




Info-Chain: Reputation-Based Blockchain for Secure Information Sharing in 6G Intelligent Transportation Systems

Kun Yan , *Graduate Student Member, IEEE*, Wenping Ma , *Member, IEEE*, Qi Yang, Shaohui Sun, *Member, IEEE*, and Weiwei Wang , *Graduate Student Member, IEEE*,

Abstract—The widespread deployment of 5G networks has accelerated the development of Internet of Vehicles (IoV), laying the foundation for the development of intelligent transportation systems (ITS) in future 6G networks. The unprecedented intelligence of 6G ITS is expected to enable the automation of vehicles, seamless collaboration, and intelligent management. High-volume information sharing plays a crucial role in this case, and its security and reliability becoming important cornerstones for 6G ITS. Without adequate security protection and trusted environments may result in unreliable and inefficient network services. In this article, we propose a reputation management-based blockchain, Info-Chain, for secure, trustworthy, and privacy-preserving information sharing in 6G ITS. Furthermore, to accommodate the distributed traffic environment in 6G ITS, we construct a novel consensus mechanism for Info-Chain, denoted as Proof of Reputation and sum (PoRs), which combines reputation with traffic environmental factors as competitive conditions. Finally, we propose a dynamic incentives and punishments mechanism that utilizes evolutionary game theory to guide vehicles to actively and honestly participate in information sharing. The security analysis shows that the proposed mechanism is capable of resisting common attacks, and the simulation result demonstrates that the proposed scheme not only enables efficient and secure information sharing in 6G ITS, but also encourages vehicles to actively participate in information sharing.

Index Terms—Information sharing, blockchain, reputation management, evolutionary game theory, intelligent transportation systems (ITS), 6G networks.

I. INTRODUCTION

5G networks brings state-of-the-art communication infrastructure to the transportation system, making vehicle-to-network collaboration a reality. To enable a variety of intelligent transportation services in future 6G networks, large-scale information sharing is essential [1]. Therefore, it is very necessary to ensure the credibility, uniqueness, integrity, and privacy of information sharing. Meanwhile, barriers to information sharing include unwillingness, fear, and inability to share. The motivation of users to share information is

influenced by the development of mutual trust relationships and the potential economic benefits of information sharing [2].

In traditional transportation information sharing, a centralized control approach is adopted, where a centralized node collects information from transportation and then trades or broadcasts it. The authority of the centralized node makes it a central hub for information sharing. Zhang *et al.* [3] utilized ciphertext-policy attribute-based encryption to achieve secure and controllable centralized cloud data storage, ensuring secure data sharing in the IoV. However, in the vast intelligent transportation network of 6G, the change in network structure may transform the single large centralized node into multiple co-maintained nodes, or even lead to decentralization. This requires further discussion on the security implications of relying on the centralized node. To encourage users to participate in traffic view information sharing, Wang *et al.* [4] proposed a crowdsourcing-based traffic view reporting system. This system allows the centralized node to collect traffic views while rewarding the users accordingly. Duo to the lack of association between the information and its sender, it is impossible to guarantee that the sender won't send second-hand information to gain benefits. The trustworthiness of information serves as the foundation for ensuring effective information sharing. To address this issue, Guo *et al.* [5] proposed a context-aware trust management model, which evaluates the trustworthiness of information during vehicle interactions. Merely proving the trustworthiness of information alone cannot enhance the secure sharing of information; therefore, it is necessary to employ reputation mechanisms to guide users.

Blockchain, as an open, anonymous, and tamper-proof distributed database, addresses the challenge of establishing trust among unfamiliar entities. Its security relies on its consensus mechanism rather than the trust of centralized nodes, which makes blockchain widely recognized as one of the most promising technologies for 6G networks [6]. Unlike ITS that solely rely on distributed servers, which lack secure interaction and synchronization between servers, by integrating blockchain with it, the same reliable computation, efficient access, and secure storage can be carried out between different servers [7]. This integration enhances the utilization of infrastructure and resources within ITS, meeting the demand for information sharing and security among distributed vehicles. While the traditional blockchain establishes an equitable and trustworthy interaction environment, it falls short of meeting

Manuscript received April 19, 2023. This work was supported in part by the Key Industry Innovation Chain Project of Shaanxi Provincial Science and the Technology Department, China under Grant 2022ZDLGY03-08. (Corresponding author: Wenping Ma.)

Kun Yan, Wenping Ma, Qi Yang, and Weiwei Wang are with the School of Telecommunications Engineering, Xidian University, Xi'an 710071, China (e-mail: kyan@stu.xidian.edu.cn; wp_ma@mail.xidian.edu.cn; qi_yang@stu.xidian.edu.cn; wweiwei@stu.xidian.edu.cn).

Shaohui Sun is with the Datang Mobile Communications Equipment Co., Ltd, Beijing 100083, China (e-mail: sunshaohui@catt.cn).

the requirement for a trusted environment for information sharing in ITS. Consequently, the implementation of an enhanced reputation system within blockchain-based ITS is essential. This can help users in the network to overcome concerns about message uncertainty and communication risks [8]. Moreover, the integration of blockchain and trust can create a highly reliable transportation information system by associating users and sharing information.

Recently, the integration of blockchain and reputation management has received tremendous attention from researchers. To reduce the burden of traditional consensus mechanisms on computing power and communication in IoV, Yan *et al.* [9] proposed a reputation-based blockchain consensus mechanism, while reputation was used as an endorsement to verify the accuracy of information through Bayesian inference. Cui *et al.* [10] leveraged the consortium blockchain to achieve traceability and immutability of shared data records, and prevent the propagation of erroneous or meaningless information. Additionally, trust management was used to improve the availability and credibility of shared information. Yan *et al.* [11] proposed a novel blockchain-based decentralized system, Social-Chain, for trust evaluation in Pervasive Social Networking, while the traditional consensus mechanism was replaced by Proof-of-Trust to enhance the efficiency of the system.

The complementarity of blockchain and reputation management has become an important part of research on distributed network information sharing, but three main issues remain:

Blockchain and reputation management are relatively independent. Although existing research uses blockchain to ensure information security and reputation management to ensure information credibility, there has been no deep integration between the two. This can result in the reputation value of the information owner not being able to directly represent the credibility of the information they transmit.

Traditional blockchain is applied to new scenarios without considering compatibility. Applying traditional blockchain to non-financial scenarios may result in lower applicability due to changes in consensus mechanisms, node types, block structures, and other factors.

Privacy issues related to reputation management. Reputation verification should be performed on the identity of each communication party to assure that their reputation is genuine, under the protection of the privacy of both parties.

To solve the above issues, we propose Info-Chain, a information sharing scheme suitable for 6G ITS, which is based on blockchain and reputation management. In Info-Chain, blockchain is utilized to record the information sharing to ensure secure and effective information sharing; reputation management assigns reputation values to vehicles to ensure trustworthy information sharing. The main contributions of this article are summarized as follows:

- We propose a new blockchain-based information sharing scheme called Info-Chain for 6G ITS, which can provide secure information interaction and trust management while protecting vehicle privacy.
- We extensively integrate blockchain and reputation to introduce a novel reputation-based distributed consensus mechanism named PoRs. Unlike other reputation-based

consensus, it incorporates traffic environmental factors into the consensus. This modification enhances the relevance of Info-Chain to ITS while simultaneously maintaining the randomness and security of the consensus.

- We develop a distinctive reputation verification mechanism utilizing the verifiable random functions (VRF). It correlates between reputation values and vehicle identities while protecting privacy, thus effectively enhancing the trustworthiness of shared information.
- We propose an incentives/punishments mechanism for promoting information sharing in 6G ITS, based on evolutionary game theory. It is an enhancement of Info-Chain, effectively encouraging honest sharing among vehicles and facilitating the flow of useful information.

The remainder of this article is structured as follows. We present review related work in Section II. In Section III, we briefly describe the proposed system model and assumptions. In Section IV, we state a detailed description of Info-Chain. In Section V, we design Info-Chain based privacy-preserving information sharing in 6G ITS. In Section VI, we analyze the security as well as the computation and communication complexity of the proposed scheme. Then, we present the simulation results in Section VII. Finally, the conclusion of this article is obtained in Section VIII.

II. RELATED WORK

In this section, we introduce the vision of ITS in 6G networks, and elaborate on the importance of information sharing in ITS.

A. Views of ITS in 6G networks

It is envisioned that 6G networks will bring extremely advanced communication experiences to ITS. Vehicle to Everything (V2X) in 5G NR inherits the underlying mechanisms and system architecture of V2X in LTE, while adding research in spectrum and hardware resources [12]. More crucially, the continuous construction and development of smart cities, as well as the intelligence of transportation facilities, will present a spurt of growth. The emerging service demands bring significant challenges for V2X [13]. Additionally, almost all information sharing studies in current traffic scenarios are primarily focused on the communication level, such as ensuring the stability of communication connections, improving the rate of communication, enhancing the throughput of system communication, and so on. This can only provide limited intelligent services and make 5G NR-based V2X potentially inadequate for the dazzling demands of ITS. As a disruptive technology, 6G networks will not only be an exploration and evolution in communication and network, but also a deep integration of artificial intelligence and traditional communication network technologies [14]. The goal of it is to build a distributed intelligent network with a space-air-ground-underwater integrated network architecture [15]. It has the potential to completely revolutionize ITS applications and services in ways that were previously thought impossible.

In the future 6G networks, a brand new communication method with ultra-reliable and low latency will produce by

the interweaving of visible light communication and wireless communication. It provides possibilities for remotely driving drones, vehicles, and other transportation facilities without discrimination, and cybertwin-driven ITS without delay will also become a reality [16], [17]. At the same time, it brings diversity in information sharing to future transportation scenarios [18]. Empowered by artificial intelligence, the cloud-edge-end collaborative 6G ITS can unload data collected by vehicles to the cloud or edge devices for computing, paving the way for extremely intelligent autonomous driving and integrated vehicle collaboration [16], [19]. The super-aware sensor can give vehicles a 360-degree view within a range of 300 meters, enabling a more precise collection of traffic information. At the same time, it allows real-time information sharing to build highly accurate maps and create an intelligent driving experience [20]. The mobile speed of devices supported by 6G networks can reach up to 1000km/h, making stable communication between satellites, drones, and ground vehicles, as well as cooperation in implementing air-ground traffic linkage, which will become an important part of future rescue scenarios [21].

B. Information Sharing in ITS

As the most promising application scenario in the 6G era, the potential of ITS will be fully unlocked by 6G networks, providing better quality transportation services. Such an intelligent experience is built on the massive information sharing between transportation facilities, including information from sensors, cameras, and communication devices. Therefore, it is important to establish a secure and comprehensive mechanism for safeguarding various types of information sharing.

Information sharing is an indispensable part of ITS. To solve the edge data sharing problem in IoV, Lu *et al.* [22] proposed a hybrid blockchain structure consisting of a permission chain maintained by Road Side Units (RSUs) and a directed acyclic graph maintained by vehicles. It integrated federated learning models into the blockchain and performed two-stage verification to ensure the reliability of shared data. Luo *et al.* [23] proposed a software-defined cooperative data sharing architecture, which includes a sharing data scheduling algorithm in 5G-VANET, to achieve the separation of context-awareness and data transmission. Meanwhile, graph theory is used to schedule collaborative data distribution and achieve continuous data sharing. Zhang *et al.* [24] proposed a data sharing scheme based on ciphertext-policy attribute-based encryption to achieve confidentiality and fine-grained access control for efficient data sharing between cloud and fog in IoV. To motivate users to participate in information sharing, Yin *et al.* [25] proposed a time and resource constrained incentive mechanism to handle crowdsourcing task allocation, and smart contracts were utilized to enable secure crowdsourcing information exchange. Wang *et al.* [26] proposed a secure and efficient information sharing scheme based on blockchain for unmanned aerial vehicle-aided disaster rescue, and designed two-layer incentive algorithms based on reinforcement learning to optimally stimulate vehicles to share their free computing resources.

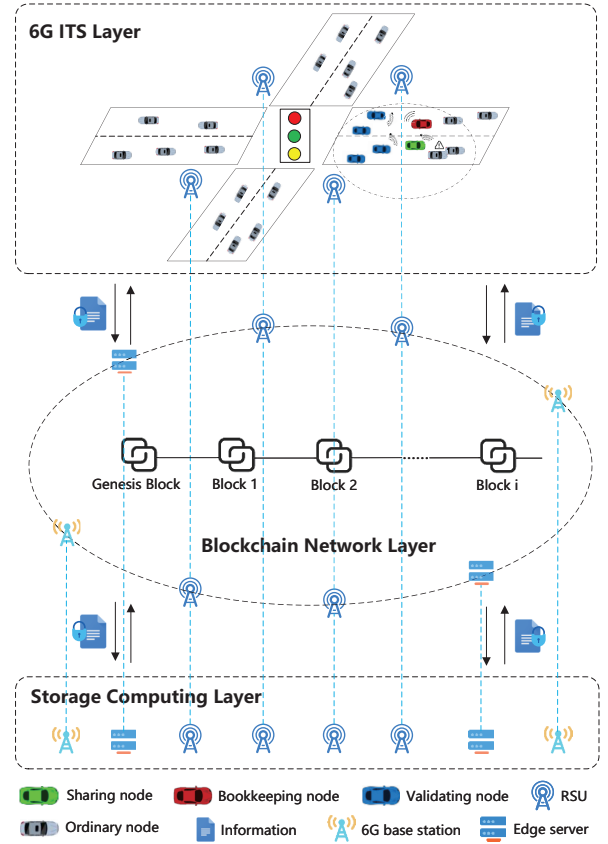


Fig. 1. System model of Info-Chain in 6G ITS.

Motivated by these considerations, we design a new reputation-based blockchain called Info-Chain, and we propose using Info-Chain for information sharing in 6G ITS.

III. MODEL AND OVERVIEW

In this section, we introduce the system model, key definitions, premise assumptions, and threat models, respectively.

A. System Model

The three-layer system model of Info-Chain is shown in Fig. 1.

1) *The 6G ITS Layer*: It comprises vehicles, drones, RSUs, 6G base stations, edge servers, and other transportation infrastructures. Light nodes such as vehicles and drones are equipped with On Board Units (OBU), enabling V2X communication and participation in various activities within the Info-Chain, which include bookkeeping, validating, and packaging. They are the primary contributors to information sharing and are responsible for collecting, reporting, and exchanging traffic information. Full nodes such as RSUs, 6G base stations, and edge servers serve as providers of communication, network, storage, and intelligent services in the 6G ITS. They are responsible for hosting and maintaining the regular operation of the Info-Chain and ensuring the stability and security of the 6G ITS.

2) *The Blockchain Network Layer*: In this layer, Info-Chain and consensus nodes collaborate to validate the collected

sharing information and record it in the blockchain supported by the full nodes. This information is stored as a distributed ledger, which ensures credible and reliable information consistency and tamper-proof. Simultaneously, the embedded reputation model can both restrict and guide light nodes in the network to make more rational behavior while assisting Info-Chain in achieving lightweight consensus.

3) *The Storage Computing Layer*: This layer, primarily composed of full nodes, is the cornerstone of 6G ITS, providing the required basic services for the entire system. Furthermore, after the extensive information in Info-Chain and ITS is de-privatized, and processed by the endogenous artificial intelligence of 6G networks, it can provide faster, more accurate, and more reliable information services for ITS.

B. Key Definitions

In this subsection, we give the definitions of nodes, transactions and blocks of Info-Chain, where nodes refer to vehicles.

Nodes Definition: The light node in Info-Chain is the main active participant for information sharing, and a light nodes N_i is defined based on its role as follows:

$$N_i = \langle ID_i, R_i, Role_i \rangle, \quad (1)$$

where ID_i is the blockchain wallet address obtained by registering and authenticating after the node enters the system, which is used as a pseudonym during communication. R_i represents the node's reputation value. $Role_i$ is the role of the node during the consensus process, mainly divided into four types:

Bookkeeping nodes: The node are used to package blocks and add them to the Info-Chain during the consensus process, which are identified as \mathbb{B} ;

Validating nodes: The node is used to verify the correctness of received transactions or blocks during the consensus process, which are identified as \mathbb{V} ;

Sharing nodes: The node is used to share information in the 6G ITS during the consensus process, which are identified as \mathbb{S} .

Ordinary nodes: The node in the Info-Chain that can participate in the information sharing or consensus process, which are identified as \mathbb{O} .

Transactions Definition: In Info-Chain, transactions are used to record the relevant information of the sharer, encapsulated as the transaction TX , as follows:

$$TX_i = \{ID_i, R_i, I_i, Sig_{sk_i}[H(I_i)]\}, \quad (2)$$

where ID_i , R_i , I_i and sk_i are the blockchain wallet address, reputation value, information, and private key of N_i , respectively. In particular, H is a hash function, $Sig_a(B)$ is a digital signature function utilizing a to sign B .

Blocks Definition: The blocks in Info-Chain mainly contain two types of information: transactions of information sharing and records of reputation updates, Fig. 2. shows the specific structure.

Header	Prehash	Block Height	Timestamp	Signature
Body	Transactions		Reputation Values	

Fig. 2. The block format of Info-Chain.

C. Premise Assumptions

The following assumptions and requirements are applied throughout the article unless otherwise stated.

- 1) The traffic scenario is the city one, with heavy traffic.
- 2) Each vehicle is equipped with GPS, which could perform real-time location inquiries and synchronization.
- 3) One vehicle can only report the identical type of information (happen or not) for the same traffic event.
- 4) After a bookkeeping node has packed a new block, it will be restricted from gaining bookkeeping rights for the next ρ blocks.
- 5) The bookkeeping node and the information sharing node cannot be the same vehicle in the same traffic event.
- 6) Full nodes are connected through reliable communication links. In general, they are trusted and never try to deviate from the pre-defined protocols, but might fail to function properly due to malfunctions.

D. Threat Models

The following types of attacks against blockchain and 6G distributed ITS are considered in information sharing.

Double-spend attacks and fork: A malicious node with high authority enables the reuse of digital currency by initiating a transaction and then revoking it. At the same time, the blockchain is forked, leading to the collapse of the entire system.

Malicious competition attacks: A bookkeeping node improves its competitiveness in the system by constructing a large number of valid transactions, but not broadcasting them externally, and packing them directly into blocks.

Collusion attacks: Some nodes in the system collude to disseminate false information and mislead other nodes, or validating nodes collude to influence the consensus result and cause the blockchain to fork, resulting in the collapse of the entire system.

Self-promoting attacks: Malicious leaders attempt to promote their own and their close nodes' reputation, and then launch an attack at a certain time, breaking the reputation rules within the system.

Bad-mouthing attacks or False-praise attacks: Malicious nodes give unreasonable reputation ratings to other nodes to achieve damage to the reputation system.

Free-ride attacks: Malicious nodes masquerade as participating in system events, but do not provide any valuable work while receiving the same reward as real workers.

Sybil attacks or Whitewashing attacks: Malicious nodes conduct attacks on the system by forging multiple identities, or re-register new identities to conceal the various malicious activities of their old identities.

IV. INFO-CHAIN: THE PROPOSED PROTOCOL

In this section, we present the detailed design of Info-Chain.

A. Reputation Model

The reputation of a node is a quantification of its behaviors and habits in the network. More specifically, it is achieved through mutual evaluation between nodes under the constraints of reputation rules. Additionally, nodes with high reputation value tend to have better behaviors and habits (providing high-quality information and accurate feedback), and vice versa [27]. Considering the highly distributed characteristics of 6G ITS, we adopt a distributed reputation model that improved on PeerTrust [28]. The reputation value of node N_i in the information sharing event e could be calculated as follows:

$$R_i(e) = \alpha_1 \sum_{j=1}^{I(e)} s(j) R_j(e-1) + \alpha_2 F_i(e) + R_i(e-1), \quad (3)$$

where $I(e)$ is the number of nodes that rate the information provided by N_i in event e , $s(j)$ is the feedback of N_j to the received information, $R_i(e-1)$ and $R_j(e-1)$ are the current reputation value of N_i and N_j , $F_i(e)$ is the result of the system's reward/punishment of N_i in event e including RS_i or RC_i , α_1, α_2 are weight factors, where $0 < \alpha_1 < \alpha_2$, and $\alpha_1 + \alpha_2 = 1$. Moreover, i, j , and e are all greater than 0.

As the feedback factor, $s(j)$ is used to measure the value of the information provided by N_i . we assign reputation scores of $\{-3, -2, -1, 0, 1, 2, 3\}$ to decisions ranging from worst, bad, poor, unknown, fair, good, and excellent, respectively. This 7-point decision allows a fine-grained classification of feedback similarity to distinguish between honest and malicious feedback. In essence, the 7-point decision is optimal in reliability, validity, and discriminating power compared to decisions with lower or higher than 7-point [29].

To guarantee the usefulness and trustworthiness of shared information, a reputation threshold R_r is set. When $R_i < R_r$, N_i cannot share information or become a bookkeeping node, and need to improve its reputation by actively participating in consensus work.

B. System Interaction

The information sharing in 6G ITS based on Info-Chain is illustrated in Fig. 3. When an event occurs in the traffic environment, the sharing nodes report the event to the blockchain network. Once consensus nodes verify this information and reach a consensus decision, the information will be packaged into a new block and stored in Info-Chain. Simultaneously, aided by the reputation model, nodes engaging in sharing and consensus will also obtain corresponding reward/punishment. The detailed process will be described in the following subsections.

C. System Initialization

In the initial phase, vehicle V_i obtains its blockchain identity by submitting real identity information ID_i , such

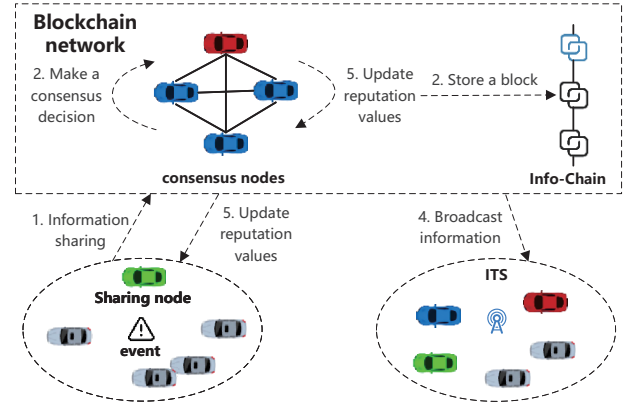


Fig. 3. Info-Chain based ITS information sharing.

as driver identity and vehicle identity, to register as a node in the Info-Chain. This blockchain identity includes the public key PK_i , private key SK_i , communication (wallet) address CA_i , and initial reputation value $R_i(0)$. Subsequently, these components are mapped to a blockchain wallet $\{ID_i, PK_i, SK_i, CA_i, R_i(0)\}$ and stored within the vehicle. Simultaneously, the hash value of the data collected during the vehicle registration process is stored separately on the server to ensure the privacy of the vehicle. Due to the absence of the necessary blockchain identities for communication, unregistered vehicles cannot engage in information sharing based on the Info-Chain.

The initial reputation value of nodes can be calculated using the weighted evaluation, as follows:

$$R_i(0) = \beta_1 DA_i + \beta_2 VA_i + \beta_3 VV_i, \quad (4)$$

where DA_i is the driver's driving age (the longer the driving age represents the better behavior of the driver), VA_i is the vehicle's age (the smaller vehicle's age represents the better condition the vehicle), VV_i the vehicle's violations within one year (the more violations represent the poorer driving behavior), $\beta_1, \beta_2, \beta_3$ are weight factors, and $\beta_1 + \beta_2 + \beta_3 = 1$.

D. Bookkeeping Nodes Selection

The most significant driving force in the blockchain is the consensus mechanism. When designing a consensus mechanism, it is important to consider many factors including network environment, service scenarios, performance requirements, and bonus-penalty mechanisms. For Info-Chain, PoRs is proposed to jointly all these aspect.

In PoRs, the reputation value of nodes is used as an endorsement for selecting bookkeeping nodes. A novel lightweight bookkeeping nodes competition mechanism based on reputation is established for Info-Chain, which allows nodes in 6G distributed ITS to prove themselves independently. The PoRs consensus mechanism is processed following Algorithm 1.

Due to the real-time and regional nature of the information in 6G ITS, the bookkeeping node also undertakes the work of verifying the accuracy of the information while packaging transactions. Therefore, the selection of bookkeeping nodes in

Algorithm 1 Bookkeeping Nodes Selection**Input:** $R_i(e-1)$, $D_i(e)$, $S_i(e)$, R_r , γ_1 , γ_2 , γ_3 , ζ , λ **Output:** The bookkeeping node BN_i

```

1: if  $R_i(e-1) < R_r$  then
2:    $N_i$  cannot become a bookkeeping node
3: else
4:   Calculate the evaluation value  $E_i(e)$  of  $N_i$  according to (5)
5:   Calculate the waiting time  $T_i(e)$  of  $N_i$  with  $E_i(e)$  according to (6)
6:   Start-up waiting time  $T_i(e)$  as a countdown
7:   if the countdown of  $N_i$  ends first then
8:      $N_i$  is the bookkeeping node  $BN_i$ 
9:   end if
10: end if
11: return  $BN_i$ 

```

PoRs takes into account the reputation value while introducing other traffic environmental factors as the comprehensive evaluation basis for the bookkeeping right. However, it is instructive to note that 6G networks will grow more heterogeneous in the foreseeable future, which may result in an inversely proportional relationship between some factors and evaluation results. Therefore, it is necessary to take the reciprocal of these data to achieve homogenization. Weight evaluation is used for multi-parameter evaluation, as follows:

$$E_i(e) = \gamma_1 R_i(e-1) + \gamma_2 \frac{1}{D_i(e)} + \gamma_3 S_i(e), \quad (5)$$

where $R_i(e-1)$ is the current reputation value of N_i , $D_i(e)$ is the distance between N_i and the information sharer, $S_i(e)$ is the success rate of N_i 's information transmission, γ_1 , γ_2 , γ_3 are used as weights to adjust the impact of different parameter weights on the results, where $\gamma_1 > \gamma_2 > \gamma_3 > 0$, and $\gamma_1 + \gamma_2 + \gamma_3 = 1$.

In contrast to other reputation-based consensus algorithms [9], [11] that merely use traditional centralized sorting methods to select bookkeeping nodes, to ensure distributed consensus, the exponential distribution is used in PoRs to map $E_i(e)$ as the waiting time $T_i(e)$ for consensus, as follows:

$$T_i(e) = \zeta \lambda e^{-\lambda E_i(e)}, \quad (6)$$

where ζ is a preset parameter to adjust the waiting time, so that it is one order of magnitude smaller than the PoRs main algorithm running time, which reduces the impact of $T_i(e)$ on the efficiency of PoRs, λ refers to the parameter in the exponential distribution.

In this case, the higher the reputation value of a node, the larger the $E_i(e)$, and the smaller the $T_i(e)$, thus, the node whose waiting time ends first is the bookkeeping node.

E. Block Generation

It is inevitable that a large volume of information will be shared in 6G ITS. When a traffic event occurs (e.g., traffic jams, traffic accidents, temporary control, HD map collection, crowdsourcing task, etc.), relevant information will be shared

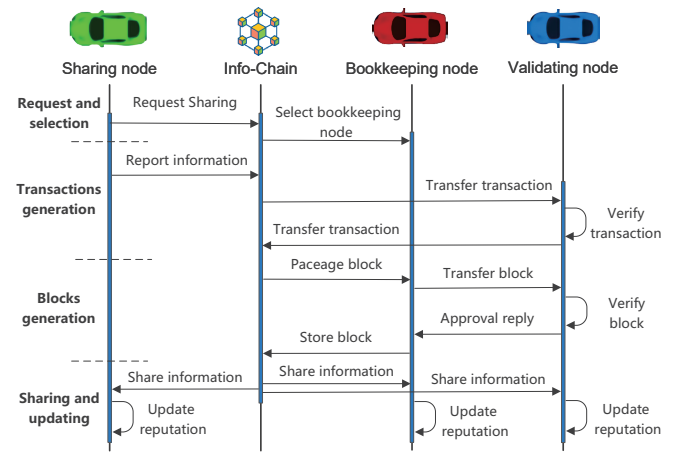


Fig. 4. Block generation process of Info-Chain.

and recorded in Info-Chain, as shown in Fig. 4. The detailed steps of block generation are as follows:

Step 1 (Request and selection): When an ordinary node detects a traffic event in 6G ITS, it will request to share information and prepare to report the shared information. Afterward, its role will change to a sharing node. After the nearby RSU receives the request, the system selects bookkeeping nodes based on traffic environmental factors and node reputation values.

Step 2 (Transactions generation): Once the information sharing is reported, the sharing node and related information will be packaged by the system into transaction TX , which contains the signature of the information by sharing node using its private key. Then the TX will be transmitted to validating nodes via RSUs. When a TX is received by a validating node, the signature of the transaction will be verified. If the verification result is correct, it will be marked and sent to the transaction pool, otherwise, it will be invalidated.

Step 3 (Block generation): Considering the timeliness of information, after a TX is generated, within a specified period, regardless of whether the TX has been verified by validating nodes, the bookkeeping node will personally verify the legitimacy of the TX and the authenticity of the information. Transactions containing true information will be packaged into new blocks. The validating nodes verify the new blocks received, including the signature, timestamp, legitimacy of participating consensus node identity, and reputation of the participating consensus nodes, then return the result to the bookkeeping node, and the correct blocks will be stored in Info-Chain.

Step 4 (Sharing and updating): After the block is stored, the information will be shared in 6G ITS through RSUs, the nodes that received the shared information need to rate the information. Then the reputation of all nodes involved in this information sharing and consensus work will be updated based on the rating and reward/punishment results.

F. Bonus-penalty

For the bookkeeping and validating nodes, (7) is leveraged to calculate rewards using the logarithmic rate of return.

Meanwhile, nodes participating in consensus have the potential to launch attacks, and in order to eliminate this situation, the reputation-based penalty mechanism is set to $-l$ times ($l > 1$) the reward for honest participation in consensus.

$$RC_i = \xi \ln [1 + (\sigma_1 CV_i + \sigma_2 CN_i)], \quad (7)$$

where CV_i and CN_i are the volume and number of communication, ξ , σ_1 , and σ_2 are preset parameters, and $\sigma_1 + \sigma_2 = 1$.

G. Node Departure

In the Info-Chain, there are two main reasons for a node to depart the system. On one hand, a node may voluntarily revoke its blockchain identity if it no longer wishes to participate in information sharing. In this scenario, the node submits a deregistration request. Subsequently, the system will recover and eliminate the associated blockchain wallet. On the other hand, if a node repeatedly shares false information, resulting in a substantial degradation of its reputation, the system will revoke the node's blockchain wallet, thus preventing its involvement in any activities within the system.

V. PRIVACY-PRESERVING INFORMATION SHARING BASED ON INFO-CHAIN

In this section, we focus on verifying the reputation value of sharer under privacy-preserving, and incentives/punishments mechanisms for information sharing.

A. Trusted Interaction based on VRF

In 6G ITS, vehicles communicate under pseudonyms to preserve their privacy. However, it is not possible to validate a vehicle's reputation value with its identity information, even though both are stored in the Info-Chain. To address this issue, we propose to verify the reputation value of the sharer before formal information sharing. This makes it feasible to verify the reputation value of sharer and ensure the reliability of shared information. Meanwhile, the VRF [30] is utilized in this process to ensure randomness, uniqueness, and verifiability.

As a pseudo-random function, VRF takes the prover's private key and arbitrary random information as input, and outputs a hash and a proof. This allows the possibility of using the public key corresponding to the private key to verify that the hash is generated by the prover. Since the hash is determined uniquely by both the prover's private key and the random information, VRF can ensure that the private key holder can prove the correctness of their output [31].

In the traffic event e , we consider vehicle V_A as the information sharer and V_B represents the vehicle participating in the consensus. Before the information is shared, the specific process of consensus V_B to determine the reputation value of V_A is as follows:

Step 1: V_A generates the hash and proof of the signature of reputation value by binding its private key to current reputation value using (8) and (9).

$$result_A^e = VRFs_Hash(sk_A || Sig_{sk_A}[R_A]), \quad (8)$$

and

$$proof_A^e = VRFs_Proof(sk_A || Sig_{sk_A}[R_A]), \quad (9)$$

where sk_A and R_A are the private key and current reputation value of V_A , respectively.

Step 2: V_A packages its public key, current reputation value, the signature of reputation value, the hash and proof of the signature of reputation value as $\langle pk_A, R_A, Sig_{sk_A}[R_A], result_A^e, proof_A^e \rangle$, and sends it to V_B .

Step 3: After $\langle pk_A, R_A, Sig_{sk_A}[R_A], result_A^e, proof_A^e \rangle$ is received, V_B uses (10) to calculate whether the result and proof of the signature of V_A 's reputation value match.

$$result_A^e = VRFs_P2H(proof_A^e). \quad (10)$$

Step 4: If step 3 is successful, V_B uses (11) to verify whether there is a unique correspondence between the signature of V_A 's reputation value and $proof_A^e$. If it succeeds, it returns true, otherwise it returns false.

$$True/False = VRFs_Verify(pk_A || Sig_{sk_A}[R_A] || proof_A^e). \quad (11)$$

The VRF can generate the same result and corresponding proof only if the input private key and the reputation value are identical. Therefore, if step 4 returns true, it confirms that the signature of V_A 's reputation value belongs to itself. Meanwhile, the reputation of vehicles is stored in the Info-Chain, which can avoid the possibility of V_A forging its reputation value.

B. Incentives and Punishment Mechanism

The main purpose of the incentive and punishment mechanism is to guide more vehicles in 6G ITS to share information honestly and reliably, while motivating vehicles to participate in information sharing. Whether vehicles participate or not in information sharing depends on their own rationality, learning ability, competitiveness, and incentive [32]. Generally speaking, they continuously adjust their strategies through exploration and experimentation. Therefore, an incentive model based on reputation-based evolutionary game theory can be established to explore a way to continuously adjust vehicles' expectations of participation in information sharing according to the current state.

1) Model and Payoff Matrix: The reputation-based information sharing incentive evolutionary game model is a quaternion array $G = (P, N, S, U)$, where:

- P : Each vehicle in the system is a player of the game and can dynamically choose whether to share the traffic information, suppose vehicles participating in the game are vehicles V_A and V_B ;
- N : a collection of individual vehicles
- S : The vehicle's strategy space $S = (s_1, s_2) = (\text{share}, \text{not share})$ in the game, in which vehicles are free to choose their strategies.
- U : The payoff matrix generated by the participating parties in the game, as shown in Table I.

TABLE I
PAYOFF MATRIX FOR PARTICIPATION IN INFORMATION SHARING

The strategy of V_A	The strategy of V_B	
	Share	Not share
Share	$\omega_A Q_A - C_A, \omega_B Q_B - C_B$	$Q_A - C_A, 0$
Not share	$0, Q_B - C_B$	$0, 0$

Since vehicles in this mechanism can only choose to share or not, the game process between V_A and V_B conforms to the “general two-person symmetric game” [33], so it can be analyzed using the same method. In order to make the evolutionary game analysis clearer, V_i is used to denote the vehicles involved in the game. C_i represents the cost of V_i in information sharing, and (12) is utilized to calculate the benefit of V_i in the game. This formula indicates that the vehicle’s benefit is positively related to the reputation value and negatively related to the time when the shared information is sent. In general, the higher the vehicle’s reputation value, the higher the credibility of the information shared. At the same time, a timing mechanism is introduced to prevent vehicles from sharing second-hand information and balance benefits.

$$Q_i = \eta_1 \ln[1 + R_i(e - 1)] + \eta_2 e^{-T_i}, \quad (12)$$

where $R_i(e - 1)$ is the current reputation value of V_i in the traffic event e , T_i is the transmission time difference between the information sent by V_i and the first information, η_1 and η_2 are scaling parameters, and $\eta_1 + \eta_2 = 1$.

2) *Dynamic Equation*: Assuming that all vehicles in 6G ITS form a group N , the probability of sharing information at time t is x , and the probability of not sharing is $1 - x$. On the basis of the payoff matrix in Table I and the rules of evolutionary game theory [34], the expected benefits for V_i to choose whether to share information could be acquired as:

$$\begin{aligned} u_i(s_1, x) &= x(\omega_i Q_i - C_i) + (1 - x)(Q_i - C_i) \\ &= \omega_i Q_i x - Q_i x + Q_i - C_i, \end{aligned} \quad (13)$$

and

$$u_i(s_2, x) = 0, \quad (14)$$

respectively.

In 6G ITS, due to the influence of factors such as region, time, and vehicle preferences on vehicles’ information sharing, dynamic parameter ω_i is introduced. When the vehicle’s activity is low, ω_i is set to be greater than 1 to incentivize vehicles to engage in collaborative sharing where group benefits outweigh the individual. On the contrary, when the vehicle’s activity is high, in order to balance the reputation distribution in the network and avoid the generation of reputation monopolies, ω_i can be set between 0 and 1.

Meanwhile, the average expected benefit of vehicles could be calculated as:

$$\begin{aligned} \bar{u}_i &= x u_i(s_1, x) + (1 - x) u_i(s_2, x) \\ &= x(\omega_i Q_i x - Q_i x + Q_i - C_i). \end{aligned} \quad (15)$$

Then, the growth rate of the sharing strategy is the dynamic equation of vehicle participation in sharing game, as follows:

$$\begin{aligned} F_i(x) &= x[u_i(s_1, x) - \bar{u}_i] \\ &= x(1 - x)[\omega_i Q_i x - Q_i x + Q_i - C_i]. \end{aligned} \quad (16)$$

Let $F_i(x) = 0$, which means that the growth rate of sharing strategy becomes 0 and the game enters into a relatively stable state. Thus, we obtain three points of steady state, which are $x_1 = 0$, $x_2 = 1$, and $x_3 = \frac{C_i - Q_i}{\omega_i Q_i - Q_i}$, respectively.

3) *Dynamic and Steady State Analysis*: In the theory of evolutionarily stable strategy (ESS), a steady state of a dynamic system should remain stable even in the presence of small disturbances. Namely, if x is the evolution equilibrium point (EEP), then the derivative of $F_i(x)$ should satisfy $F'_i(x) < 0$. Hence, we can analyze the evolutionary strategies (ES) of vehicles’ selection under different situations based on the above three stability points, as shown in Table II.

The sharing game contains four steady state strategies (1, 3, 4, 6) and two dynamic state strategies (2, 5). The factors that influence the evolution trend include incentives, participation costs, dynamic parameters, and the initial ratio of vehicles sharing information. With other parameters fixed, dynamic parameters are the key factor to increase the ratio of vehicles participating in information sharing.

TABLE II
EVOLUTIONARILY STABLE STRATEGY ANALYSIS

Range of ω_i	Strategy number	Range of C_i	Evolution strategy analysis
$\omega_i > 1$	Strategy 1	$C_i < Q_i < \omega_i Q_i$	$F'(x_1) > 0; F'(x_2) < 0; x_3 < 0$ does not exit EEP: x_2 ; ES: sharing
	Strategy 2	$Q_i < C_i < \omega_i Q_i$	$F'(x_1) < 0; F'(x_2) < 0; F'(x_3) > 0$ EEP: x_1, x_2 ; ES: $x \in (0, x_3)$, not sharing, and $x \in (x_3, 1)$, sharing
	Strategy 3	$Q_i < \omega_i Q_i < C_i$	$F'(x_1) < 0; F'(x_2) > 0; x_3 > 1$ does not exit EEP: x_1 ; ES: not sharing
$0 < \omega_i < 1$	Strategy 4	$C_i < \omega_i Q_i < Q_i$	$F'(x_1) > 0; F'(x_2) < 0; x_3 > 1$ does not exit EEP: x_2 ; ES: sharing
	Strategy 5	$\omega_i Q_i < C_i < Q_i$	$F'(x_1) > 0; F'(x_2) > 0; F'(x_3) < 0$ EEP: x_3 ; ES: x_3 ratio of vehicles choose sharing in the evolution results
	Strategy 6	$\omega_i Q_i < Q_i < C_i$	$F'(x_1) < 0; F'(x_2) > 0; x_3 < 0$ does not exit EEP: x_1 ; ES: not sharing

Since the steady state is constant in the game results and is not affected by parameter changes, we focus on analyzing the two dynamics in the above content. In dynamic strategy 2, for V_i , we can obtain the range of values for the dynamic parameter ω_i that incentivizes vehicle participation in sharing, as follows:

$$\frac{C_i - Q_i}{\omega_i Q_i - Q_i} < x^*, \quad (17)$$

where x^* represents the initial ratio of vehicles sharing information.

The equivalent transformation of (17) is $\omega_i > \frac{C_i - Q_i}{x^* Q_i} + 1$. Considering that in reality, the smallest incentive is always chosen to enhance vehicle motivation, therefore in dynamic strategy 2, the lower bound of ω_i is used to ensure that vehicles are motivated to share information with the smallest incentive, as in (18). It can be seen that ω_i is dynamically related to the vehicle's reputation, information sending time, and initial ratio of vehicles sharing information.

$$\begin{aligned} \omega_i &= \frac{C_i - Q_i}{x^* Q_i} + 1 \\ &= \frac{C_i - \{\eta_1 \ln[1 + R_i(e - 1)] + \eta_2 e^{-T_i}\}}{x^* [\eta_1 \ln[1 + R_i(e - 1)] + \eta_2 e^{-T_i}]} + 1. \end{aligned} \quad (18)$$

In dynamic strategy 5, since the evolution equilibrium point is not a definite value, when $x_3 = \frac{C_i - Q_i}{\omega_i Q_i - Q_i} \rightarrow 1$, namely, $\omega_i \rightarrow \frac{C_i}{Q_i}$, while satisfying that x_3 belongs to $(0, 1)$, V_i is more willing to participate in information sharing.

4) *Incentive and Punishment Strategy*: In order to motivate vehicles to participate in information sharing and maintain the balance of system reputation, the vehicle information sharing participation ratio in the current system can be queried and the dynamic parameters can be dynamically adjusted to drive vehicles' strategy evolution towards sharing. (19) could be leveraged to calculate the incentives that vehicles receive during information sharing. At the same time, there is also a possibility of malicious behavior among the vehicles participating in information sharing. Similar to the penalty mechanism in PoRs consensus, a reputation-based punishment mechanism is set at $-l$ times ($l > 1$) for honest participation in information sharing to prevent such situations.

$$RS_i = \omega_i Q_i - C_i = \omega_i \{\eta_1 \ln[1 + R_i(e - 1)] + \eta_2 e^{-T_i}\} - C_i. \quad (19)$$

The results of incentive or punishment vary dynamically with changes in dynamic parameters, initial sharing ratio, vehicle reputation, and information sending time for different vehicles, times, and regions. This can better maintain the reputation and order in 6G ITS [35].

VI. SECURITY ANALYSIS AND DISCUSSION

In this section, we analyze the security of the proposed scheme and discuss the computational and communication complexity of Info-Chain.

A. Preventing False Information Propagation

In Info-Chain based information sharing in 6G ITS, if a malicious vehicle reports false information in the network and wants to package it into a block and broadcast, it needs a bookkeeping node as its colluder. This is difficult to achieve in PoRs that consider traffic environmental factors. Even if this collusion succeeds, surrounding vehicles receiving the information will greatly negatively rate the reputation of the malicious vehicle if they find out that the information is false. Moreover, in the proposed mechanism, vehicles with reputation values below a certain threshold cannot share information.

B. Privacy Protection

In Info-Chain based information sharing in 6G ITS, when a vehicle registers as an Info-Chain member, it must submit its real information to the system. However, the system abstains from retaining this data. Instead, it retains the hash value related to the pertinent information. This approach ensures that even if information is leaked, attackers will be unable to pilfer the real vehicle information and compromise its privacy. Meanwhile, vehicles communicate in pseudonymous form in the Info-Chain. Specifically, vehicles use blockchain wallet addresses as communication pseudonyms. During information sharing, information, transactions, and blocks are signed using the sender's private key. If a malicious vehicle wants to forge the signature of vehicle i , it must know vehicle i 's private key. Generally speaking, a malicious vehicle can only obtain the vehicle i 's public key. Therefore, in the proposed scheme, the pseudonym and digital signature effectively protect the privacy of vehicles during information sharing.

C. Info-Chain Security

In Info-Chain, all full nodes are connected via reliable communication links. This implies that the Info-Chain, hosted and maintained by them, will operate in a relatively secure, efficient, and dependable communication, network, and storage environment [36]. Herein, RSUs act as a bridge between Info-Chain and ITS, responsible for synchronizing information from the traffic environment with the blockchain. As a trusted device, an RSU might malfunction. This would only result in the information in a limited area being less easily synchronized and would not affect the overall functionality of the entire system. Simultaneously, with the upgrade to the 6G networks, the security and reliability of wireless links will also be significantly enhanced. This provides a reliably guaranteed of secure communication for light nodes.

In the new block generation process of Info-Chain, communication between vehicles and vehicles/RSUs is encrypted. The elliptic curve algorithm utilized by the system for processing transactions and blocks is secp256k1, the same algorithm used in Bitcoin and Ethereum, ensuring the security of the system effectively. Without the appropriate key, attackers cannot access the communication. During the interaction, all information and transactions are signed, preventing attackers from forging information or denying it. Simultaneously, all vehicles within the system are authenticated, ensuring that

external attacks attempting to send disruptive messages to RSUs will be ineffective. Additionally, the reputation model can restrict and guide light nodes within Info-Chain to interact more rationally according to pre-defined protocols, which guarantees the secure operation of the system.

D. Resisting Against Threat Model Attacks

In Info-Chain, an information sharing event includes an information sharing node and a bookkeeping node. These are two completely different nodes, and the bookkeeping node is only responsible for verifying and packaging blocks. Therefore, malicious nodes cannot revoke their own transactions, and **double-spend attacks** can be avoided. PoRs selects a unique bookkeeping node for an information sharing event, and the consensus process also needs to consider the traffic environmental factors. Therefore, the selection of bookkeeping nodes has strong randomness, and a node can only have either a bookkeeping or sharing role. This makes it impossible for malicious nodes to package large amounts of valid transactions they construct into blocks, and **malicious competitive attacks** can be effectively resisted. Moreover, PoRs only produces one bookkeeper each time, which avoids blockchain forks. For **collusion attacks** and **self-promoting attacks**, firstly, most bookkeeping nodes and sharing nodes have high reputation values, which can greatly avoid collusion with validating nodes. Secondly, if a group wants to successfully launch collision attacks, it must ensure that all vehicles have high reputation values and appear in the same place simultaneously. At the same time, it needs to ensure that no other vehicles with high reputation values could report information. This is very challenging to achieve in 6G ITS with heavy traffic. In the proposed scheme, the increase or decrease of node reputation value mainly comes from both information sharing and working for consensus, thus the value of α_1 is relatively small in (3), which also makes the impact from **bad-mouthing attacks** or **false-praise attacks** negligible. Additionally, malicious ratings from individual vehicles will be offset to some extent by the reputation-based multi-vehicle comprehensive ratings. Volume and number of communications are used as measurement parameters in (7) to prevent **free-rider attacks**. During initial registration in the system, an exclusive blockchain wallet is allocated to each vehicle. This signifies that each vehicle has only one blockchain identity for communication within the system. Additionally, the reputation value verification before information interaction and the strong randomness of PoRs, effectively eradicates **sybil attacks**. Simultaneously, the system securely retains the hash value of the real information about the vehicle during the registration phase, which enables the system to compare the hash value of newly registered vehicle information with the hash values stored in the database, **whitewashing attacks** can be thwarted.

E. Computational and communication complexity of Info-Chain

Assuming that the 6G ITS has m vehicles. A subset of n vehicles participate in consensus (where $n < m$); which comprises 1 sharing vehicle, 1 bookkeeping vehicle, and

$n - 2$ validating vehicles. The communication complexity refers to the number of interactions between two parties in communication [37], and the computation and communication complexity of Info-Chain are shown in Table III.

TABLE III
COMPUTATIONAL AND COMMUNICATION COMPLEXITY

	Computational complexity	Communication complexity
Request and selection	$\mathcal{O}(n)$	$\mathcal{O}(1)$
Transactions generation	–	$\mathcal{O}(n)$
Blocks generation	–	$\mathcal{O}(n)$
Sharing and updating	$\mathcal{O}(n)$	$\mathcal{O}(m)$

In the Request and selection phase, it is necessary to select the bookkeeping nodes. There are $n - 1$ vehicles that need to calculate (5) and (6), with a computational complexity of $\mathcal{O}(1)$, and the system's computational complexity is $\mathcal{O}(n)$. The sharing vehicle sends a sharing request to the system, and the communication complexity of this phase is $\mathcal{O}(1)$. In the Transactions generation phase, there is no calculation involved. From the system's perspective, information from the sharing vehicle is received and the TX is sent to all validating vehicles, then the verification results are received. During this process, the system generates $2n - 3$ interactions, therefore the communication complexity is $\mathcal{O}(n)$. In the Blocks generation phase, there is also no calculation involved. From the perspective of bookkeeping nodes, packing the block and storing it in the blockchain requires 1 time communication with the system, respectively. In addition, it is necessary to communicate twice with $n - 2$ validating vehicles separately regarding block validation. During this process, the system generates $2n - 2$ interactions, so the communication complexity is $\mathcal{O}(n)$. In the Sharing and updating phase, the reputation value of nodes participating in sharing and consensus needs to be updated. It needs to calculate n vehicles using formulas (7) and (19), with a computational complexity of $\mathcal{O}(1)$, and the system computational complexity is $\mathcal{O}(n)$. The system needs to share information with all m vehicles in 6G ITS, so the complexity is $\mathcal{O}(m)$.

VII. SIMULATION RESULT AND ANALYSIS

In this section, we first test the Info-Chain and proposed reputation model. Then, we simulated the traffic communication in Info-Chain based ITS. Finally, we examined the evolution of incentives/punishments mechanism based on evolutionary game theory. The configurations of critical parameters are listed in Table IV. The elliptic curve algorithm utilized in the experiments is secp256k1, and ECC-secp256k1 and ECDSA-secp256k1 are employed to perform encryption/decryption and signing/verification of all information in Info-Chain. The selected map area covers $3 \text{ km} * 3.2 \text{ km}$ (latitude: $34.2509^\circ \text{N} \sim 34.2795^\circ \text{N}$, longitude: $108.0455^\circ \text{E} \sim 108.9455^\circ \text{E}$). Furthermore, communication distances of RSU and vehicles are set according to [38], and the data packet size for information transmission in ITS is based on [39]. When evaluating node reputation $R_i(e)$ using (3), we set $\alpha_1 = 0.25$ and $\alpha_2 = 0.75$,

since ratings from other nodes may be unfair and incentives/punishments from the system are absolutely reliable. This ensures the validity of the real rating feedback from other nodes while reducing the harm to the system from collusive bad-mouthing attacks, aiming to safeguard the interests of sharing nodes as much as possible. We set the weights in (5) based on the different levels of factors referenced by the proposed PoRs consensus mechanism for selecting bookkeepers. In the proposed mechanism, reputation serves as the foundation for assessing a node's reliability and is also the critical factor in calculating $E_i(e)$, hence we set $\gamma_1 = 0.6$. The distance between the vehicle and the information source is the criterion used to determine whether the bookkeeper can perform more effectively, thus γ_2 is set to 0.25. The 6G network is expected to deliver more advanced and stable communication services for the ITS, therefore, we minimize γ_3 to 0.15. Finally, when calculating the waiting time using (6), we predefine the reputation interval of the vehicle as $[0, 100]$, and determine $\lambda = 0.006$ through calculation, which ensures the appropriate mapping between $E_i(e)$ and $T_i(e)$. Meanwhile, setting $\zeta = 0.1$ can reduce the magnitude of the waiting time and minimize its impact on the consensus algorithm.

A. Simulation of Info-Chain

In this part, to validate the superiority of PoRs, we test and compare PoRs with traditional consensus algorithms [22], [40] and another reputation-based consensus algorithm [9] by Golang language 1.19.2. Each algorithm is tested 100 times, and the average value of every 10 experiments is taken as experimental data to eliminate the influence of hardware fluctuations during operation. We consider vehicles as nodes in Info-Chain, with test numbers ranging from 20 to 200. When the nodes reach consensus, a new block is outputted, which implies a consensus among an equal number of vehicles in 6G ITS. We verify the efficiency of PoRs from two aspects: the consensus time and the transaction throughput.

First, we test the time it takes for four algorithms to reach a consensus. As shown in Fig. 5, the time consumption of PoRs is reduced by up to 52.41%, 34.63%, and 17.88% compared to PoS, DPoS, and tPoR, respectively. Moreover, as the number

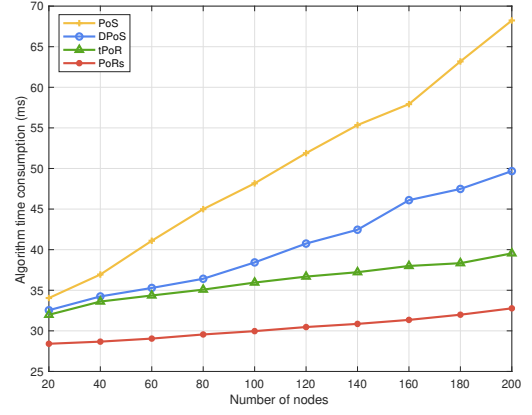


Fig. 5. Consensus time comparison.

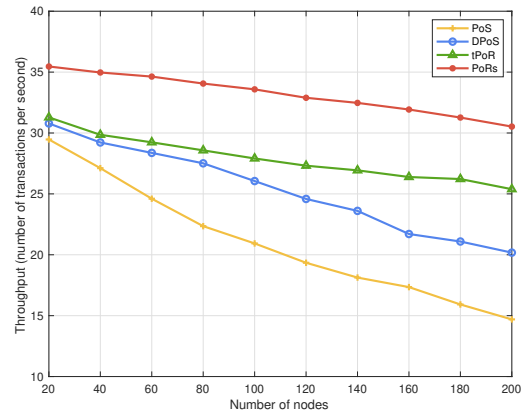


Fig. 6. Throughput comparison.

of nodes increases, PoRs increases less significantly than the other three, ensuring efficient information sharing in 6G ITS. Since PoRs uses reputation-based weight evaluation to achieve consensus without involving hash computation in PoS and DPoS, node voting in DPoS, or matrix computation in tPoR, the consensus process is completed more efficiently, reducing the consumption of consensus time excellently.

Then, we compare the transaction throughput by testing the Transaction Per Second (TPS) of the above four algorithms based on (20), and the result is as illustrated in Fig. 6. As the number of nodes increases, the time it takes for the consensus process to complete increases, resulting in decreased TPS for all four algorithms. However, the advantage of PoRs remains obvious. Comparing its TPS to PoS, DPoS, and tPoR, it has increased by 51.87%, 33.9%, and 16.84%, respectively. The main reason for this result is that the time consumption of PoRs is much lower than the other three, therefore it can process more transactions within a unit of time.

$$\text{TPS} = \frac{N_T}{\Delta t}, \quad (20)$$

where N_T represents the number of transactions and Δt is the time required to process these transactions.

TABLE IV
KEY PARAMETERS

Parameters	Values
Physical machine	Intel i5-8500@3.00GHz with 8GB RAM
Operating systems	Windows 11
Elliptic curve	secp256k1
Hash algorithm	SHA-256
Digital signatures	ECDSA (secp256k1)
Simulation area	3 km * 3.2 km
RSU transmission range	300 m
Vehicles transmission range	150 m
Simulation time	200 s
Data packet size	500 bytes
$\alpha_1, \alpha_2, \gamma_1, \gamma_2, \gamma_3, \zeta, \lambda$	0.25, 0.75, 0.6, 0.25, 0.15, 0.1, 0.006

B. Simulation of Proposed Reputation Model

In this part, to validate the effectiveness of the proposed reputation model, six potential scenarios are simulated using MATLAB 2022b. These scenarios comprehensively account for variations in sharers' reputations due to incentives/punishments for sharing true/false information and the fair/neutral/negative ratings given by other vehicles. The specific comparisons are presented in Table V. In this experiment, vehicles engage in honest interactions for the first 9 times, malicious vehicles attack on the 10th interaction, and then vehicles continue to interact honestly until the 50th interaction when they launch another attack, as shown in Fig. 7.

TABLE V
SIX POTENTIAL SCENARIOS IN PROPOSED REPUTATION MODEL

Scenarios	Information	Rating	Raputation
1	true	fair	increase
2		neutral	increase slowly
3		negative	increase overall
4	false	fair	decrease slowly
5		neutral	decrease
6		negative	decrease rapidly

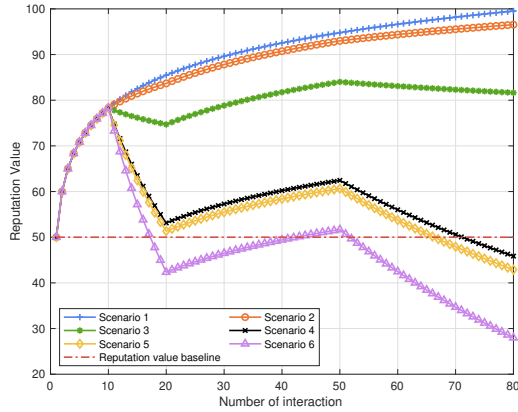


Fig. 7. The reputation variation in different scenarios.

In scenario 1, the vehicle shares true information and obtains a reward RS_i . Afterward, it also receives fair ratings from other vehicles, which keeps its reputation increasing in a virtuous cycle. In both scenarios 2 and 3, the vehicle also shares true information and obtains a reward RS_i . This could undermine the equity of the reputation ratings of the sharers and result in a deceleration in the growth of their reputations. Nevertheless, the overall increasing trend in reputation encourages vehicles to continue their efforts in enhancing their reputation by sharing true information. Consequently, the proposed reputation model effectively withstands both bad-mouthing attacks and false-praise attacks. In scenarios 4 and 5, collusion attacks are considered, wherein the vehicle shares false information and receive positive or neutral ratings from other colluding vehicles. The punishment for sharing false information, $-lRS_i$, will substantially diminish the attacker's reputation, even in the presence of a positive or

neutral collusion assessment. This is because the weight of the reward/punishment in (3) exceeds that of the ratings from other vehicles. This deters collusion and cooperation in engaging in malicious activities. Therefore, the proposed reputation model can resist collusion attacks. In scenario 6, the vehicle shares false information, and other vehicles give negative ratings, thus the sharer's reputation decreases significantly. Subsequently, the malicious vehicle continued to improve its own reputation before launching a second attack, causing its reputation to decline again. Across all the aforementioned scenarios, it is observed that the increase in vehicle reputation is notably smaller than the decrease. This observation points to the fact that malicious vehicles require more time to enhance their reputation values. This, in turn, could contribute to the reduction in attack frequency in the context of 6G ITS.

C. Simulation of Info-Chain in Traffic Communication

In this part, to verify the impact of Info-Chain based 6G ITS on traffic communication, the proposed scheme is evaluated using the OMNeT++ 6.0, SUMO 1.11.0, and Veins 5.2 co-simulation platforms with Ubuntu 20.04. A real map of the city of Xi'an, China is used to simulate the traffic network and IoV scenario, as shown in Fig. 8. We test the variation of Communication Delay (CD) and Packet Loss Rate (PLR) for 40, 60, and 80 vehicles participating in the consensus (1/5 of which are validating vehicles) at different speeds with the proposed scheme, respectively.

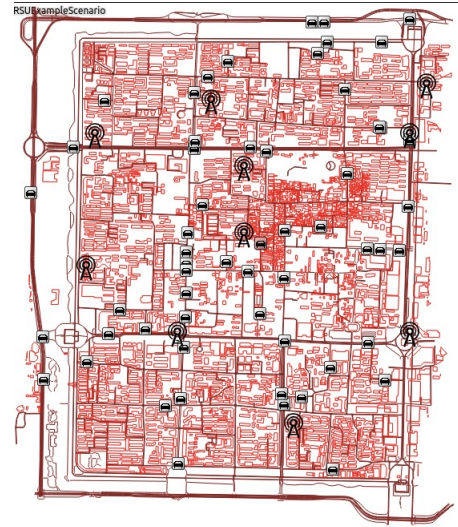


Fig. 8. Traffic network and IoV scenario in simulations.

In this experiment, CD is the difference between the time when the information is sent from a sharing vehicle and the time when the new block is received by the RSU maintaining Info-Chain. Fig. 9 depicts the impact of vehicle speed and number on CD. The increase in CD is accompanied by an increase in vehicle speed for a constant number of vehicles. This is caused by the change in vehicle speed leads to an increase in the frequency of packets sent by the vehicle per unit of time, which increases the queuing time of the packets at the receiving end. Moreover, as vehicle speed increases,

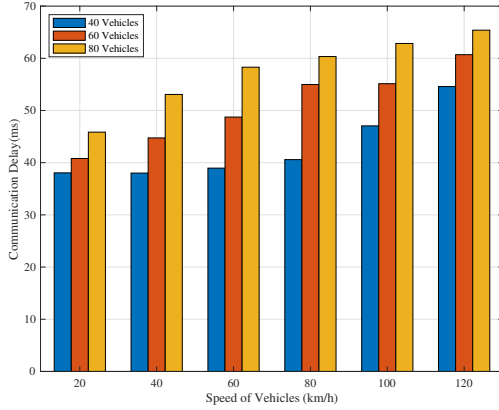


Fig. 9. Impact of vehicle speed and number of vehicles on CD.

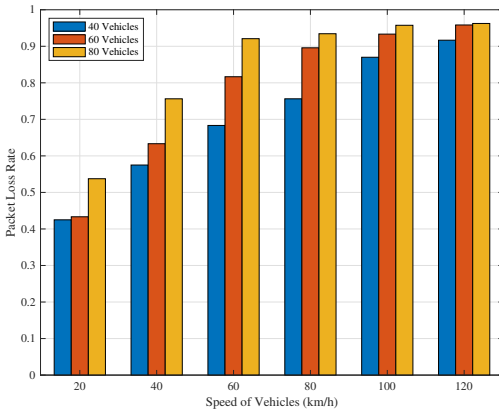


Fig. 10. Impact of vehicle speed and number of vehicles on PLR.

the distance between communication parties also increases, increasing communication delay. With constant vehicle speed, the number of validating vehicles and packets increases with the number of participating consensus vehicles. This results in increased queuing delay for packets and thus leads to an increase in CD.

This experiment defines PLR as the ratio of the difference between the total number of packets sent by the validating vehicle and the total number of packets received by the bookkeeping vehicle to the total number of packets received by the bookkeeping vehicle during the simulation time. Fig. 10 depicts the impact of vehicle speed and number on PLR. The increase in PLR is also accompanied by an increase in vehicle speed for a constant number of vehicles. This is because the faster the vehicle speed changes, the more packets are sent in the same area, and the queuing time of packets at the receiving end exceed the threshold, increasing the packet loss rate. With constant vehicle speed, an increase in the number of vehicles results in an elevated amount of packets generated within the communication range. This increase leads to more message collisions and queuing delays that result in the loss of packets, causing a higher PLR.

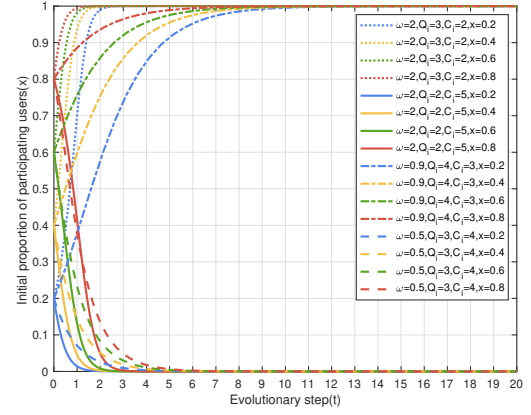


Fig. 11. Evolutionary graph of steady state.

D. Simulation of Evolutionary Game Theory

In this part, to verify the impact of different parameters on the game, we simulate the steady state and dynamic evolution of the proposed sharing game model under different dynamic parameters and initial sharing ratios using MATLAB 2022b.

1) Steady state Strategy

The proposed sharing game model consists of four steady state strategies. We simulate the evolution of these four steady state strategies with different dynamic parameters and initial sharing ratios, as shown in Fig. 11. In steady state strategies 1 ($\omega_i = 2, Q_i = 3, C_i = 2$) and 4 ($\omega_i = 0.9, Q_i = 4, C_i = 3$), the high incentive obtained by vehicles' participation in information sharing due to the large dynamic parameters. This leads to active participation from vehicles even if initial sharing ratios are very low and eventually evolves into participation in information sharing; in steady state strategies 3 ($\omega_i = 2, Q_i = 2, C_i = 5$) and 6 ($\omega_i = 0.5, Q_i = 3, C_i = 4$), even initial sharing ratios of 0.8 eventually evolves into not sharing information, as the high cost of participation that it makes the vehicle unaffordable. Therefore, in the process of setting ω_i and η_1, η_2 in Q_i , the current sharing cost of vehicles should be considered, and the incentive strategy should be dynamically adjusted to guide the vehicles in the system to participate in information sharing.

2) Dynamic Strategy

The proposed sharing game model consists of two dynamics. To verify the evolution process of the two dynamics and subsequently adjust the dynamic parameters to guide vehicles to participate in information sharing, we simulate the evolution of these two dynamic strategies with different dynamic parameters and initial sharing ratios.

In dynamic strategy 2 ($\omega_i > 1, Q_i < C_i < \omega Q_i$), vehicles with initial sharing ratio $x \in (0, x_3)$ evolve to not participate in sharing, while those with initial sharing ratio $x \in (x_3, 1)$ evolve to sharing. Fig. 12. shows the simulation results. When $\omega_i = 1.5$, the final evolution results in not sharing, regardless of the initial sharing ratios. When $\omega_i = 2$, the evolution results for initial sharing ratios $x = 0.6$ and 0.8 are to participate in sharing, while other proportions eventually evolve into not sharing. As ω_i increases, only the evolution results for

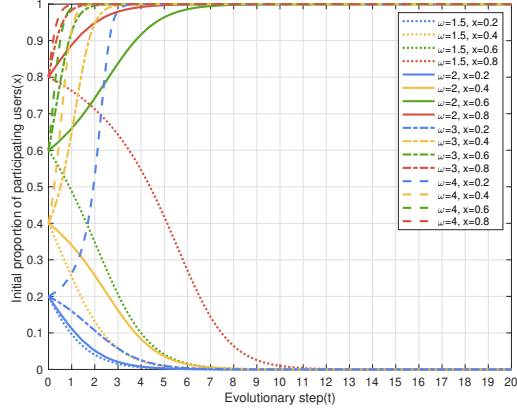


Fig. 12. Evolutionary graph of dynamic strategy 2.

$x = 0.2$ is not to share; and when ω_i is increased to 4, all situations eventually evolve into participation sharing. From the perspective of the initial sharing ratios, the willingness of vehicles to participate in sharing increases as ω_i increases. Therefore, in dynamic strategy 2, when the initial participation rate is low, the dynamic parameter can be increased to motivate vehicles to share information. When the system tends towards a steady state of sharing, the dynamic parameter can be slightly reduced to stabilize the balance of reputation in the system.

In dynamic strategy 5 ($0 < \omega_i < 1$, $\omega_i Q_i < C_i < Q_i$), x_3 is the ratio of vehicles that participate in sharing in the evolution results. Fig. 13. shows the simulation results, which reveal that regardless of the value of ω_i , the eventual evolution results do not evolve into share or not share information. However, the eventual ratio of vehicles that choose to participate in sharing increases as ω_i increases. Notably, in the case where ω_i is determined, the group with high initial sharing ratios and the group with low initial sharing ratios also influence each other. Therefore, in order to continuously motivate vehicles to participate in information sharing, dynamic parameters should be increased as much as possible to promote a higher participation ratio in the final evolution result. It may even be necessary to further increase the dynamic parameters to guide vehicles to evolve into strategy 4.

VIII. CONCLUSION

This article proposes Info-Chain, a secure, trusted blockchain based on reputation for information sharing in 6G ITS. PoRs is used to evaluate the bookkeeper based on the vehicles' reputation values and traffic environmental factors, and the evaluation results are consensus wait times for distributed consensus. Meanwhile, VRF is used to verify the reputation value of the sharer before information sharing under privacy protection. Furthermore, an incentives/punishments mechanism based on evolutionary game theory is used to enhance the desire of vehicles to share information in 6G ITS. We next intend to explore the application of other information exchange methods such as information trading and information crowdsourcing with the proposed scheme. Concurrently, we will enhance the privacy protection mechanism of this scheme,

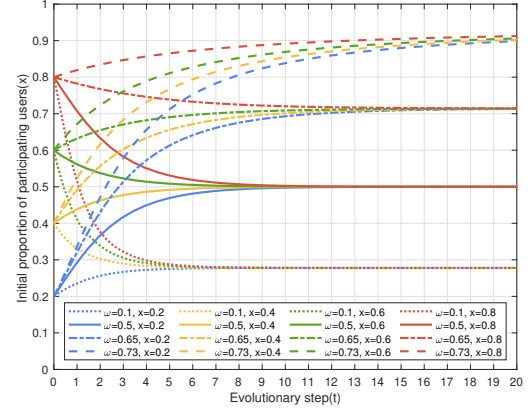


Fig. 13. Evolutionary graph of dynamic strategy 5.

and propose a novel pseudonym scheme that facilitates distributed and secure management of vehicle pseudonyms during information interaction.

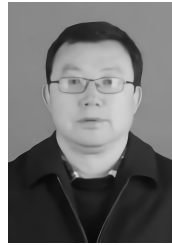
REFERENCES

- [1] Z. Zhou, M. Wang, J. Huang, S. Lin, and Z. Lv, "Blockchain in big data security for intelligent transportation with 6g," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 9736–9746, 2022.
- [2] S. Xuan, L. Zheng, I. Chung, W. Wang, D. Man, X. Du, W. Yang, and M. Guizani, "An incentive mechanism for data sharing based on blockchain with smart contracts," *Comput. Elect. Eng.*, vol. 83, p. 106587, 2020.
- [3] J. Zhang, T. Li, M. S. Obaidat, C. Lin, and J. Ma, "Enabling efficient data sharing with auditable user revocation for iov systems," *IEEE Syst. J.*, vol. 16, no. 1, pp. 1355–1366, 2022.
- [4] X. Wang, L. Ding, Q. Wang, J. Xie, T. Wang, X. Tian, Y. Guan, and X. Wang, "A picture is worth a thousand words: Share your real-time view on the road," *IEEE Trans. Veh. Technol.*, vol. 66, no. 4, pp. 2902–2914, 2017.
- [5] J. Guo, X. Li, Z. Liu, J. Ma, C. Yang, J. Zhang, and D. Wu, "Trove: A context-awareness trust model for vanets using reinforcement learning," *IEEE Internet Things J.*, vol. 7, no. 7, pp. 6647–6662, 2020.
- [6] T. Hewa, G. Gür, A. Kalla, M. Yliantila, A. Bracken, and M. Liyanage, "The role of blockchain in 6g: Challenges, opportunities and research directions," in *Proc. 2nd 6G Wireless Summit (6G SUMMIT)*, 2020, pp. 1–5.
- [7] R. Yang, F. R. Yu, P. Si, Z. Yang, and Y. Zhang, "Integrated blockchain and edge computing systems: A survey, some research issues and challenges," *IEEE Commun. Surv. Tutorials*, vol. 21, no. 2, pp. 1508–1532, 2019.
- [8] Z. Yan, P. Zhang, and A. V. Vasilakos, "A survey on trust management for internet of things," *J. Network Comput. Appl.*, vol. 42, pp. 120–134, 2014.
- [9] K. Yan, P. Zeng, K. Wang, W. Ma, G. Zhao, and Y. Ma, "Reputation consensus-based scheme for information sharing in internet of vehicles," *IEEE Trans. Veh. Technol.*, pp. 1–6, 2023.
- [10] J. Cui, F. Ouyang, Z. Ying, L. Wei, and H. Zhong, "Secure and efficient data sharing among vehicles based on consortium blockchain," *IEEE Trans. Intell. Transp. Syst.*, vol. 23, no. 7, pp. 8857–8867, 2022.
- [11] Z. Yan, L. Peng, W. Feng, and L. T. Yang, "Social-chain: Decentralized trust evaluation based on blockchain in pervasive social networking," *ACM Trans. Internet Technol.*, vol. 21, no. 1, 2021.
- [12] F. Tariq, M. R. A. Khandaker, K.-K. Wong, M. A. Imran, M. Bennis, and M. Debbah, "A speculative study on 6g," *IEEE Wireless Commun.*, vol. 27, no. 4, pp. 118–125, 2020.
- [13] S. Nayak and R. Patgiri, "6g communication: A vision on the potential applications," in *Proc. Edge Analytics: Sel. Proc. 26th Int. Conf. (ADCOM 2020)*, 2022, pp. 203–218.
- [14] M. Noor-A-Rahim, Z. Liu, H. Lee, M. O. Khyam, J. He, D. Pesch, K. Moessner, W. Saad, and H. V. Poor, "6g for vehicle-to-everything (v2x) communications: Enabling technologies, challenges, and opportunities," *Proc. IEEE*, vol. 110, no. 6, pp. 712–734, 2022.

- [15] Z. Zhang, Y. Xiao, Z. Ma, M. Xiao, Z. Ding, X. Lei, G. K. Karagiannidis, and P. Fan, "6g wireless networks: Vision, requirements, architecture, and key technologies," *IEEE Trans. Veh. Technol.*, vol. 14, no. 3, pp. 28–41, 2019.
- [16] V.-L. Nguyen, R.-H. Hwang, P.-C. Lin, A. Vyas, and V.-T. Nguyen, "Towards the age of intelligent vehicular networks for connected and autonomous vehicles in 6g," *IEEE Network*, pp. 1–8, 2022.
- [17] G. Li, C. Lai, R. Lu, and D. Zheng, "Seccdv: A security reference architecture for cybertwin-driven 6g v2x," *IEEE Trans. Veh. Technol.*, vol. 71, no. 5, pp. 4535–4550, 2022.
- [18] G. Singh, A. Srivastava, V. A. Bohara, M. N. Rahim, Z. Liu, D. Pesch, and L. Hanzo, "Towards 6g-v2x: Hybrid rf-vlc for vehicular networks," *arXiv preprint arXiv:2208.06287*, 2022.
- [19] X. You, C.-X. Wang, J. Huang, X. Gao, Z. Zhang, M. Wang, Y. Huang, C. Zhang, Y. Jiang, J. Wang *et al.*, "Towards 6g wireless communication networks: Vision, enabling technologies, and new paradigm shifts," *Sci. China Inf. Sci.*, vol. 64, pp. 1–74, 2021.
- [20] M. Adhikari, A. Hazra, V. G. Menon, B. K. Chaurasia, and S. Mumtaz, "A roadmap of next-generation wireless technology for 6g-enabled vehicular networks," *IEEE Internet of Things Mag.*, vol. 4, no. 4, pp. 79–85, 2021.
- [21] R. Shrestha, R. Bajracharya, and S. Kim, "6g enabled unmanned aerial vehicle traffic management: A perspective," *IEEE Access*, vol. 9, pp. 91 119–91 136, 2021.
- [22] Y. Lu, X. Huang, K. Zhang, S. Maharjan, and Y. Zhang, "Blockchain empowered asynchronous federated learning for secure data sharing in internet of vehicles," *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, pp. 4298–4311, 2020.
- [23] G. Luo, H. Zhou, N. Cheng, Q. Yuan, J. Li, F. Yang, and X. Shen, "Software-defined cooperative data sharing in edge computing assisted 5g-vanet," *IEEE Trans. Mob. Comput.*, vol. 20, no. 3, pp. 1212–1229, 2021.
- [24] J. Zhang, T. Li, M. S. Obaidat, C. Lin, and J. Ma, "Enabling efficient data sharing with auditable user revocation for iov systems," *IEEE Syst. J.*, vol. 16, no. 1, pp. 1355–1366, 2022.
- [25] B. Yin, Y. Wu, T. Hu, J. Dong, and Z. Jiang, "An efficient collaboration and incentive mechanism for internet of vehicles (iov) with secured information exchange based on blockchains," *IEEE Internet of Things J.*, vol. 7, no. 3, pp. 1582–1593, 2020.
- [26] Y. Wang, Z. Su, Q. Xu, R. Li, and T. H. Luan, "Lifesaving with rescuechain: Energy-efficient and partition-tolerant blockchain based secure information sharing for uav-aided disaster rescue," in *Proc. IEEE Conf. Comput. Commun. (IEEE INFOCOM)*, 2021, pp. 1–10.
- [27] C. Lai, K. Zhang, N. Cheng, H. Li, and X. Shen, "Sirc: A secure incentive scheme for reliable cooperative downloading in highway vanets," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 6, pp. 1559–1574, 2017.
- [28] L. Xiong and L. Liu, "Peertrust: supporting reputation-based trust for peer-to-peer electronic communities," *IEEE Trans. Knowl. Data Eng.*, vol. 16, no. 7, pp. 843–857, 2004.
- [29] R. Kumar and R. Goyal, "Performance based risk driven trust (prtrust): On modeling of secured service sharing in peer-to-peer federated cloud," *Comput. Commun.*, vol. 183, pp. 136–160, 2022.
- [30] S. Micali, M. Rabin, and S. Vadhan, "Verifiable random functions," in *Proc. 40th Annu. Symp. Found. Comput. Sci.*, 1999, pp. 120–130.
- [31] C. Fang, Y. Guo, J. Ma, H. Xie, and Y. Wang, "A privacy-preserving and verifiable federated learning method based on blockchain," *Comput. Commun.*, vol. 186, pp. 1–11, 2022.
- [32] P. K. R. Maddikunta, Q.-V. Pham, D. C. Nguyen, T. Huynh-The, O. Aouedi, G. Yenduri, S. Bhattacharya, and T. R. Gadekallu, "Incentive techniques for the internet of things: A survey," *J. Network Comput. Appl.*, vol. 206, p. 103464, 2022.
- [33] S.-M. Hosseini-Motlagh, T.-M. Choi, M. Johari, and M. Nouri-Harzvili, "A profit surplus distribution mechanism for supply chain coordination: An evolutionary game-theoretic analysis," *Eur. J. Oper. Res.*, vol. 301, no. 2, pp. 561–575, 2022.
- [34] S. Phelps and M. Wooldridge, "Game theory and evolution," *IEEE Intell. Syst.*, vol. 28, no. 04, pp. 76–81, 2013.
- [35] E. K. Wang, C.-M. Chen, S. M. Yiu, M. M. Hassan, M. Alrubaian, and G. Fortino, "Incentive evolutionary game model for opportunistic social networks," *Future Gener. Comput. Syst.*, vol. 102, pp. 14–29, 2020.
- [36] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Secure computation offloading in blockchain based iot networks with deep reinforcement learning," *IEEE Trans. Network Sci. Eng.*, vol. 8, no. 4, pp. 3192–3208, 2021.
- [37] L. Zhang, H. Xu, O. Onireti, M. A. Imran, and B. Cao, "How much communication resource is needed to run a wireless blockchain network?" *IEEE Network*, vol. 36, no. 1, pp. 128–135, 2022.
- [38] B. Ko, K. Liu, S. H. Son, and K.-J. Park, "Rsu-assisted adaptive scheduling for vehicle-to-vehicle data sharing in bidirectional road scenarios," *IEEE Trans. Intell. Transp. Syst.*, vol. 22, no. 2, pp. 977–989, 2021.
- [39] Y. Regragui and N. Moussa, "A real-time path planning for reducing vehicles traveling time in cooperative-intelligent transportation systems," *Simul. Modell. Pract. Theory*, vol. 123, p. 102710, 2023.
- [40] M. Li, L. Zhu, and X. Lin, "Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4573–4584, 2019.



Kun Yan received a B.S. degree in internet of things engineering from Xi'an University of technology, Xi'an, China, in 2019. He is currently working toward a Ph.D. degree in the School of Telecommunications Engineering, Xidian University. His research interests include blockchain, internet of vehicles, reputation management, and 6G network security.



Wenping Ma received the B.S. and M.S. degrees in fundamental mathematics from Shaanxi Normal University, Xi'an, China, in 1987 and 1990, respectively, and the Ph.D. degree in communication and information system from Xidian University, Xi'an, in 1999, where he is currently a Full Professor with the School of Telecommunications Engineering. His current research interests include information theory, communication theory, blockchain, and 6G network security.



Qi Yang received a B.S. degree in Telecommunications engineering from Xidian University, Xi'an, China, in 2020, he is currently working toward a M.S. degree in the School of Telecommunications Engineering, Xidian University. His research interests include blockchain, internet of vehicles, and cyber security.



Shaohui Sun (Member, IEEE) received his Ph.D. from Xidian University, Xi'an, China, in 2003. From March 2003 to June 2006, he was a postdoctoral research fellow at the Datang Telecom technology and industry group, Beijing, China. From June 2006 to December 2010, he worked at the Datang Mobile Communications Equipment Co., Ltd., Beijing, where he has been deeply involved in the development and standardization of the Third-Generation Partnership Project Long-Term Evolution (3GPP LTE). Since January 2011, he has been the Chief Technical Officer with Datang Wireless Mobile Innovation Center of the Datang Telecom Technology and Industry group. His current research interest includes advanced technologies related to B5G/6G.



Weiwei Wang received the B.S. degree in mathematics from Baicheng Normal University, Jilin, China, in 2018, and the M.S. degree in 2021 in the school of mathematics at Liaoning University, Liaoning, China. He is currently pursuing the Ph.D. degree in the School of Communication Engineering, Xidian University, Xi'an, China. His research interest includes information security, cryptography.