_2 = P_4 - P_6 + F_4 + L_4$, $\lambda_3 = -P_9 - m_2C_5 + m_2P_8 - m_2F_6 - m_2L_6$, $\lambda_4 = C_6 - F_4 - P_{10} + P_{11} - bF_7 - m_1F_5$, Decide on the symbol of $\lambda_1$, $\lambda_2$, $\lambda_3$, $\lambda_4$.

If $a_1P_2 - a_1C_1 + a_2P_3 - a_2C_2 - a_1F_1 - a_2F_2 - a_1L_1 - a_2L_2 < P_1$, $P_4 < P_6 - F_4 - L_4$, $m_2P_8 - m_2C_5 - m_2F_6 - m_2L_6 < P_9$ and $P_{11} - bF_7 < P_{10} - C_6 + F_4 + m_1F_5$. If an agent node's revenue from normal voting exceeds that of bribery adjusted for penalties, and a malicious node's revenue from cooperation exceeds malicious behavior, the system stabilizes at (non-bribery, abnormal voting, evil, supervisory). Even with supervision, abnormal voting and malicious behavior persist, threatening system security and efficiency.

To optimize, impose stricter penalties for abnormal voting and enhance supervisory rewards to ensure active supervision. These steps promote secure and efficient evolution.

(9) $E_1(1,1,1,1)$: $\lambda_1, \lambda_2, \lambda_3 < 0$ , $\lambda_4 = C_6 - P_{10} + P_{11}$, Decide on the symbol of $\lambda_4$.

If $P_{11} < P_{10} - C_6$. In the ideal state, agent nodes secure block generation rights through normal voting; voting nodes objectively vote based on performance; malicious nodes adopt cooperative strategies; and supervisory nodes actively monitor. This state aligns with the design goal of a secure, efficient, and trustworthy blockchain consensus system.

This optimized blockchain system effectively balances the interests of agent, voting, malicious, and supervisory nodes, ensuring operational efficiency while minimizing security risks. Through dynamic evolution, the system converges to an ideal state, providing a robust foundation for blockchain networks in complex environments.

Because the incentive, punishment, and reputation mechanisms simultaneously enter the four-party replicator dynamic equations, the evolutionary outcome is determined not by a single mechanism but by the joint coupling thresholds formed by their interaction. Adjusting one mechanism alone is insufficient to alter the system's stability; only when the joint threshold is exceeded will the system transition among multiple equilibrium candidates. This leads to a multi-equilibrium and multi-stability structure that fundamentally differs from the single-path selection typically observed in PDPoS models.

In particular, within certain coupling intervals, multiple local ESSs may coexist, and their attraction domains depend on both initial strategies and the direction of mechanism adjustments. Such phenomena— including equilibrium switching and basin-of-attraction shifts—do not occur in static PDPoS frameworks. These results demonstrate that the dynamic coupling of the incentive–punishment–reputation mechanisms fundamentally reshapes the stability landscape, providing the theoretical foundation for the parameter-coupling analysis presented in Section IV-D.

### G. Theoretical Proof of Parameter Coupling Effects

Building on the previous analysis of equilibrium stability, this section further provides a theoretical demonstration of the coupling effects among key parameters, highlighting their profound influence on evolutionary trajectories and equilibrium stability.

First, consider the replicator dynamics equation (13) for agent nodes. The payoff difference not only involves bribery intensities $a_1$, $a_2$ and cost terms $C_1$, $C_2$, but also incorporates punishment terms $F_1$, $F_2$ and reputation loss terms $L_1$, $L_2$. Equation (13) shows that the evolutionary behavior of agent nodes is not determined by any single factor, but rather by the joint effects of ($a_i$, $F_i$, $L_i$). When bribery intensity rises while penalties and reputation losses remain insufficient, agent nodes are more likely to adopt the bribery strategy; conversely, when both punishment and reputation costs increase, the stability of non-bribery strategies is nonlinearly reinforced.

Second, in the dynamic equation (14) for voting nodes, supervisory intensity $z$ and reputation losses $L_3$, $L_4$ do not

act independently but are coupled with fines $F_3$, $F_4$ through product terms. When $z$ is low, abnormal voting behavior is barely constrained; as $z$ increases, the effects of fines and reputation losses are amplified, gradually destabilizing the abnormal voting strategy.

For malicious nodes, the dynamic equation (15) also exhibits parameter coupling. Malicious intensities $m_1$, $m_2$, together with cost terms $C_4$, $C_5$ and penalties $F_5$, $F_6$, $L_5$, $L_6$, jointly shape the payoff function, producing interaction terms such as ($zm_1F_5$, $zm_2F_6$, $zm_1L_5$, $zm_1L_6$). Thus, the evolution of malicious behavior depends not only on attack costs and benefits but also on the coupled effects of supervisory intensity and reputation losses. Insufficient regulation allows malicious behavior to persist, whereas stronger supervisory and reputation constraints lead malicious strategies to converge toward cooperation.

Finally, the dynamic equation (16) for supervisory nodes shows that their supervisory choices are jointly influenced by fines, supervisory costs, and the parameter $bF_7$. When fines $F_1 - F_7$ and reputation loss coefficients increase synergistically, the marginal benefits of supervisory behavior rise, thereby reinforcing overall system compliance.

In summary, within the four-party evolutionary game framework, the stability of the system's equilibrium is shaped not by isolated parameters but by the nonlinear coupling of bribery intensity, punishment severity, and reputation loss. This explains why, in simulation experiments, simultaneously increasing punishment and reputation loss accelerates convergence to the ideal equilibrium of "non-bribery—normal voting—cooperation—supervision," providing a solid theoretical foundation for optimizing the DPoS consensus mechanism.

## V. Simulation Results and Analysis

### A. Simulation Setup

This section aims to validate the dynamic evolution characteristics and stability of the improved DPoS four-party game model through numerical simulations, while further exploring how variations in key parameters influence the evolutionary trajectories of system strategies. The analysis primarily focuses on comparing the time-dependent changes in strategy selection among agent nodes, voting nodes, malicious nodes, and supervisory nodes under different mechanisms and initial conditions, thereby verifying the stability conclusions obtained from theoretical analysis.

The simulations were implemented using Python 3.8 and MATLAB R2017b within a unified hardware environment, configured with an Intel Core i7 processor, 32 GB of memory, and Windows 11 as the operating system. The evolutionary process was examined over a finite time interval of $\{0, 2\}$. The initial probabilities for strategy selection across the four node types were set as $\{0.5, 0.3, 0.2, 0.3\}$. Parameter configurations were determined based on the characteristics of practical DPoS consensus mechanisms, informed by prior studies [18], [28], [30], and aligned with the replicator dynamic equations and constraints introduced in Section IV to ensure consistency between theoretical assumptions and experimental design.

To enhance real-world relevance and external validity, the Edge-IIoTset industrial IoT dataset was incorporated, leveraging its multi-dimensional device attributes and representative attack behaviors to drive simulation inputs. Detailed parameter configurations are provided in Table V. For scientific rigor and reproducibility, all experiments were performed with a fixed random seed and repeated 20 times under each parameter setting. The averaged results were then reported to reduce the impact of randomness and ensure the robustness of the experimental conclusions.

TABLE V
Parameter Settings

| Parameter | Value | Parameter | Value | Parameter | Value |
|---|---|---|---|---|---|
| $P_1$ | 8 | $P_2$ | 12 | $P_3$ | 11 |
| $P_4$ | 13 | $P_5$ | 12 | $P_6$ | 10 |
| $P_7$ | 7 | $P_8$ | 16 | $P_9$ | 9 |
| $P_{10}$ | 18 | $P_{11}$ | 8 | $F_1$ | 1 |
| $F_2$ | 2 | $F_3$ | 5 | $F_4$ | 6 |
| $F_5$ | 8 | $F_6$ | 4 | $F_7$ | 7 |
| $L_1$ | 0.6 | $L_2$ | 0.3 | $L_3$ | 0.5 |
| $L_4$ | 0.9 | $L_5$ | 1 | $L_6$ | 2 |
| $C_1$ | 3 | $C_2$ | 6 | $C_3$ | 4 |
| $C_4$ | 5 | $C_5$ | 6 | $C_6$ | 7 |
| $a_1$ | 0.4 | $a_2$ | 0.8 | $m_1$ | 0.7 |
| $m_2$ | 0.9 | $b$ | 0.5 | | |

### B. Impact of Malicious Nodes on the Evolution of Parties' Strategies

The strategy choice of malicious nodes significantly affects overall system stability. Through simulation, this section investigates how different strategies adopted by malicious nodes ("evil" or "cooperation") impact the system's stability, as shown in Figure 4. The results reveal the following:

When a malicious node adopts the "evil" strategy, its high gains incentivize agent and voting nodes to adopt abnormal strategies, while suppressing the effectiveness of supervisory nodes. This leads to a reduction in system stability.

Conversely, when a malicious node adopts the "cooperation" strategy, its revenue aligns with positive strategies, resulting in a significant increase in the proportion of positive behaviors from agent and voting nodes. Additionally, the supervisory node's monitoring capability is strengthened, leading to a rapid stabilization of the system.

These findings demonstrate that when malicious nodes choose the "cooperation" strategy, the system's strategy evolution rate accelerates, quickly converging to the ideal stable point. In contrast, the "evil" strategy hinders system evolution and negatively impacts overall efficiency.

### C. Influence of Initial Participation Intentions

The initial participation intentions of the four types of nodes were set to $\{0.5, 0.3, 0.2, 0.3\}$, corresponding to agent nodes, voting nodes, malicious nodes, and supervisory nodes, respectively. As shown in the simulation results in Figure 5, the system eventually evolves into a stable equilibrium state of (1, 1, 1, 1), where the agent node adopts a non-bribery strategy, the voting node adopts a normal voting strategy, the malicious

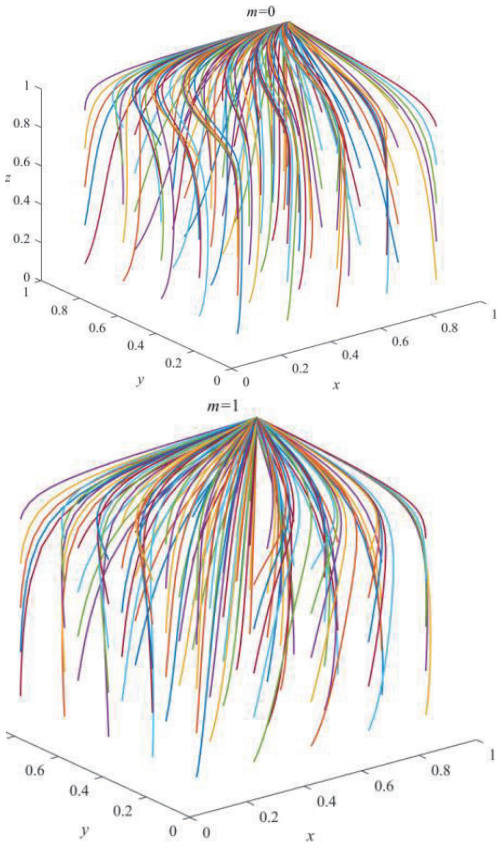


Fig. 4. Impact of malicious nodes on the evolution of the parties' strategies

node adopts a cooperative strategy, and the supervisory node adopts a supervisory strategy. At this equilibrium, all four parties achieve optimal or near-ideal payoffs.

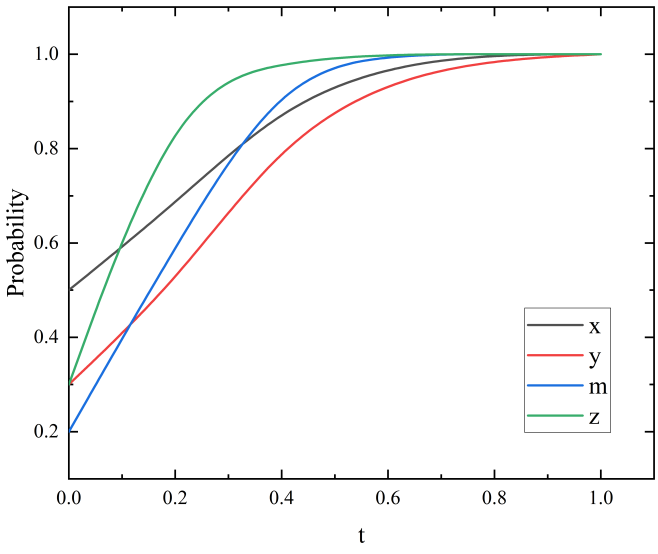


Fig. 5. Evolution results of four-party game

To further investigate the impact of initial intentions on the system's evolutionary dynamics, the non-bribery probability of the agent node was treated as a variable, with values of 0.1, 0.5, and 0.9 representing low, medium, and high intention levels, respectively. Figure 6 depicts the evolutionary trajectories of the game system under these different initial conditions. The results reveal that as the initial non-bribery willingness of agent nodes increases, the system converges more rapidly toward the cooperative equilibrium state (1, 1, 1, 1). This demonstrates that stronger initial non-bribery intentions among agent nodes not only accelerate their own transition to the non-bribery strategy but also significantly reinforce the inclination of voting nodes to engage in normal voting, enhance the cooperative willingness of malicious nodes, and gradually reduce the supervisory intensity of supervisory nodes. Ultimately, this process fosters a virtuous cycle of multi-party collaboration and mutual benefit.

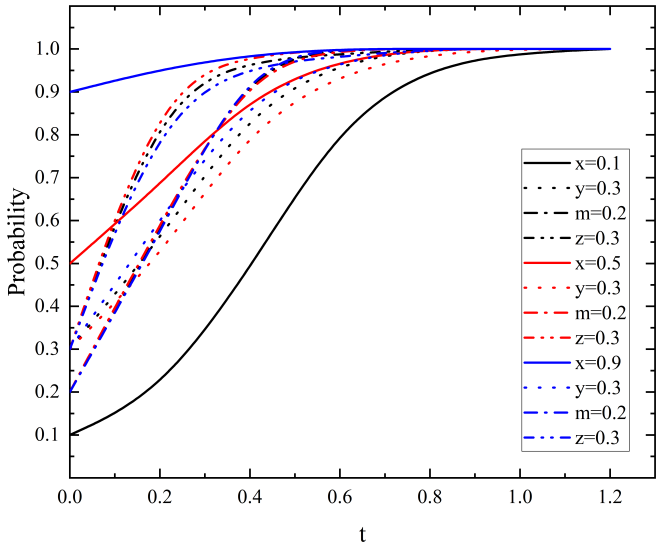


Fig. 6. The influence of agent nodes' initial willingness on evolution results

### *D. The Effect of Different Bribe Strengths of Agent Nodes on the Subject's Strategy Choice*

The existence of bribery behavior in the agent nodes of the DPoS consensus mechanism should be taken into account. To assess the impact of bribery behavior on model evolution, the bribery strength is set at values of $\{0, 0.4, 1.5\}$ and $\{0, 0.8, 1.8\}$. Figure 7 illustrates the evolution process of the strategies and the outcomes of the four-party game.

As can be observed in Figure 7, the cost of the bribe required steadily grows as the bribe strength of the agent nodes increasingly increases. This has essentially no effect on malicious and voting nodes but instead leads to a progressive increase in the willingness of supervisory nodes to regulate. Consequently, the counteracting agent nodes themselves take on an ever-greater reluctance to accept bribes. It is possible to minimize both agent node bribery and poor node behavior by introducing an appropriate amount of bribery strength into the DPoS consensus process, as may be discovered through the examination of behavioral decisions made by nodes.

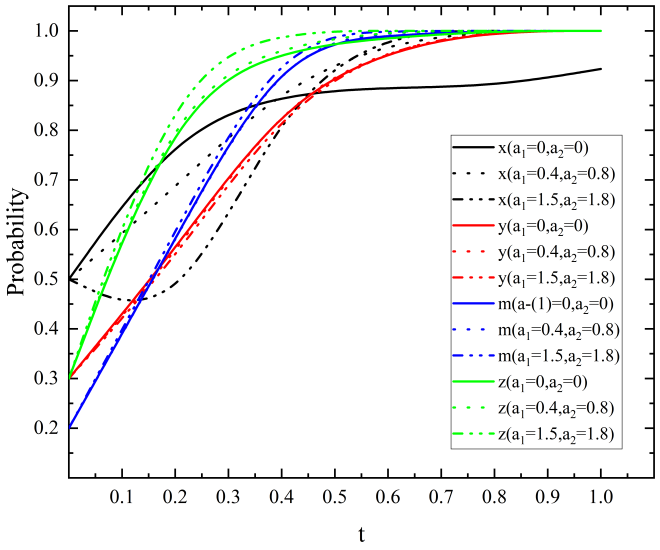


Fig. 7. Effect of different bribe strengths of agent nodes on subject's strategy choice

### *E. The Effect of Different Evil Strengths of Malicious Nodes on the Subject's Strategy Choice*

In the DPoS consensus mechanism, the malicious behavior of nodes poses a significant threat to system security and efficiency. To analyze the impact of evil strength on the strategy selection of each subject, the simulation sets the evil strength of malicious nodes to $\{0, 0.7, 2.2\}$ and $\{0, 0.9, 2.8\}$. The strategy evolution process of the four-party game is illustrated in Figure 8.

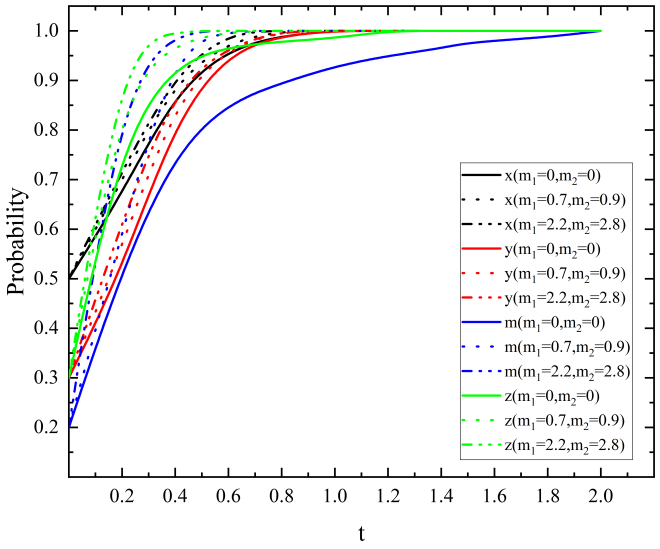


Fig. 8. Impact of different evil strengths of malicious nodes on the subject's strategy choice

According to Figure 8, as the evil strength increases, the benefits of malicious nodes exhibit a non-linear growth. However, their evil costs also rise proportionally. The simulation results show that higher evil strength significantly enhances the supervisory node's inclination to adopt the "supervisory" strategy, increasing its probability of doing so. Additionally, the likelihood of agent nodes refraining from bribery and malicious nodes adopting cooperative strategies increases as supervisory strength intensifies.

The findings suggest that incorporating the evil strength parameter helps establish an inhibitory mechanism against malicious behaviors in the system, thereby encouraging malicious nodes to adopt cooperative strategies.

### *F. Impact of Different Evil Costs of Malicious Nodes on Strategy Choice*

The cost of evil directly influences the decision-making of malicious nodes, and higher evil costs can effectively limit malicious behaviors. To examine the effect of evil cost on system evolution, the evil cost of malicious nodes is set to $\{0, 5, 10\}$ and $\{0, 6, 18\}$. The strategy evolution process of the four-party game is depicted in Figure 9.

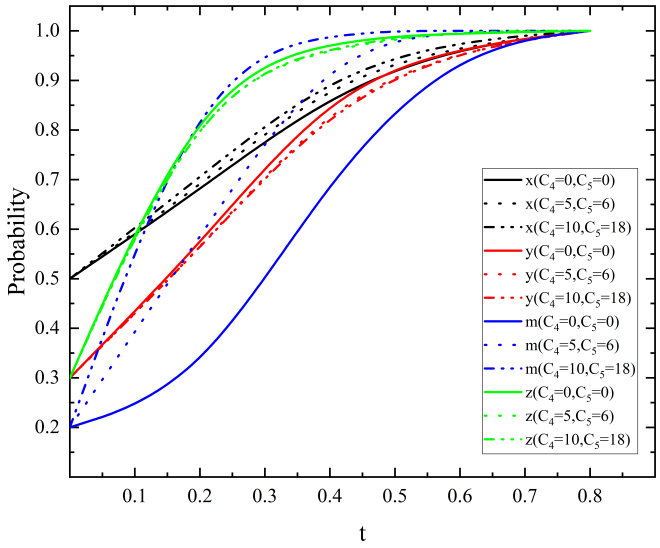


Fig. 9. Impact of different evil costs of malicious nodes on subject's strategy choice

Figure 9 shows that as the cost of evil increases, the probability of malicious nodes adopting the "cooperation" strategy rises significantly. Simultaneously, the probability of agent nodes refraining from bribery and voting nodes voting normally also increases. Additionally, the supervisory strength of supervisory nodes shows a clear upward trend with higher evil costs. These findings suggest that increased evil costs can promote positive behavioral evolution within the system.

The results demonstrate that a well-designed evil cost parameter in the DPoS consensus mechanism can effectively constrain malicious node behaviors and enhance overall system stability.

### *G. Impact of Punishment Mechanisms on Subjects' Strategy Choices*

The penalty mechanism, as a crucial constraint in the DPoS consensus mechanism, directly inhibits malicious behavior. To analyze the impact of penalty strength on the strategies of each subject, the penalty values are set to $\{0, 1, 5\}$, $\{0, 2, 8\}$,

$\{0, 5, 12\}$, $\{0, 6, 15\}$, $\{0, 8, 16\}$, and $\{0, 4, 13\}$. The strategy evolution process of the four-party game is depicted in Figure 10.

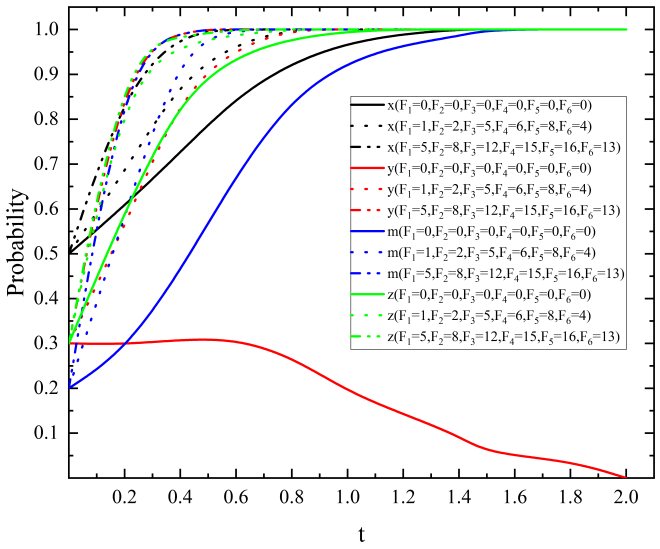


Fig. 10. Impact of different fines on subject's strategy choice

Figure 10 shows that when penalty strength is low, abnormal voting by voting nodes and harmful behaviors by agent and malicious nodes increase significantly. As penalty strength rises, the probability of voting nodes choosing normal voting increases rapidly, while the willingness of agent nodes to avoid bribery and malicious nodes to cooperate also increases substantially. Additionally, the supervisory intensity of supervisory nodes grows significantly with stronger penalties.

The simulation results confirm the effectiveness of the penalty mechanism in curbing malicious behaviors and enhancing system security. Properly setting penalty values can balance node behaviors and improve system stability.

### *H. Impact of Reputation Mechanisms on Subject's Strategy Choice*

In the DPoS consensus mechanism, the reputation mechanism enhances positive incentives by penalizing violations through reputation loss. To examine the impact of reputation loss on subjects' strategies, reputation loss values are set to $\{0, 2, 6\}$, $\{0, 2.5, 6.5\}$, $\{0, 3, 7\}$, $\{0, 2.8, 6.8\}$, $\{0, 3.4, 7.5\}$, and $\{0, 3.5, 7.8\}$. The strategy evolution process of the four-party game is depicted in Figure 11.

Figure 11 shows that as the reputation loss for bribery and collusion by voting nodes increases, the likelihood of voting nodes adopting normal voting rises significantly. Similarly, the probability of agent nodes refraining from bribery also increases. Under higher reputation loss, malicious nodes are more inclined to choose the "cooperation" strategy, while the supervisory intensity of regulatory nodes gradually decreases. These findings indicate that the reputation mechanism positively influences the reduction of bad behaviors and optimizes system evolution.

The results demonstrate that integrating a well-designed reputation mechanism into the DPoS consensus mechanism

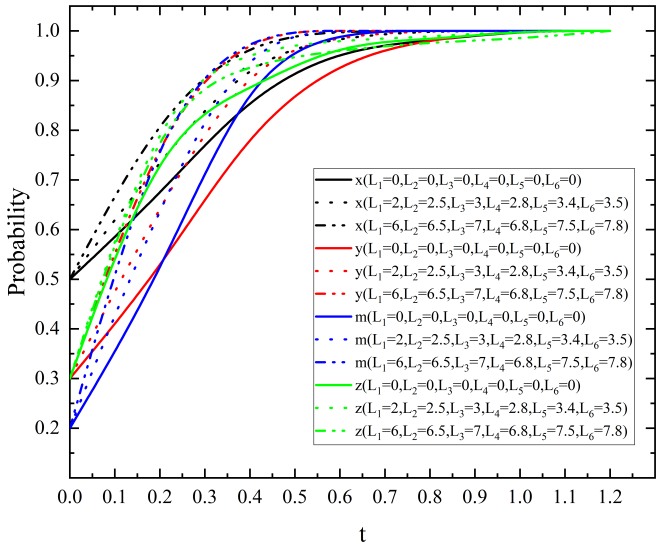


Fig. 11. Impact of loss of reputational value due to supervision

enhances node motivation for compliance and effectively limits the occurrence of malicious behaviors.

### *I. The Effect of Different Levels of Punishment on Subject's Strategy Choice*

To ensure that the blockchain system reaches consensus safely and efficiently with minimal computational overhead while completing transaction recording, it is essential to adjust penalty strength at different stages of node population evolution. The penalty strength is set to $b = 0, 0.5, 3$. The simulation results are shown in Figure 12.

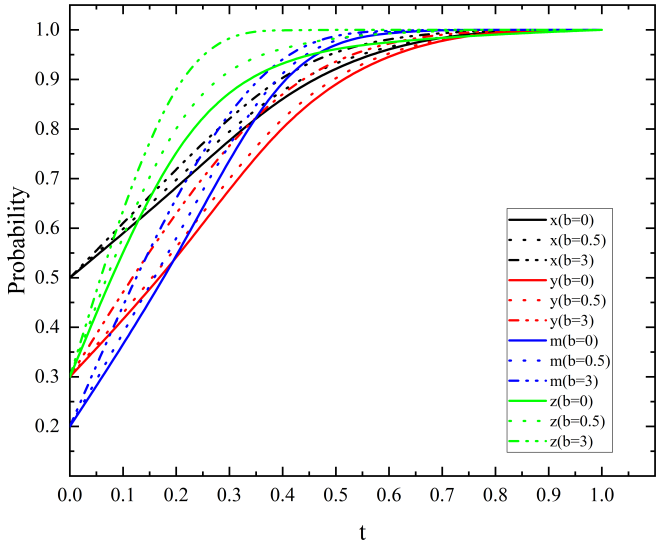


Fig. 12. Effect of different penalty levels on subject's strategy choice

Figure 12 demonstrates that as the punishment for supervisory nodes' inaction increases, the willingness of supervisory nodes to enforce supervision rises significantly. Concurrently, the voting nodes show a higher inclination toward normal voting, and the probabilities of agent nodes refraining from

bribery and malicious nodes adopting cooperative strategies also increase.

The results indicate that dynamically adjusting the punishment factor at different stages of node population evolution enhances supervisory behavior, thereby improving the overall efficiency and security of the system.

### J. Performance Comparison of Consensus Mechanisms

To comprehensively assess the overall performance of the proposed optimized DPoS consensus mechanism in an industrial IoT environment, this section introduces the traditional PoS and PDPoS mechanisms as baselines, while retaining the fundamental parameters summarized in Table V. Comparative simulation experiments are conducted along three key dimensions: efficiency, scalability, and security. The corresponding quantitative evaluation metrics include system throughput, average transaction latency, and the success rate of double-spending attacks. The experimental environment is implemented in Python 3.8 and leverages the publicly available industrial IoT dataset Edge-IIoTset to ensure data authenticity and representativeness. For scalability testing, the number of nodes is varied from 100 to 1000 in increments of 100, resulting in 10 test scenarios. The proportion of malicious nodes is fixed at 10%, the merchant transaction confirmation threshold is set to $k = 3$, the average transaction data size is 500 B, the block capacity is 1 MB, the block generation interval is 2 s, and the number of validators is 21. The success rate of double-spending attacks is estimated using the Monte Carlo method over multiple rounds of independent simulations to enhance the robustness and reliability of the statistical outcomes. These settings enable a comprehensive comparison of the performance differences and advantages of the three consensus mechanisms under consistent experimental conditions.

As illustrated in Figure 13, the TPS of all three consensus mechanisms shows a gradual decline as the number of nodes increases. This degradation can be attributed to higher network propagation latency and greater consensus coordination overhead associated with larger node scales. Nevertheless, the optimized DPoS consistently outperforms PoS and PDPoS in terms of TPS across all scales, with its advantage becoming increasingly evident in large-scale networks. This superior performance primarily stems from the incorporation of fairness constraints and reputation-weighted strategies in the validator selection process, which effectively lower the likelihood of inefficient nodes being elected, thereby improving block production efficiency and enhancing overall TPS.

As illustrated in Figure 14, the average latency of all three consensus mechanisms increases with the number of nodes. However, the rate of latency growth for the optimized DPoS is significantly lower than that of PoS and PDPoS, indicating superior scalability. This improvement arises from the ability of the optimized DPoS to sustain a high-quality validator set even in large-scale network environments, while simultaneously reducing redundant verification overhead during block propagation and confirmation, thereby shortening transaction confirmation time.

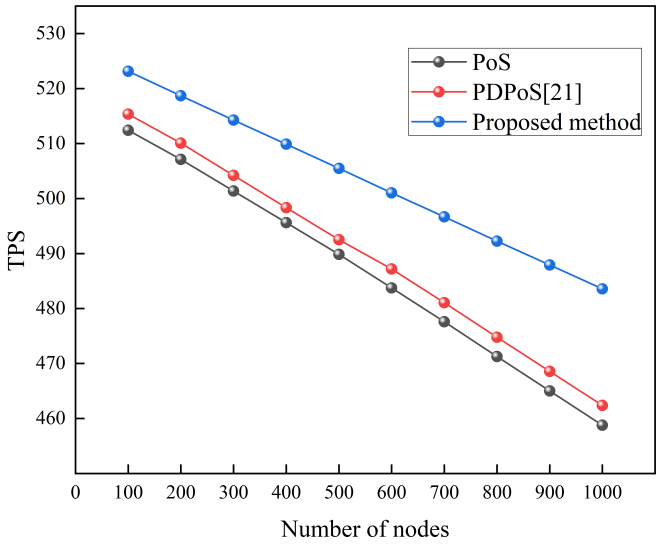


Fig. 13. Comparison of TPS under different numbers of nodes

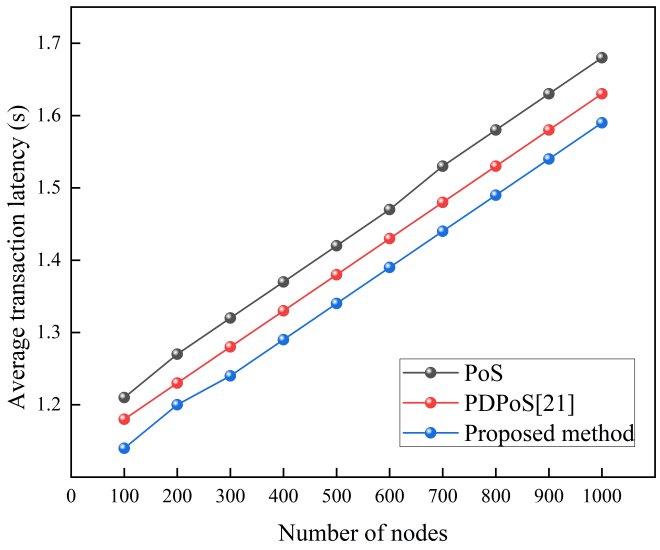


Fig. 14. Comparison of average transaction latency under different numbers of nodes

As illustrated in Figure 15, under the conditions of a confirmation threshold of and a malicious node ratio of 10%, the improved DPoS achieves the lowest double-spending attack success rate, reducing it by approximately 40% compared with PoS and by about 30% compared with PDPoS. As the number of nodes increases, the attack success rates of all three mechanisms exhibit a downward trend, with the improved DPoS demonstrating the most substantial reduction. These results highlight the significant advantages of the proposed mechanism in enhancing transaction finality and resisting double-spending attacks, thereby making it more suitable for high-security industrial IoT scenarios.

### K. Performance Comparison of Game Models

To validate the advantages of the proposed four-party game model in capturing real-world dynamics and enhancing system robustness, we constructed two baseline models:

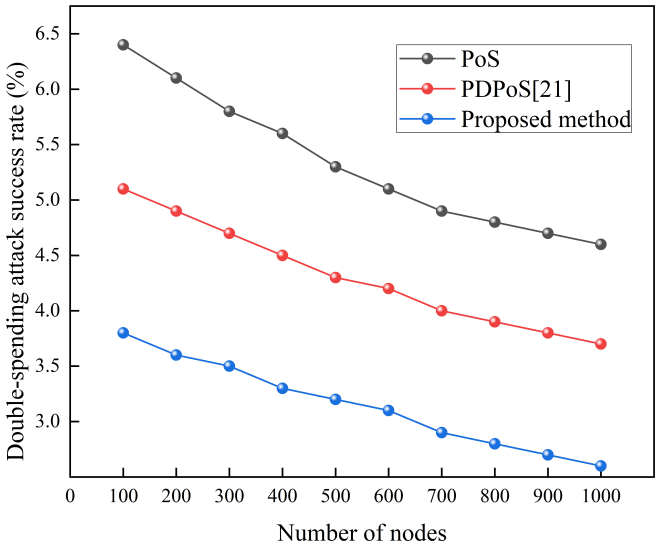


Fig. 15. Comparison of double-spending attack success rate under different numbers of nodes

a two-party model (agent–voting) and a three-party model (agent–voting–supervisor), while keeping all parameters and initial conditions identical. These two baseline models were derived through role ablation from the four-party model, with all parameters maintained consistently except for the removal of the corresponding entities.

As illustrated in Figure 16, the strategy convergence curves of the three models under identical initial conditions are presented. The four-party model converges to the ideal stable strategy (i.e., non-bribery, normal voting, cooperation, and supervisory behavior) at approximately $t \approx 1.25$, achieving a convergence time that is roughly 15% shorter than that of the three-party model and about 25% shorter than that of the two-party model.

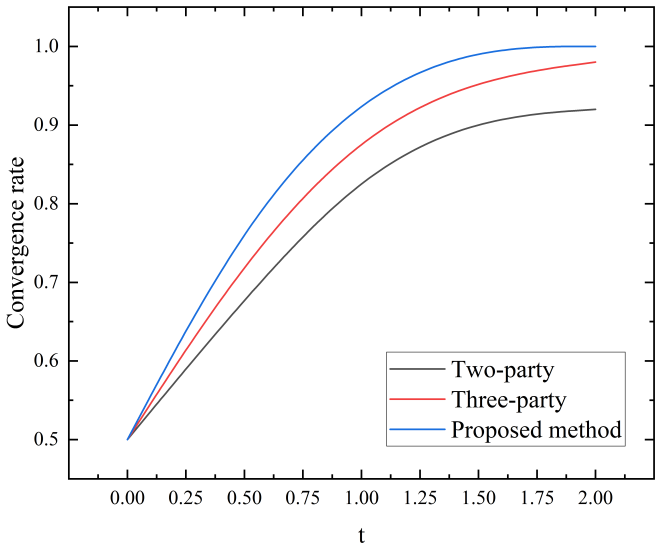


Fig. 16. Comparison of double-spending attack success rate under different numbers of nodes

As illustrated in Figure 17, the four-party model integrates a dynamic game mechanism between malicious nodes and supervisory nodes. Upon reaching a stable state, the proportion of malicious nodes is reduced to below 5%. In contrast, the stable-state proportion of malicious nodes in the three-party model is approximately 12%, while that in the two-party model is around 18%.

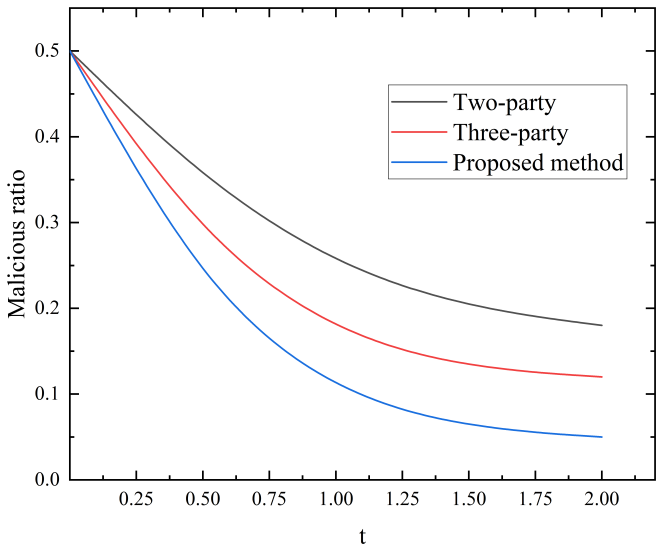


Fig. 17. Comparison of double-spending attack success rate under different numbers of nodes

## VI. Discussion

### A. Comparison with Existing Studies

To further validate the effectiveness of the proposed mechanism, we conduct a comparative analysis with existing consensus mechanisms and game models, and the results are presented in Table VI and Table VII.

TABLE VI
PERFORMANCE COMPARISON OF POS, PDPOS, AND THE PROPOSED DPOS

| Consensus mechanism | TPS (↑) | Average latency s (↓) | Double-spending attack success rate % (↓) |
|---|---|---|---|
| PoS | 458.78 | 1.68 | 4.6 |
| PDPoS [21] | 462.38 | 1.63 | 3.7 |
| Proposed method | 483.58 | 1.59 | 2.6 |

TABLE VII
PERFORMANCE COMPARISON OF GAME MODELS

| Performance metric | Two-party model | Three-party model | Proposed method |
|---|---|---|---|
| Convergence time | 1.65 | 1.45 | 1.25 |
| Stable proportion of malicious nodes | 18% | 12% | <5% |
| Multi-party interaction modeling capability | Low | Medium | High |

As shown in Table VI,the comparison results demonstrate that the improved DPoS mechanism proposed in this paper consistently outperforms PoS and PDPoS across the dimensions of efficiency, scalability, and security. With respect to

efficiency, when the number of nodes reaches 1,000, the improved DPoS achieves a TPS increase of approximately 5.4% compared with PoS and about 4.6% compared with PDPoS. In terms of scalability, it exhibits the lowest latency growth rate, indicating that the mechanism can sustain fast response times even in large-scale network environments. Regarding security, the double-spending attack success rate is reduced to 2.6%, representing a decrease of approximately 43.5% compared with PoS and around 29.7% compared with PDPoS. These findings clearly highlight the superiority of the improved mechanism in resisting attacks and demonstrate its potential to significantly enhance the overall performance of blockchain systems in high-security, high-concurrency application scenarios such as industrial IoT.

As shown in Table VII, the four-party evolutionary game model substantially outperforms the two-party and three-party models in terms of convergence speed and mitigation of malicious behavior, while demonstrating clear advantages in capturing multi-agent interactions and adapting to complex IIoT application scenarios.

### B. Policy Recommendations

Based on the research results, the following policy recommendations are proposed to further optimize the DPoS consensus mechanism and enhance its practical application in IIoT:

Implementation of Dynamic Incentive and Penalty Mechanism: A flexible incentive and punishment mechanism should be established to dynamically adjust fines, rewards, and reputation parameters according to different application scenarios. For instance, in systems with frequent malicious behaviors, stronger penalties and higher mischief costs can curb negative actions. Conversely, in scenarios where node motivation is low, increasing incentives for positive behaviors can enhance system efficiency.

Introduction of Multi-Level Supervisory Architecture: A hierarchical supervision strategy is recommended, categorizing supervisory nodes into basic and advanced levels. Basic supervisory nodes focus on real-time monitoring of malicious behaviors, while advanced nodes analyze abnormal behavior patterns and formulate precise punitive measures. This layered approach enhances system security and response speed.

Early Warning System for Malicious Node Behavior: A dynamic monitoring and early warning system for malicious node behavior should be developed. By analyzing node behavior data in real time through machine learning algorithms, potential threats can be identified in advance. This mechanism enables the system to implement preventive measures before malicious behaviors occur, minimizing their impact.

Deep Integration of Reputation Mechanism and Economic: Incentives Long-term node reputation should be closely tied to the economic incentive mechanism to create a sustainable node behavior management framework. Specific measures include dynamically adjusting nodes' revenue distribution based on their reputation and restricting low-reputation nodes from participating in voting or candidacy.

Adaptive Model Extension To ensure practical applicability across different IIoT scenarios (e.g., smart manufacturing, supply chain management, energy monitoring), the game model should be extended with scenario-specific parameters such as data sharing sensitivity and node computing power. This approach enhances the operational viability of the proposed optimization scheme.

### C. Practical Implementation Pathways in IIoT

The improved DPoS consensus mechanism proposed in this manuscript offers a clear implementation pathway in existing IIoT environments, as outlined below:

First, at the architectural mapping level, the blockchain storage framework introduced in Section III can be integrated with real-world IIoT platforms. For instance, in a smart manufacturing production line, multi-dimensional sensor data from edge devices can be transmitted to the blockchain network via industrial gateways. Agent and voting nodes can be deployed on enterprise servers or edge computing nodes, while supervisory nodes can be realized through trusted third parties or internal audit modules, thereby completing the mapping from the conceptual framework to the operational system.

Second, at the mechanism integration level, the four-party game–based incentive and punishment mechanisms can be embedded into the blockchain system via smart contracts. On platforms such as Hyperledger Fabric or EOSIO, chain codes can dynamically update node reputations and, combined with optimal parameter settings (e.g., penalty coefficients and reputation decay rates) derived from game-theoretic analysis, automatically detect and mitigate abnormal behaviors.

Third, at the incremental deployment level, implementation should begin with small-scale pilots in enterprise private blockchain environments to validate performance in terms of throughput, latency, and security. Subsequently, deployment can be gradually expanded to consortium blockchains or cross-enterprise IIoT applications, such as supply chain traceability and smart energy trading. Operational data collected during this process can be used to iteratively optimize parameters, ensuring evolutionary stability and security in real-world environments.

Finally, at the operations and supervision level, a reputation model combined with behavior-tracking mechanisms can monitor and dynamically isolate malicious nodes. By integrating with enterprise IT/OT security systems, game-theoretic blockchain governance strategies can be embedded into daily operations and compliance management, supporting the long-term sustainable operation of the mechanism.

In summary, this implementation pathway provides a practical blueprint for deploying the improved DPoS mechanism in IIoT scenarios, thereby enhancing the real-world applicability and value of the research.

### D. Discussion on Practical Deployment Constraints

Although the simulation results demonstrate that the improved DPoS outperforms in terms of efficiency, security, and scalability, several challenges remain in real-world industrial IoT deployments. First, terminal devices typically have limited computing and storage capabilities, making it impractical for them to directly participate in the full consensus process;

this highlights the need for lightweight consensus solutions. Second, heterogeneous network environments may introduce latency and packet loss, which can hinder block propagation and synchronization efficiency. Third, many edge devices are highly sensitive to energy consumption, necessitating strategies to reduce the energy cost of consensus without compromising security. Finally, large-scale node participation increases both storage and communication overhead, requiring optimization approaches such as sharding, sidechains, or cross-chain mechanisms to improve scalability. In summary, the practical deployment of the improved DPoS still calls for further refinement in areas including lightweight design, network adaptability, energy efficiency, and cross-chain scalability to enable secure and efficient large-scale applications.

### E. Limitations

Although the four-party game model proposed in this study demonstrates good robustness and adaptability in simulations, its effectiveness in large-scale real industrial scenarios requires further verification.

## VII. Conclusions

This paper presents an improved DPoS consensus mechanism tailored for IIoT scenarios. By constructing a four-party evolutionary game model, it systematically captures the dynamic interactions among different types of nodes and introduces incentive and penalty strategies to reinforce system stability. Simulation results confirm that the proposed mechanism delivers superior performance in efficiency, scalability, and security, thereby strengthening blockchain-based data management in complex IIoT environments. The findings offer both solid theoretical support and practical guidance for advancing secure and efficient industrial applications. Future research will focus on extending the modeling of diverse types of malicious behaviors and examining their empirical applications in cross-industry IIoT scenarios, with the aim of enhancing the adaptability and generalizability of the proposed model.

## References


[1] A. Dwivedi, D. Agrawal, A. Jha, and K. Mathiyazhagan, "Studying the interactions among industry 5.0 and circular supply chain: Towards attaining sustainable development," *Computers & Industrial Engineering*, vol. 176, p. 108927, 2023, doi: 10.1016/j.cie.2022.108927.

[2] K. N. Zhang, C. K. M. Lee, and Y. P. Tsang, "Stateless blockchain-based lightweight identity management architecture for industrial iot applications," *IEEE Transactions on Industrial Informatics*, vol. 20, no. 6, pp. 8394–8405, 2024, doi: 10.1109/TII.2024.3367364.

[3] L. P. Li, X. Zhao, J. F. Fan, F. C. Liu, N. Liu, and H. Zhao, "A trustworthy security model for iiot attacks on industrial robots," *Future Generation Computer Systems*, vol. 153, pp. 340–349, 2024, doi: 10.1016/j.future.2023.11.027.

[4] K. P. Yu, L. Tan, C. X. Yang, K.-K. R. Choo, A. K. Bashir, J. J. P. C. Rodrigues, and T. Sato, "A blockchain-based shamir's threshold cryptography scheme for data protection in industrial internet of things settings," *IEEE Internet of Things Journal*, vol. 9, no. 11, pp. 8154–8167, 2021, doi: 10.1109/JIOT.2021.3125190.

[5] J. Wang, J. H. Chen, Y. J. Ren, P. K. Sharma, O. Alfarraj, and A. Tolba, "Data security storage mechanism based on blockchain industrial internet of things," *Computers & Industrial Engineering*, vol. 164, p. 107903, 2022, doi: 10.1016/j.cie.2021.107903.

[6] Y. J. Ren, X. Y. Liu, P. K. Sharma, O. Alfarraj, A. Tolba, S. Q. Wang, and J. Wang, "Data storage mechanism of industrial iot based on lrc sharding blockchain," *Scientific Reports*, vol. 13, no. 1, p. 2746, 2023, doi: 10.1038/s41598-023-29917-x.

[7] J. Sengupta, S. Ruj, and S. Das Bit, "Fairshare: Blockchain enabled fair, accountable and secure data sharing for industrial iot," *IEEE Transactions on Network and Service Management*, vol. 20, no. 3, pp. 2929–2941, 2023, doi: 10.1109/TNSM.2023.3239832.

[8] P. C. Yao, B. J. Yan, T. Yang, Y. B. Wang, Q. Yang, and W. H. Wang, "Security enhanced operational architecture for decentralized industrial internet of things: A blockchain-based approach," *IEEE Internet of Things Journal*, vol. 11, no. 6, pp. 11 073–11 086, 2023, doi: 10.1109/JIOT.2023.3329352.

[9] P. Liu, Y. Q. Xian, C. J. Yao, P. Wang, L.-e. Wang, and X. X. Li, "A trustworthy and consistent blockchain oracle scheme for industrial internet of things," *IEEE Transactions on Network and Service Management*, vol. 21, no. 5, pp. 5135–5148, 2024, doi: 10.1109/TNSM.2024.3399837.

[10] G. Rathee, C. A. Kerrache, C. T. Calafate, and M. S. Halimi, "Secureblock: An ml-blockchain consumer-centric sustainable solution for industry 5.0," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 1452–1462, 2023, doi: 10.1109/TCE.2023.3325419.

[11] L. You, Z. B. Wang, G. R. Hu, C. T. Cao, and L. Li, "An improved model on the vague sets-based dpos's voting phase in blockchain," *IEEE Transactions on Network Science and Engineering*, vol. 10, no. 6, pp. 4010–4019, 2023, doi: 10.1109/TNSE.2023.3279571.

[12] J. Cui, F. Q. Wang, Q. Y. Zhang, C. J. Gu, and H. Zhong, "Efficient batch authentication scheme based on edge computing in iiot," *IEEE Transactions on Network and Service Management*, vol. 20, no. 1, pp. 357–368, 2022, doi: 10.1109/TNSM.2022.3206378.

[13] H. Dutta, S. Nagesh, J. Talluri, and P. Bhaumik, "A solution to blockchain smart contract based parametric transport and logistics insurance," *IEEE Transactions on Services Computing*, vol. 16, no. 5, pp. 3155–3167, 2023, doi: 10.1109/TSC.2023.3281516.

[14] Y. G. Lin, X. M. Wang, H. G. Ma, L. Wang, F. Hao, and Z. P. Cai, "An efficient approach to sharing edge knowledge in 5g-enabled industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 1, pp. 930–939, 2022, doi: 10.1109/TII.2022.3170470.

[15] M. S. Abegaz, H. N. Abishu, Y. H. Yacob, T. A. Ayall, A. Erbad, and M. Guizani, "Blockchain-based resource trading in multi-uav-assisted industrial iot networks: A multi-agent drl approach," *IEEE Transactions on Network and Service Management*, vol. 20, no. 1, pp. 166–181, 2022, doi: 10.1109/TNSM.2022.3197309.

[16] J. S. Wang, R. Zhu, T. Li, F. S. Gao, Q. Wang, and Q. Xiao, "Etc-oriented efficient and secure blockchain: Credit-based mechanism and evidence framework for vehicle management," *IEEE Transactions on Vehicular Technology*, vol. 70, no. 11, pp. 11 324–11 337, 2021, doi: 10.1109/TVT.2021.3116237.

[17] D. Wang, Y. J. Jia, L. Liang, M. X. Dong, and K. Ota, "A game for task offloading in reputation-based consortium blockchain networks," *IEEE Wireless Communications Letters*, vol. 11, no. 7, pp. 1508–1512, 2022, doi: 10.1109/LWC.2022.3177431.

[18] N. Ren and Y. Y. Ma, "Research on evolutionary game and strategy of dpos consensus mechanism improvement." *Journal of Computer Engineering & Applications*, vol. 58, no. 12, 2022, doi: 1002-8331(2022)58:12¡102:DGSJZG¿2.0.TX;2-V.

[19] Y. T. Liu, X. J. Wang, G. F. Zheng, X. Wan, and Z. L. Ning, "An aoi-aware data transmission algorithm in blockchain-based intelligent healthcare systems," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 1180–1190, 2024, doi: 10.1109/TCE.2024.3365198.

[20] D. Wang, Y. J. Jia, M. X. Dong, K. Ota, and L. Liang, "Blockchain-integrated uav-assisted mobile edge computing: Trajectory planning and resource allocation," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 1, pp. 1263–1275, 2024, doi: 10.1109/TVT.2023.3306740.

[21] Q. Y. Zhu, A. K. Jing, C. Q. Gan, X. W. Guan, and Y. Z. Qin, "Hcsc: A hierarchical certificate service chain based on reputation for vanets," *IEEE Transactions on Intelligent Transportation Systems*, vol. 24, no. 6, pp. 6123–6145, 2023, doi: 10.1109/TITS.2023.3250279.

[22] L. You, Z. B. Wang, G. R. Hu, C. T. Cao, and L. Li, "An improved model on the vague sets-based dpos's voting phase in blockchain," *IEEE Transactions on Network Science and Engineering*, vol. 10, no. 6, pp. 4010–4019, 2023, doi: 10.1109/TNSE.2023.3279571.

[23] H. Lin and J. Z. Du, "Sp-dewoa: An evolutionary distributed witness node election method for delegated proof of stake," *IEEE Internet of Things Journal*, vol. 12, no. 3, pp. 3003–3016, 2025, doi: 10.1109/JIOT.2024.3476248.

[24] G. X. Xu, Y. Liu, and P. W. Khan, "Improvement of the dpos consensus mechanism in blockchain based on vague sets," *IEEE Transactions*

*on Industrial Informatics*, vol. 16, no. 6, pp. 4252–4259, 2020, doi: 10.1109/TII.2019.2955719.
[25] D. Wang and X. H. Zhang, "Secure ride-sharing services based on a consortium blockchain," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2976–2991, 2020, doi: 10.1109/JIOT.2020.3023920.
[26] Y. Li, C. H. Xia, C. Y. Li, Y. Zhao, C. Chen, and T. B. Wang, "Hl-dpos: An enhanced anti-long-range attack dpos algorithm," *Computer Networks*, vol. 249, p. 110473, 2024, doi: 10.1016/j.comnet.2024.110473.
[27] Y. Z. Wei, Q. Xu, and H. Peng, "An enhanced consensus algorithm for blockchain," *Scientific reports*, vol. 14, no. 1, p. 17701, 2024, doi: 10.1038/s41598-024-68120-4.
[28] J. Mišić, V. B. Mišić, and X. Chang, "Towards decentralization in dpos systems: election, voting and leader selection using virtual stake," *IEEE Transactions on Network and Service Management*, vol. 21, no. 2, pp. 1777–1790, 2023, doi: 10.1109/TNSM.2023.3322622.
[29] T. Zhao and Z. X. Liu, "A novel analysis of carbon capture and storage (ccs) technology adoption: An evolutionary game model between stakeholders," *Energy*, vol. 189, p. 116352, 2019, doi: 10.1016/j.energy.2019.116352.
[30] D. Wang, Y. J. Jia, L. Liang, M. X. Dong, and K. Ota, "A game for task offloading in reputation-based consortium blockchain networks," *IEEE Wireless Communications Letters*, vol. 11, no. 7, pp. 1508–1512, 2022, doi: 10.1109/LWC.2022.3177431.
[31] Y. R. Chen, Y. Y. Zhang, S. W. Wang, F. Wang, Y. Li, Y. M. Jiang, L. Y. Chen, and B. Guo, "Dim-ds: Dynamic incentive model for data sharing in federated learning based on smart contracts and evolutionary game theory," *IEEE Internet of Things Journal*, vol. 9, no. 23, pp. 24 572–24 584, 2022, doi: 10.1109/JIOT.2022.3191671.
[32] L. L. Zhu, J. M. Rong, and S. Y. Zhang, "Three-party evolutionary game and simulation analysis of drug quality supervision under the government reward and punishment mechanism," *Chinese Journal of Management Science*, vol. 29, no. 11, pp. 55–67, 2021.

**Wencheng Chen** (Graduate Student Member, IEEE) received the M.S. degree from Fujian University of Technology, China. He is pursuing the Ph.D. degree in the College of Electrical Engineering and Automation, Fuzhou University, China. His research interests include blockchain, Internet of Things, cryptographic accumulator, edge computing, and game theory.

**Jun Wang** (Senior Member, IEEE) received the B.S. and M.S. degrees in communication and information systems from Hohai University, Nanjing, China, in 2003 and 2006, respectively, and the Ph.D. degree in communication and information systems from Southeast University, Nanjing, in 2012. He is currently a Faculty Member with the College of Electrical Engineering and Automation, Fuzhou University, Fuzhou, China. He is also a member of Fujian Integrated Circuits Design Center. His current research interests include statistical signal processing, cyclostationary signal analysis, ultra-wide band wireless communication, and cognitive radios.

**Jeng-Shyang Pan** (Senior Member, IEEE) is a Professor and Doctoral Supervisor at the School of Artificial Intelligence, Nanjing University of Information Science and Technology. He received his Ph.D. in Electrical Engineering from the University of Edinburgh, UK(1996), after earning an M.S. in Telecommunications from National Chiao Tung University (1988) and a B.S. in Electronics from Taiwan University of Science and Technology (1986). A Fellow of the Institution of Engineering and Technology (IET, UK) and a recipient of China's National Distinguished Experts Program (2010), he has published over 800 papers (500+ SCI-indexed, H-index 81, citations 26,000). His research spans artificial intelligence, signal processing, and neural computing. He holds 80 patents, has authored 8 monographs, and edited 70+ conference proceedings. Prof. Pan has led multiple grants, including NSFC projects, an 863 Program sub-project, and major provincial initiatives in Fujian and Shan- dong. He has served as Guest Editor for 20+ SCI/EI journals, including Information Sciences and Neural Computing. His awards include a gold medal at the 25th International Invention Show (Pittsburgh, 2010) and recognition as a Highly Cited Scholar in China.

**R. Simon Sherratt** (Fellow, IEEE) is currently a Professor of Biomedical Engineering at the University of Reading, UK. Professor Simon Sherratt received the B.Eng. From Sheffield City Polytechnic (now Sheffield Hallam University), M.Sc. from The University of Salford, and Ph.D. from The University of Salford; he was elected as Fellow of the IEEE in 2012, Fellow of the IET in 2009; Senior Fellow of the Higher Education Academy in 2014. He is a Chartered Engineer (C.Eng.) and registered European Engineer (Eur Ing). Professor Simon Sherratt was awarded the IEEE International Symposium on Consumer Electronics (ISCE) 2006 1st Place Best Paper Award: IEEE Chester Sall Award for best papers in the IEEE Transactions on Consumer Electronics in 2006, 2016, 2017, 2018. He has published over 200 articles in peer review journals and international conferences. His research area is wearable devices, mainly for healthcare and emotion detection.

**Jin Wang** (Senior Member, IEEE) received the B.S and M.S. degree from Nanjing University of Posts and Telecommunications, China in 2002, 2005 respectively. He received Ph.D. degree from Kyung Hee University Korea in 2010. Now, he is a professor at Hunan University of Science and Technology. He has published more than 400 international journal and conference papers. His research interests mainly include Internet of Things (IoT), data center networks, network performance analysis and optimization etc. He is a Fellow of IET and a senior member of the IEEE.