Hindawi
Mathematical Problems in Engineering
Volume 2021, Article ID 9954599, 13 pages
https://doi.org/10.1155/2021/9954599

Research Article

Blockchain-Based Authentication with Optional Privacy Preservation for Internet of Vehicles

Jinxin Zhang and Meng Wu

School of Computer Science & Technology, Nanjing University of Posts and Telecommunications, Nanjing 210023, China

Correspondence should be addressed to Meng Wu; wum@njupt.edu.cn

Received 30 March 2021; Accepted 10 June 2021; Published 19 October 2021

Academic Editor: Hou-Sheng Su

With the rapid development of the mobile internet and intelligent technology of in-vehicle equipment, the Internet of Vehicles (IoV), centered on intelligent connected cars, has gradually entered people's lives. However, these technologies also bring serious privacy risks and security issues in terms of data transmission and storage. In this article, we propose a blockchain-based authentication system to provide vehicle safety management. The privacy and security attributes of various vehicle authentication transactions are based on high-level cryptographic primitives, realizing temporary and formal authentication methods. At the same time, a fair blockchain consensus mechanism Auction of block generation Rights (AoR) is proposed. To demonstrate the feasibility and scalability of the proposed scheme, security and performance analyses are presented. The relevant experimental results show that the scheme can provide superior decentralized management for IoV.

1. Introduction

In recent years, as a potential technology, the Internet of Vehicles [1] has attracted great attention, bringing a better life to human beings. It can be applied in the fields of logistics and transportation. According to a report [2] from the World Health Organization on road safety, in 2018, a total of 1.35 million people died in traffic accidents worldwide, and traffic accidents are the number one killer in the 5–29 age group. The Internet of Vehicles can solve such problems well. This is just one example of many applications of the Internet of Vehicles.

The Internet of Vehicles usually consists of a large number of static basic settings and dynamic vehicles as the main participants in the system. It is equipped with advanced in-vehicle sensors, controllers, actuators, and other devices and integrates modern communication and network technologies to realize the information exchange and sharing between vehicles and vehicles, roads, and service providers. It has complex environmental perception, intelligent decision-making, and collaborative control and performs other functions. The purpose of the Internet of Vehicles is to avoid unnecessary traffic accidents and congestion. The ultimate goal is to provide a comfortable driving experience including autonomous driving and in-vehicle entertainment.

The Internet of Vehicles technology system mainly includes the automotive sensor, automotive wireless communication, automotive navigation, electronic map and positioning, vehicle-mounted Internet of Things terminal, intelligent control, massive data processing, data integration, intelligent transportation technology, video surveillance, and mobile communication network. It differs from other types of network application scenarios; thus, all these technologies complement each other and cooperate to achieve. The future of the Internet of Vehicles system will face the requirements of system function integration, dataset quantification, and high transmission rate.

With the gradual evolution of closed-loop information services to IoV services and the close integration of vehicle, road, and surrounding environmental data, the Internet of Vehicles will more effectively reduce the incidence of car accidents and provide a safer, more economical, and more convenient travel service. On the Internet of Vehicles, the

vehicle must periodically broadcast the identity, current location, speed, and other related information of the traffic vehicle to all vehicles around it. Malicious vehicles can obtain the private information (identity, location, etc.) of the vehicle driver by analyzing the relationship between the message and the sender. This poses a potential threat to the privacy of vehicle users, increases the risk of data leakage and may potentially affect the safety of vehicle occupants [3, 4].

Authentication is considered the first line of defense against malicious vehicles and messages [5–7]. It is the basis for the security of all other applications of the Internet of Vehicles in the open traffic environment. Identity authentication includes the verification of the legitimacy of the identity of the connected vehicles, to ensure the authenticity of the identity of the communicating parties. At the same time, it is necessary to protect the privacy of users through anonymity [8–10]. Therefore, the automotive industry needs to establish more secure authentication methods to avoid this risk.

The characteristics that need to be considered in the identity authentication of the car network are as follows:

(1) Due to the fast-moving speed of the vehicle and the limited coverage of the roadside unit (RSU), high real-time identity verification is required.

(2) The environments in the IoV vary widely, with diverse application scenarios and performance differences between devices. Transaction processing may be delayed. Therefore, such realistic factors need to be considered to build a fair authentication environment so that vehicles can have equal opportunities to be authenticated.

The Internet of Vehicles currently uses centralized facilities, Public Key Infrastructure (PKI), or trust authority (TA) to perform the authentication mechanism. The disadvantage is that the centralization of the authentication node leads to heavy tasks and attacks on the central node. These shortcomings can cause data leakage of sensitive user information. Besides, the centralized facility is not suitable for the wide and complex geographically distributed IoV and high real-time requirements.

To address the issue, some scholars [11–13] use blockchain [14] to develop a decentralized scheme, which provides a secure way of managing vehicle registration. Some review articles [15–18] believe that blockchain can provide a boost to the Internet of Things. The essence of the blockchain is a distributed ledger database of a peer-to-peer (P2P) network. A complete blockchain system includes technologies such as data encryption, digital signatures, and timestamps, as well as consensus algorithms to support P2P and maintenance systems, mining, and anonymous transactions. The blockchain can also be applied in many fields [19–23] with its unique security mechanism.

In this paper, we propose an identity authentication system for IoV. Our system utilizes the following advantages of the blockchain:

(i) We use the common private key, public key, and address based on elliptic curve cryptography (ECC) in the blockchain to achieve anonymous security authentication, without the need to construct other cryptographic primitives.

(ii) Based on the decentralization nature of blockchain, trust management can be conducted among distributed RSUs, which can effectively avoid the problem of centralization. To sink a large number of vehicle registration functions, reduce the delay of neutralization, and reduce security risks.

(iii) We assign different node roles to vehicles and facilities and make the best use of them and enable RSUs to work together and maintain a consistent blockchain, and the vehicle node ensures that the basic information of the vehicle is maintained.

Thus, the key contributions of this paper can be summarized as follows:

(1) For high real-time requirements, we propose a decentralized vehicle registration with TA providing authentication keys for each RSU.

(2) We achieve optional privacy-preserving authentication for diverse scenarios. It includes short-term temporary authentication and long-term formal authentication.

(3) We propose a fair consensus mechanism to equalize the opportunity to process things on different devices and ensure that vehicle information can be treated equally.

The rest of this paper is organized as follows: Section 2 describes the related work. Section 3 describes the overall design. We present the system performance evaluation results in Section 4. Contrastive analysis is discussed in Section 5. Section 6 concludes this paper and presents some future work.

2. Related Work

In the traditional solution, a completely trusted neutral server is required. Such a central server is easily a target for attackers. Moreover, it is not suitable for deployment in scenarios where a large number of vehicles participate, and a large amount of data will bring high latency or even congestion. To deal with such problems, decentralized solutions have gradually become a research focus.

By using the tamper-proof, hash-encrypted features of blockchain technology, a decentralized and trusted identity can be defined as a set of keys used to prove the source and validity of the information. These keys are directly controlled by the principal with this identity. With the help of the consensus mechanism, this identity based on the blockchain can be effectively published and recorded.

2.1. Asymmetric Encryption Technology. In 1976, Diffie and Hellman proposed the concept of an asymmetric cryptosystem [24], that is, a public-key cryptosystem, which created a new direction in cryptography research. The asymmetric encryption algorithm is relative to the

symmetric algorithm. The difference between the two is reflected in whether the key can be disclosed. The symmetric key requires the same key to be used in the encryption and decryption process, while asymmetric encryption can provide a pair of keys. The private key is kept by yourself, and the public key can be made public. The common symmetric encryption algorithms are DES, 3DES, AES, and IDEA, and the common asymmetric encryption algorithms are RSA, D-H, and ECC [25].

The security of the blockchain is provided by cryptography. In many blockchain projects, asymmetric encryption algorithms are mainly used at the account level. In the symmetric encryption algorithm, because both parties need to share the key in advance, there are many inconveniences in the use process. The emergence of asymmetric algorithms solves this problem. Take Bitcoin [26] as an example. The Bitcoin address is converted from the public key, and the public key is converted from the private key. All user information is protected by a randomly generated private key.

Since the content of each block in the blockchain is open to the entire network, privacy protection is an important issue. The blockchain represented by Bitcoin uses the wallet address generated by the public key hash to externally represent the input and output process of the transaction which brings such a benefit: the public key is generated by a random private key. Only by relying on the public key hash, it is impossible to know who caused the transaction. The relationship between blockchain keys and addresses is shown in Figure 1. The owner of the private key is the only representative of the transaction generated by the corresponding address, but no one knows who the true private key holder is.

2.2. Consensus. The word consensus comes from Latin, meaning "agreement, accord," which in turn comes from consentire, meaning "feel together." Its meaning and usage relate to both a generally accepted opinion and the conclusion of a decision based on a collective agreement.

In an isolated system, the system always develops in disorder, and the same is true for information systems. However, this feature is not suitable for its use. To deal with this feature, the consensus mechanism has become an important choice. Consensus issues require multiple processes (or agents) to agree on single data [27]. Some processes (agents) may fail or be unreliable in other ways, so the consensus protocol must be fault-tolerant or flexible. The process must propose its candidate values in some way, communicate with each other, and reach a consensus on individual data.

The consensus problem is basic in controlling multiagent systems [28]. One way to reach consensus is to get a majority of all processes (agents) to agree. In this case, the majority requires at least more than half of the available votes (where each process is voted). However, one or more wrong processes may bias the final result, which may lead to failure to reach a consensus or a wrong consensus.

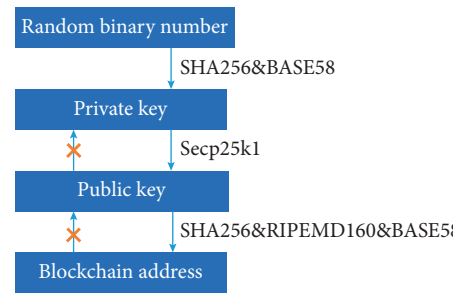

Figure 1: The relationship between blockchain keys and addresses.

2.2.1. Evolution of Consensus in the Internet. From the perspective of the development of the consensus mechanism, its development process is closely related to the process of network evolution. This section will sort out the development process of the network and consensus mechanism, clarify the relationship between the two issues, and find out the possible development direction of the future consensus mechanism. The Internet is a complex that has been evolving rapidly. From different perspectives such as history and technology, it can be divided into different stages. After synthesizing the scale and structure of the network, Table 1 divides the development of the Internet into five phases and reveals the development trajectory of the consensus mechanism.

The surge of intelligent Internet between 5G and artificial intelligence (AI) will be achieved in the 2020s, which is the most worthy of imagination. With the emergence of new business types and requirements such as the Internet of Vehicles, Internet of Things, Industrial Internet, 4K/8K, and AR/VR, the future network is appearing in a ubiquitous trend. It expects that the intelligent Internet will build an essential framework for a smart society in the future.

For the consensus mechanism, it is necessary to combine the specific requirements and application scenarios to implement adaptive settings for specific services [29, 30]. At this stage, increasingly or increasing various devices will become the main body of consensus. Decentralization makes the relationship between nodes equal. How to reach a fair and effective consensus is an inevitable problem. The following content of this article will clarify our consensus mechanism, which combines incentives and penalties to ensure its stable operation.

2.2.2. Blockchain Consensus Algorithm. In the decentralized network structure, there are no fixed nodes to manage transactions on the blockchain. Therefore, it is necessary to regularly allocate accounting rights from all mining nodes according to certain rules. At the same time, to achieve order from unnecessary to order and achieve entropy reduction, a certain amount of energy is inevitable. Since the blocks in the blockchain are generated at a certain time interval, in the interval phase, the transaction needs to be temporarily stored in the transaction pool. After the accounting node is selected in the network, the transaction is retrieved and

Table 1: The evolution of consensus in the internet.

Era of origin	Scale	Participants	Implementation process	Content
The late 1960s	Small scale	The network structure is simple, the differences between nodes are small, and there is no consensus requirement. Propose relevant problem assumptions		
In the mid-1980s	Medium scale	Distributed databases	Assuming there is no Byzantine fault node	Database agreement
In the mid-1990s	Large scale	Distributed databases	Tolerating Byzantine error nodes	Solving the problem of the efficiency of the Byzantine fault tolerance
The 2010s	Ultralarge scale	Nodes in the network	Tolerating Byzantine error nodes and focusing on performance and safety	Achieving open and transparent public accounts
The 2020s	Giga scale	People-machine-thing, full time and space, intelligent terminal	Intelligent, humanized interactive node	Configurable, fine-grained value delivery

packaged according to certain rules. After the packaging is completed, the results will be broadcasted and passed to other nodes for verification, and, finally, a consensus will be reached. The more classic blockchain consensus algorithms are shown in Table 2.

On this basis, many new algorithms based on the aforementioned consensus mechanism have emerged. Proof of activity [31] is a combination of PoW and PoS. It has been developed in the wake of an assumption based on an economic phenomenon called "Tragedy of the Commons." Practical Byzantine Fault Tolerance (PBFT) [32] is designated as more efficient than PoW in terms of latency and energy consumption, and it can only tolerate up to 33% of malicious nodes. Liu et al. [33] developed a novel consensus mechanism called Proof of Collaborative Work.

In the Internet of Vehicles, participants have a large number of devices with substantial differences, and they are easily affected by external environments such as regions and communication environments. Traditional consensus algorithms have insufficient transaction processing capabilities. There has also been some new consensus mechanism for the Internet of Vehicles [34, 35]. Nodes or devices with superior resources are in an advantageous position in the blockchain, which is prone to the phenomenon of the winner winning forever.

3. System Overview

In the ecosystem of the Internet of Vehicles, it is necessary to consider a large number of participants and the susceptibility to real factors such as geographic area and communication environment. The traffic system in the environment of the Internet of Vehicles is a complex system in which various parts are intertwined and interact with each other. It is necessary to pay attention to related safety issues such as the reliability and effectiveness of the system.

The factors that need to be considered for the safety of the Internet of Vehicles are shown in Figure 2.

3.1. System Model. In this section, we will demonstrate the system model.

As shown in Figure 3, the system consists of the following parts:

(1) Traffic management center (TC) is the highest authority on the Internet of Vehicles. It is connected to the roadside unit (RSU) and is mainly responsible for the registration of traffic participants and core information processing. The permanent identity and temporary identity of the vehicle are directly or indirectly related to the TC. It is considered completely credible and able to complete the work according to the design without being compromised by the adversary. As a complete node of the blockchain, it generates genesis blocks. It is responsible for mining and issuing and uploading various equipment official certificates to the blockchain ledger.

(2) Roadside units (RSUs) are distributed at intersections and on both sides of the road to generate vehicle access, identity verification, and other related matters. RSUs are considered as the edge computing node [36] that hosts the blockchain.

(3) Vehicle (V) is a general term for all types of vehicles driving on the road and represents the main participants of the network, namely, intelligent vehicles. Each vehicle can maintain its blockchain account and accompanying public and private key pairs and addresses on the blockchain. However, there are differences in computing power between different manufacturers and different types of in-vehicle devices.

(4) The operation of the blockchain relies mainly on four components: encryption algorithm, transaction processing, consensus algorithm, and distributed ledger technology. Using the encryption algorithm in the blockchain, a unique public-private key pair and wallet address are generated for each participant of the Internet of Vehicles.

Assume that all devices can protect their private keys from being obtained by others.

For vehicle information, we classify it as follows:

Table 2: Classic blockchain consensus.

Consensus mechanisms	Core concept	Pros	Cons
PoW	Computing power competition	It is completely decentralized to avoid the risks of concentration	The computing resources waste a lot, and the process of reaching a consensus takes a long time
PoS	Financial power competition	It shortens the time for a consensus to reach and avoids wasting power	Under the control of a few wealthy nodes, there is the possibility of unfairness
DPoS	Election and voting	It drastically reduces the time for a consensus to reach the second level	It is easy to be dominated by some nodes, and the voting representative may have doubts

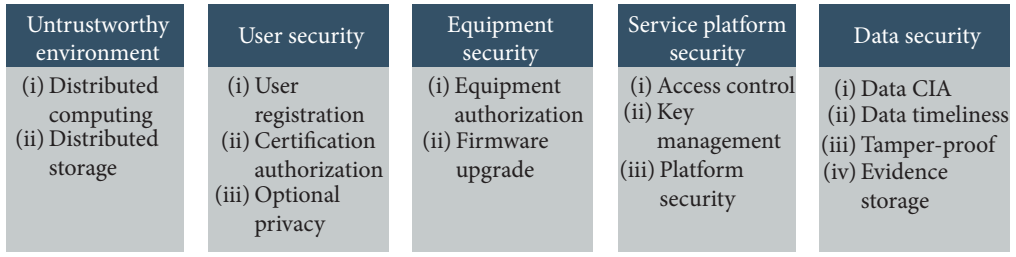

Figure 2: The factors for the safety of the Internet of Vehicles.

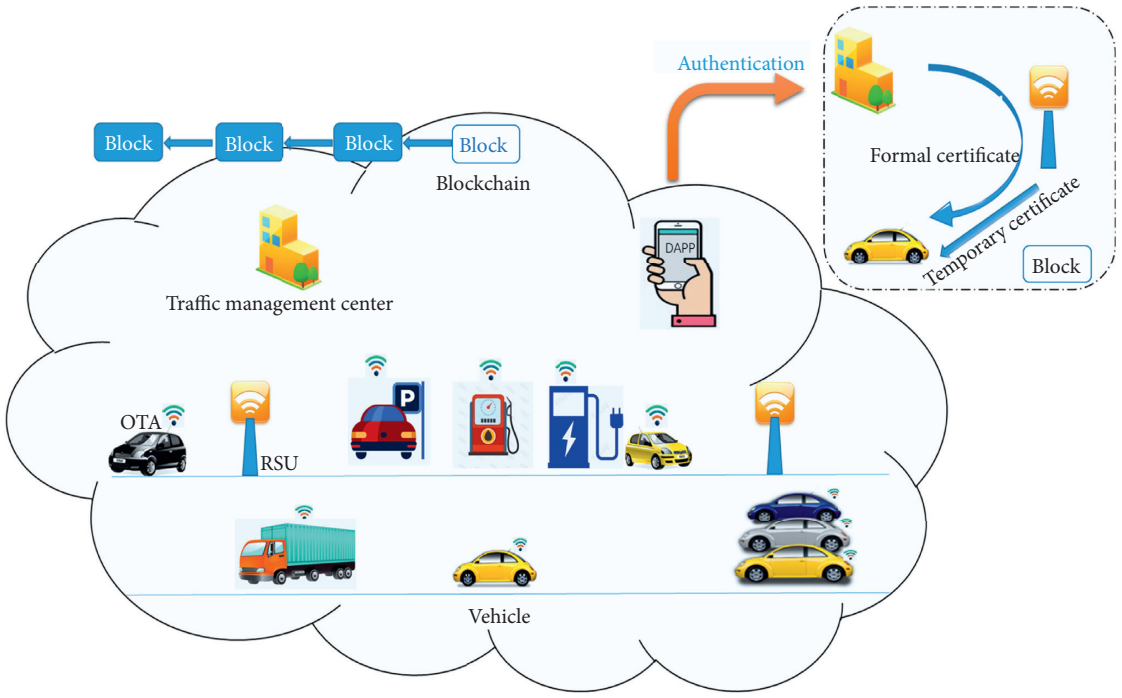

Figure 3: System model of IoV.

(i) General information

(ii) Sensitive information

Among them, general information includes license plates, models, brands, and colors, and sensitive information includes car owner information and vehicle identification number (VIN).

3.2. Proposed Overall Architecture. In this scheme, the main objects are devices on the Internet of Vehicles, including the aforementioned traffic management center, roadside units, and vehicles. Assume that every device can run the blockchain client and can protect its account.

In the initialization phase of the system, each device needs to run a blockchain client, complete the initialization

of the blockchain, and generate basic blockchain information (public key, private key, address, etc.).

The specific process is as follows.

3.2.1. Transportation Equipment Establishment Stage. After TC and RSU enter the Internet of Vehicles system supported by blockchain, the device will generate unique public and private key pairs and wallet addresses as part of its information. Then, Roadside unit RSU_i encrypts its attribute information (device serial number, location coordinates, etc.) with pk_{TC}, signs on it, and sends it to TC to apply for a device certificate.

When Tc receives an identity application request from RSU_i, it first verifies the digital signature of the application information. After verification, TC designed the authentication key for RSU_i $k_i = \{u_i | (u_i, v_i) = pk_{TC}\, sk_{RSUi} \bmod p\}$, encrypting ($k_i$, $address_i$) with the public key of RSU_i and writing it to the blockchain as the certificate of the RSU_i after TC signature.

It is worth noting that a timestamp is attached to the transaction after it is written to the blockchain, which ensures the traceability of the transaction. This can also be used to manage and maintain certificates.

3.2.2. Vehicle Equipment Establishment Stage. When a vehicle enters the Internet of Vehicles ecosystem for the first time, the registration needs to be completed for easy management. Therefore, it is necessary to apply to the Internet of Vehicles to obtain identification. Considering that the process of writing a transaction to the blockchain takes a nonnegligible time, in response to this, we design a type of temporary certificate to facilitate the timely connection of vehicles before the vehicle is officially certified.

The process of generating a temporary certificate is as follows:

(1) RSU_i broadcasts its signed identity certificate periodically.

(2) The vehicle j receives the broadcast information; it uses the public keys of TA and RSU_i to verify the legitimacy of the identity.

(3) If the signature is legal, it is determined that the RSU_i is credible, and the vehicle encrypts its attributes (attributes consist of two parts: general information authentication is encrypted with pk_{RSUi}, and sensitive information is encrypted with pk_{TC}).

(4) The vehicle signs the information and sends it to RSU_i. RSU_i verifies the signature, and it can decrypt the general information, perform preliminary authentication, and issue a lightweight temporary certificate ($address_{V_j}$ || timeliness || $addressRSU_i$ || RSU_i signature). The validity period of the certificate must be greater than the time it takes for things to be written on the blockchain.

(5) After receiving the temporary certificate, the vehicle verifies the signature and uses it as a temporary identity in the system to participate in the operation and maintenance of the system.

(6) RSU_i encrypts the general attributes of the received vehicle with the key k_i and attaches the encrypted sensitive information and a temporary certificate as a blockchain transaction. After completing the consensus agreement, it will be written into the blockchain.

As the complete nodes of the blockchain, RSU and TA are jointly maintained and can read and write data on the blockchain.

The process of generating a formal certificate is as follows.

(1) TA gets the transaction generated by the RSU_i in the blockchain.

(2) TA completes the decryption of the data and verifies the data signature. What we need to highlight here is

(3) $k_i = \{u_i | (u_i, v_i) = pk_{TC}\, sk_{RSUi} \bmod p\} = \{u_i | (u_i, v_i) = pk_{RSUi}\, sk_{TC} \bmod p\}$.

(4) This ensures that TC and RSU can calculate the same key without revealing their private key.

(5) Decrypt and verify the data. Then, TC issues a formal certificate ($address_{V_j}$ || timeliness || TA's signature) to the vehicle to complete the formal registration and certification. TC writes it into the blockchain as a transaction.

The notations in this paper are summarized in Table 3.

3.3. Fair Consensus Mechanism. We propose a consensus mechanism AoR, dedicated to the consortium blockchain. The commissioners maintain the blockchain.

3.3.1. Role Classification of Blockchain Nodes. There are three roles in the consensus mechanism:

Ordinary node (U): as the fundamental aspect of blockchain, they use cryptography to verify their identity and use the signature to verify their information sent. Ordinary nodes can join or leave the network without restriction. They are not permitted to participate in the block generation process directly but can "observe" the entire consensus process. They also can be involved in the process of block distribution and message forwarding and get a small number of online credit rewards.

Commissioners (C): different commissioners form the committee and maintain a consortium blockchain jointly. The commissioners exercise equal rights and obligations, reviewing bidders and organizing auctions, and verifying and forwarding blocks and transactions. A new block generated in the blockchain will be sent to all commissioners for verification signature. When a block receives at least 51% of the commissioners' approval, it will add to the blockchain as valid. The

Table 3: Summary of notations.

RSU_i	Roadside unit i
V_j	Vehicle j
p	Prime number in elliptic curve cryptography
k_i	The authentication key for RSU_i
pk_x	The public key of device x in the blockchain
sk_x	The private key of device x in the blockchain
$address_x$	The address of device x in the blockchain
N_u	The number of ordinary nodes
N_c	The number of commissioners
T_w	Each round of auction interval
T_a	The time of the vendee is determined
T_b	The time of new block be packaged
$T_{newblock}$	A new block's deadline
$b_{i,t}$	The credit of node i at time t

commissioners will be rewarded. The result of the vote will be the choices of all commissioners.

Bidder (B): in each round of auction, the ordinary node is required to submit a deposit within the specified time. The bidder competes for the right to generate the new block. Within the specified time, the bidder is ranked by the auction mechanism to determine the vendee (V). At the same time, the vendee's credit for the transaction price is used to reassign to the online nodes, and a block is generated in the blockchain. After completing the task, the vendee receives the corresponding reward.

3.3.2. Consensus Process. The AoR consensus assumes that the number of ordinary nodes is N_u, the number of commissioners appointed from ordinary nodes is N_c, and each auction interval is T_w. The vendee is determined within time T_a, and a new block needs to be generated within the time T_b, $T_a + T_b \ll T_w$. The valid block records the whole process of the auction transaction and gets $(N_c/2) + 1$ commissioners' signature at least. This process is known as a round of consensus. If no valid block is generated within T_b, it means that the original vendee has given up the right to generate the new block and the second highest bidder will generate the block as a winner and so on. As long as one bidder can work properly, the network can achieve a consensus finally.

Generating a new block requires the following steps:

S1. At the beginning of the chain, all nodes are assigned a certain amount of participation credit, and all nodes can trade each other and generate signed transaction data. At the same time, they verify the transaction data. If the transaction data are valid, they will forward the transaction data to the commissioners. The online task will be assigned a credit bonus after each round of the auction.

S2. All commissioners monitor the transaction data and store the legal data in the transaction pool.

S3. The vendee takes the valid transactions from the transaction pool and packs them into a block, sending the block to all commissioners. The block's deadline is

$$T_{newblock} = \text{PreviousBlockTime} + T_a + T_b. \quad (1)$$

S4. After receiving a raw block, the commissioner verifies the data in the block. If the commissioner approves this block, it shall sign for confirmation. After receiving at least $(N_c/2) + 1$ signatures, the vendee obtains the timestamp information of the NTP server. If the timestamp is earlier than $T_{newblock}$, the block will be signed by the vendee and published on the network. The committee accepts the vendee's credit and allocates it. If the timestamp is later than $T_{newblock}$, it means that the new block cannot be generated efficiently. The vendee will be replaced by the auction mechanism, and the specified task should be completed within the new deadline $T_{newblock} = T_{newblock} + T_b$. The former vendee who failed to complete the task will be liable. This mechanism prevents nodes from poor performance and malicious motives.

S5. After receiving the valid block, the vendee deletes the illegal transactions from the transaction pool. Moreover, all nodes wait for the time T_w to start the next round of the auction.

In particular, if $T_{newblock} > T_w$, it means that all bidders cannot complete the generation of the new block in time, or the network has truncated. In this article, we assume that the above situation does not transpire. The various relationships of the characters are given in Figure 4.

4. Experiments and Performance Analysis

In the scheme mentioned in this article, the system security is based on the difficult problem of the elliptic curve discrete logarithm problem (ECDLP). Each device node participating in the Internet of Vehicles can generate its private key, public key, and address according to the protocol and can use TA's public key to generate an encryption key.

4.1. Safety Analysis

(i) The adversary cannot get the private key of the IoV device:

Any node, including the adversary, can collect the public keys and system parameters of all nodes in the scheme, which is also a prerequisite guarantee for the use of blockchain. As mentioned earlier, we assume that any node can protect its private key from being acquired by an adversary. The adversary cannot calculate the encryption key. If the adversary calculates the private key of the node through the public parameters and public key, it violates the difficult problem of ECDLP. Therefore, the probability of the adversary compromising in our scheme is negligible.

(ii) The anonymity of the vehicle:

Whether it is a temporary certificate or a formal certificate, it only contains the blockchain address of the vehicle and does not contain any information

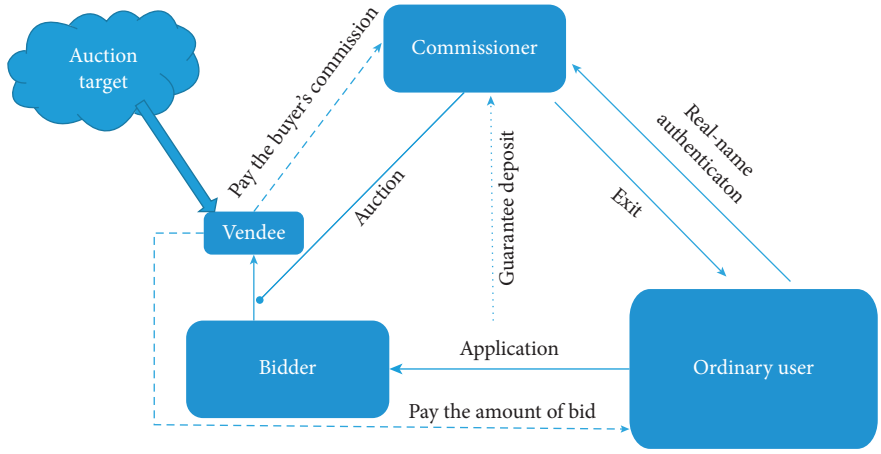

Figure 4: Interaction of various roles in the network.

related to the identity of the vehicle. The private information of the vehicle is encrypted with the public key of the TC. As long as the private key of the TC is not exposed, the private information of the vehicle can only be obtained by the TC.

(iii) Sybil attack protection:

In a network, the attacker simulates the existence of multiple entities (devices), that is, a single node has multiple identities. These entities send erroneous information to the server or management application weakening the role of redundant backup. In our design, each object can only have one formal certificate at a given time, and each identity can only have one key pair. Every communication message must be signed by the private key associated with this identity. Moreover, all formal identities must be approved by the traffic management center, so attackers cannot use forged identities.

(iv) DoS/DDoS protection:

Denial of service (DoS) or distributed DoS (DDoS) attacks are characterized by an explicit attempt by the attacker to prevent legitimate use of the service [37]. Since DoS/DDoS does not need to identify and utilize protocol or service flaws, they are highly efficient for any type of service and are therefore the most dangerous network attack. The decentralized architecture of the blockchain makes it powerful against DoS/DDoS attacks. The data on the blockchain is redundant and distributed on different nodes. Even if an attacker manages to stop one node, it cannot stop all other nodes. In addition, transactions in the blockchain require a certain cost, which prevents an attacker from sending a large number of transactions to attack.

4.2. Consensus Fairness Analysis. Based on the auction mechanism and the consortium blockchain, this paper proposes a new consensus model. The consensus mechanism needs a trade-off between performance, fairness, and security. Our model will guarantee fairness on the premise of blockchain security. In the following, we will analyze the fairness and effectiveness of AoR.

Suppose that N nodes share B credits $N > 3$, and Nc represents the number of committees considered; $t = 0, 1, 2 \ldots, T$ is the index of the period. At time t, the credit of node i is represented by $b_{i,t}$. Assume that the total credits are distributed equally among the participating nodes in the initial stage. That is, for any node, $b_{i0} = B/N$.

During the operation of the blockchain, the credit updates of different nodes are as follows:

$$\text{Ordinary nodes: } b_{i,t+1} = b_{i,t} + (1/N - 1 - Nc)\alpha x_{\mathrm{v,t}}$$
$$\text{Vendee: } b_{v,t+1} = b_{v,t} - x_{\mathrm{v,t}} \quad \text{s.t.} \quad x_{\mathrm{v,t}} < b_{v,t}$$
$$\text{Commissioners: } b_{c,t+1} = \alpha b_{c,t} + (1/Nc)\beta x_{\mathrm{v,t}}$$

$x_{\mathrm{v,t}}$ represents the amount of credit used by Vendee v at a time t, α is the proportion of the auction price, and β is the proportion of Commissioner's commissions and satisfies $\alpha + \beta = 1$.

Proposition 1. *At any given moment t, the sum of credits assigned to each node is certain.*

Proof. At $t = 0$, the sum of node credits is initialized to $\sum_0^N b_{i0} = B$. Considering the previous assumptions, no node in the system carries credits away, and no new credits are generated in the life cycle. Therefore, the sum of credits of each node remains constant, B.

This method can prevent some nodes from occupying the generation right for a long time. Because spending credit $x_{\mathrm{v,t}}$ means that other nodes will have a higher credit budget at a time $t + 1$. This movement of credit guarantees fairness among nodes.

Proposition 2. *At any time t, for any two nodes i and j,* $|\sum_0^t x_{i\tau} - \sum_0^t x_{j\tau}| < (N - 2/N - 3)B$. *N is the total of nodes, and* $x_{i\tau}$ *is the cost of node i at time* τ.

Proof. Consider the extreme case. At time $t = 0$, all credits belong to node i, $b_{i0} = B$ (actually $b_{i0} < B$). Other nodes have zero credit.

After the node i completes the first auction, the x_i transaction value is at most B, and node j gets the credit $b_j = (B/N)$. To minimize x_j, it assumes that node j never bid. Node i can collect up to $b_i = (N - 2/(N-1)^2)B$ before the next bid.

After the second round, x_i receives up to $(N - 2/(N-1)^2)B$.

And so,

$$\begin{aligned}\sum_0^t x_{i\tau} &< B\left(1 + \frac{N-2}{(N-1)^2} + \frac{(N-2)^2}{(N-1)^4} + \frac{(N-2)^3}{(N-1)^6} + \cdots \frac{(N-2)^t}{(N-1)^{2t}}\right)\\ &< B\left(1 + \frac{N-2}{(N-2)^2} + \frac{(N-2)^2}{(N-2)^4} + \frac{(N-2)^3}{(N-2)^6} + \cdots \frac{(N-2)^t}{(N-2)^{2t}}\right)\\ &< B\left(\frac{1-\left(1/(N-2)^t\right)}{1-(1/N-2)}\right)\\ &< \frac{N-2}{N-3}B.\end{aligned} \tag{2}$$

Thus, $|\sum_0^t x_{i\tau} - \sum_0^t x_{j\tau}| \le |\sum_0^t x_{i\tau}| < (N - 2/N - 3)B$.

The time-averaged expenditure credit difference between any two nodes is

$$\lim_{t\longrightarrow\infty} \frac{1}{t}\left|\sum_0^t x_{i\tau} - \sum_0^t x_{j\tau}\right| < \lim_{t\longrightarrow\infty} \frac{1}{t}\left|\frac{N-2}{N-3}B\right| = 0. \tag{3}$$

This means that the sum of credits for all nodes' expenditures tends to be the same. No node can spend more credits and take the dominant position. The aforementioned ensures fairness between nodes.

4.3. Performance Analysis

4.3.1. Encryption and Signature Performance. We conducted experiments on a 1.9 GHz processor, Intel Core i5 with 12 GB RAM, and Windows 10 running in python3.7 to study operating costs. Figure 5 depicts the time-consuming signature and verification, encryption, and decryption. The average time consumption of signature and verification is 9.6 ms and 0.34 ms. The average time consumption of encryption and decryption is 182.6 ms and 62.8 ms. It can be found that signature and encryption take more time than verification and decryption. However, the above operations are tolerable in terms of time consumption.

4.3.2. Consensus Algorithm Analysis. In this part, the simchain (https://github.com/YaoyaoBae/simchain) is used to evaluate the time consumption. As described in Section 3, we simulated 200, 500, and 1000 nodes participating in the generation of blockchain 40 times and compared the consensus mechanism we designed with PoW under the same conditions.

Figure 6 depicts the time it takes for nodes to reach a consensus. Figures 6(a)–6(c) depict the consensus system time consumption for 200, 500, and 1000 node scales, respectively. In PoW, it takes a long time to solve the hash puzzle, so we assume that 20%–60% of the nodes randomly participate in each round. However, in the AoR simulation, only a brief bid is submitted in each round of consensus, and we assume that all nodes participate. For each scale, we perform 40 experiments. In all three cases, AoR takes much less time than PoW. Figure 6(d) describes the consequences of AoR in networks with various node quantities. The collection and validation of transactions and the selection of the bid order by the ledger manager consume some time costs. Besides, these tasks are influenced by the size of the network.

5. Comparison with Related Work

The advancement of the Internet of Things technology has promoted the development of the Internet of Vehicles with autonomous vehicles and roadside infrastructure as the main components. IoV aims to provide innovative services for different traffic equipment through adaptive traffic management and to improve traffic safety and efficiency. In this section, we compare the functions of our scheme with the existing schemes.

A paper [4] proposes an efficient and practical pseudonymous authentication protocol with conditional privacy preservation. It expects an honest-but-curious behavior from otherwise fully trusted authorities. The proposed protocol protects a user's privacy until the user honestly follows the protocol. In case of malicious activity, the true identity of the user is revealed to the appropriate authorities.

The authors proposed a new identity-based (ID) signature based on the elliptic curve cryptosystem (ECC) and employed it to propose a new conditional privacy-preserving authentication scheme based on the ID-based signature they invented [38]. The scheme provides a secure authentication process for the information transmitted between the vehicle and the RSU.

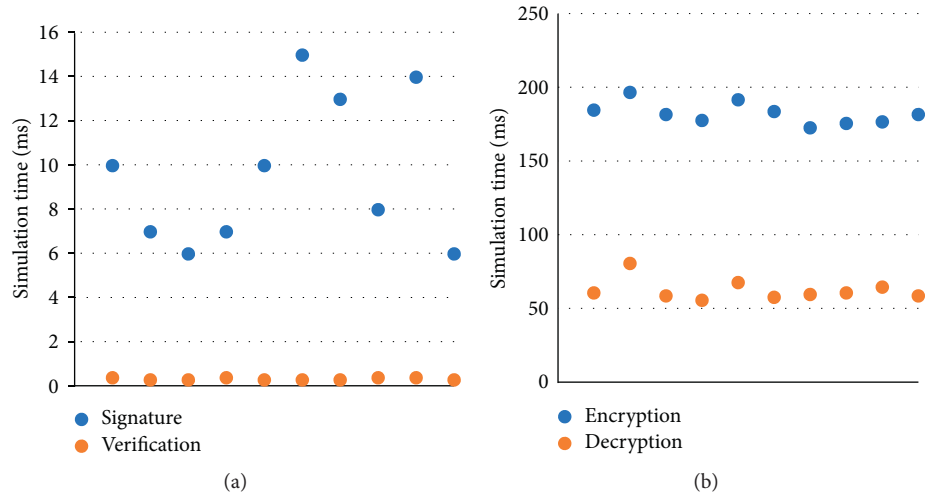

Figure 5: Time consumption of the basic operations. (a) Signature and verification. (b) Encryption and decryption.

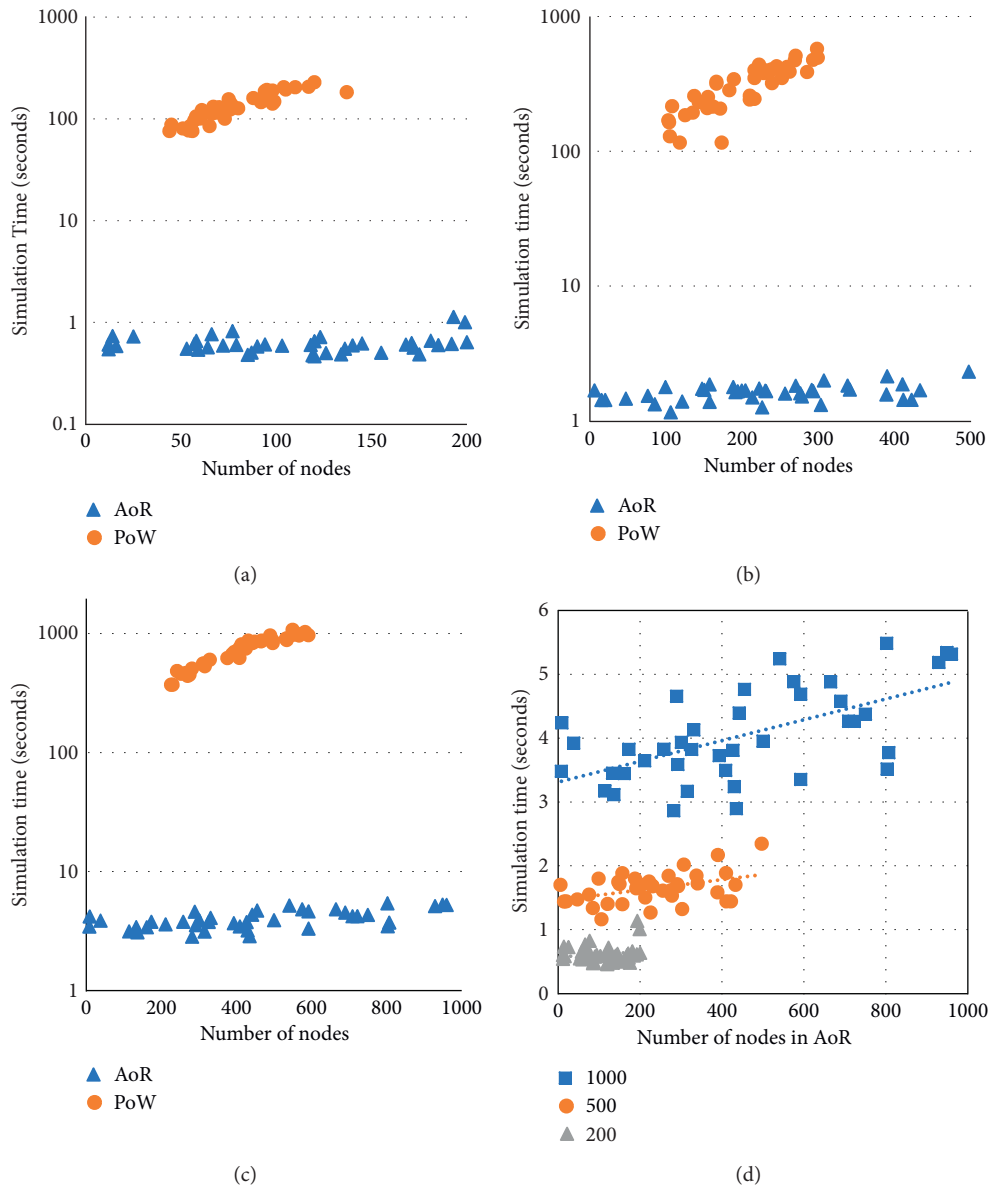

Figure 6: Time consumption of AoR and PoW.

Table 4: Comparisons of the related work.

Scheme	Anonymity	Authentication	Traceability	Decentralization	Certificate permanency
Lo's scheme [38]	Yes	Yes	Yes	No	Yes
Rajput's scheme [4]	Yes	Yes	Yes	No	Yes
Azees's scheme [3]	Yes	Yes	Yes	No	Yes
Wang et al. [7]	Yes	Yes	Yes	Yes	Yes
Pu's scheme [13]	Yes	Yes	Yes	Yes	Yes
Our scheme	Yes	Yes	Yes	Yes	Optional

In [3], Azees et al. propose an efficient anonymous authentication scheme to avoid malicious vehicles entering the VANET. Besides, the proposed scheme offers a conditional tracking mechanism to trace the vehicles or roadside units that abuse the VANET. As a result, the scheme revokes the privacy of misbehaving vehicles to provide conditional privacy computationally efficiently, through which the VANET entities will be anonymous to each other until they are revoked from the VANET system.

Javaid et al. [12] proposed a blockchain-based protocol for IoV using smart contracts, physical unclonable functions (PUFs), certificates, and a dynamic Proof-of-Work (dPoW) consensus algorithm. The blockchain with smart contracts provides a secure framework for registering trusted vehicles and blocking malicious ones. PUFs are used to assign a unique identity to each vehicle via which trust is established. Certificates are issued by roadside units that preserve the privacy of vehicles, whereas the dPoW consensus allows the protocol to scale according to the incoming traffic generated by the vehicles.

The authors introduced an efficient, reliable, and privacy-preserving scheme based on blockchain for VSNs [13]. In their scheme, a pseudonym mechanism is employed to achieve individual anonymization by concealing the vehicles' identity. To encourage vehicles to report trustworthy information, incentive punishment mechanism is proposed. Meanwhile, they propose a multifactor and single-factor weight-based evaluation mechanism to evaluate the reliability of the message. Practical Byzantine Fault Tolerance (PBFT) and blockchain are also employed to achieve consensus and store records, respectively, which can prevent malicious entities from manipulating vehicles' reward scores and credit scores.

To summarize, Table 4 describes the studied works. From the table, we can find that our scheme is used in a variety of scenarios and more comprehensive and suitable for IoV.

6. Conclusions

The latest development of the Internet of Things has promoted the evolution of the Internet of Vehicles. IoV aims to provide new and innovative services for different modes of transportation through adaptive traffic management to improve traffic safety and efficiency. However, due to the actual untrusted environment, establishing trust in IoV is a critical security issue. Therefore, we proposed an authentication with optional privacy preservation. In our scheme, we mainly consider two situations. One situation is that the vehicle temporarily enters the system, and the scheme is designed for temporary authentication. Another situation is that the vehicle has been participating in the Internet of Vehicles for a long time, and the program has been designed for formal certification. In the authentication process, the scheme inherits the decentralized, credible, and tamper-proof characteristics of the blockchain. At the same time, the certificate uses the cryptographic primitives in the blockchain, without using a new one. Furthermore, we design a new consensus mechanism that provides a fair chance for nodes in the blockchain to obtain bookkeeping rights. Security analysis and experimental results show that our scheme is efficient and secure for IoV devices.

In future work, we consider using aggregation technology [39] and coordination control [40] to process data to facilitate the use and transmission of data. For a wider range of Internet of Vehicles applications, we will consider upgrading the chain structure [41, 42] of the blockchain to reduce the resource consumption and transaction processing time of the blockchain.

Data Availability

No additional data were used to support this study.

Conflicts of Interest

The authors declare that there are no conflicts of interest regarding the publication of this paper.

Acknowledgments

This work was funded by the Postgraduate Research and Practice Innovation Program of Jiangsu Province under Grant KYCX18_0903.

References

[1] F. Yang, S. Wang, J. Li, Z. Liu, and Q. Sun, "An overview of internet of vehicles," *China Communications*, vol. 11, no. 10, pp. 1–15, 2014.

[2] WHO Organization, *Global Status Report on Road Safety 2018: Summary*, World Health Organization, Geneva, Switzerland, 2018.

[3] M. Azees, P. Vijayakumar, and L. J. Deboarh, "EAAP: efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 18, no. 9, pp. 2467–2476, 2017.

[4] U. Rajput, F. Abbas, and H. Oh, "A hierarchical privacy preserving pseudonymous authentication protocol for VANET," *IEEE Access*, vol. 4, pp. 7770–7784, 2016.

[5] P. Vijayakumar, M. Azees, A. Kannan, and L. J. Deborah, "Dual authentication and key management techniques for secure data transmission in vehicular ad hoc networks," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 1015–1028, 2015.

[6] M. Li, L. Zhu, and X. Lin, "Efficient and privacy-preserving carpooling using blockchain-assisted vehicular fog computing," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4573–4584, 2018.

[7] K. Wang, J. Yu, X. Liu, and S. Guo, "A pre-authentication approach to proxy re-encryption in big data context," *IEEE Transactions on Big Data*, 2017.

[8] M. Du, K. Wang, Y. Chen, X. Wang, and Y. Sun, "Big data privacy preserving in multi-access edge computing for heterogeneous internet of things," *IEEE Communications Magazine*, vol. 56, no. 8, pp. 62–67, 2018.

[9] S.-C. Cha, J.-F. Chen, C. Su, and K.-H. Yeh, "A blockchain connected gateway for BLE-based devices in the internet of things," *IEEE Access*, vol. 6, pp. 24639–24649, 2018.

[10] R. Sharma and S. Chakraborty, "Blockapp: using blockchain for authentication and privacy preservation in IoV," in *Proceedings of the 2018 IEEE Globecom Workshops (GC Wkshps)*, pp. 1–6, IEEE, Abu Dhabi, UAE, December 2018.

[11] C. Xu, H. Liu, P. Li, and P. Wang, "A remote attestation security model based on privacy-preserving blockchain for V2X," *IEEE Access*, vol. 6, pp. 67809–67818, 2018.

[12] U. Javaid, M. N. Aman, and B. Sikdar, "A scalable protocol for driving trust management in internet of vehicles with blockchain," *IEEE Internet of Things Journal*, vol. 7, no. 12, pp. 11815–11829, 2020.

[13] Y. Pu, T. Xiang, C. Hu, A. Alrawais, and H. Yan, "An efficient blockchain-based privacy preserving scheme for vehicular social networks," *Information Sciences*, vol. 540, pp. 308–324, 2020.

[14] M. Swan, *Blockchain: Blueprint for a New Economy*, O'Reilly Media, Inc., Sebastopol, CA, USA, 2015.

[15] M. Wu, K. Wang, X. Cai, S. Guo, M. Guo, and C. Rong, "A comprehensive survey of blockchain: from theory to IoT applications and beyond," *IEEE Internet of Things Journal*, vol. 6, no. 5, pp. 8114–8154, 2019.

[16] J. Sengupta, S. Ruj, and S. Das Bit, "A comprehensive survey on attacks, security issues and blockchain solutions for IoT and IIoT," *Journal of Network and Computer Applications*, vol. 149, Article ID 102481, 2020.

[17] M. A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, and H. Janicke, "Blockchain technologies for the internet of things: research issues and challenges," *IEEE Internet of Things Journal*, vol. 6, no. 2, pp. 2188–2204, 2018.

[18] S. Chen, L. Yang, C. Zhao, V. Varadarajan, and K. Wang, "Double-blockchain assisted secure and anonymous data aggregation for fog-enabled smart grid," *Engineering*, 2020.

[19] N. Kshetri, "Can blockchain strengthen the internet of things?" *IT Professional*, vol. 19, no. 4, pp. 68–72, 2017.

[20] P. Treleaven, R. Gendal Brown, and D. Yang, "Blockchain technology in finance," *Computer*, vol. 50, no. 9, pp. 14–17, 2017.

[21] J. Zhang and M. Wu, "Blockchain use in IoT for privacy-preserving anti-pandemic home quarantine," *Electronics*, vol. 9, no. 10, p. 1746, 2020.

[22] H. Li, K. Wang, T. Miyazaki, C. Xu, S. Guo, and Y. Sun, "Trust-enhanced content delivery in blockchain-based information-centric networking," *IEEE Network*, vol. 33, no. 5, pp. 183–189, 2019.

[23] Y. Liu, K. Wang, Y. Lin, and W. Xu, "LightChain: a lightweight blockchain system for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3571–3581, 2019.

[24] W. Diffie and M. Hellman, "New directions in cryptography," *IEEE Transactions on Information Theory*, vol. 22, no. 6, pp. 644–654, 1976.

[25] R. Yegireddi and R. K. Kumar, "A survey on conventional encryption algorithms of cryptography," in *Proceedings of the 2016 International Conference on ICT in Business Industry & Government (ICTBIG)*, pp. 1–4, IEEE, Indore, India, November 2016.

[26] S. Nakamoto, Bitcoin: a peer-to-peer electronic cash system, 2008.

[27] X. Wang, H. Su, X. Wang, and G. Chen, "Fully distributed event-triggered semiglobal consensus of multi-agent systems with input saturation," *IEEE Transactions on Industrial Electronics*, vol. 64, no. 6, pp. 5055–5064, 2017.

[28] X. Wang, G.-P. Jiang, H. Su, and Z. Zeng, "Consensus-based distributed reduced-order observer design for LTI systems," *IEEE Transactions on Cybernetics*, 2020.

[29] H. Li, K. Wang, X. Liu, Y. Sun, and S. Guo, "A selective privacy-preserving approach for multimedia data," *IEEE Multimedia*, vol. 24, no. 4, pp. 14–25, 2017.

[30] V. Ortega, F. Bouchmal, and J. F. Monserrat, "Trusted 5G vehicular networks: blockchains and content-centric networking," *IEEE Vehicular Technology Magazine*, vol. 13, no. 2, pp. 121–127, 2018.

[31] I. Bentov, C. Lee, A. Mizrahi, and M. Rosenfeld, "Proof of activity," *ACM SIGMETRICS Performance Evaluation Review*, vol. 42, no. 3, pp. 34–37, 2014.

[32] M. Castro and B. Liskov, "Practical Byzantine fault tolerance and proactive recovery," *ACM Transactions on Computer Systems*, vol. 20, no. 4, pp. 398–461, 2002.

[33] Y. Liu, K. Wang, K. Qian, M. Du, and S. Guo, "Tornado: enabling blockchain in heterogeneous internet of things through a space-structured approach," *IEEE Internet of Things Journal*, vol. 7, no. 2, pp. 1273–1286, 2019.

[34] Y.-T. Yang, L.-D. Chou, C.-W. Tseng, F.-H. Tseng, and C.-C. Liu, "Blockchain-based traffic event validation and trust verification for VANETs," *IEEE Access*, vol. 7, pp. 30868–30877, 2019.

[35] R. Shrestha, R. Bajracharya, and S. Y. Nam, "Blockchain-based message dissemination in VANET," in *Proceedings of the 2018 IEEE 3rd International Conference on Computing, Communication and Security (ICCCS)*, pp. 161–166, IEEE, Kathmandu, Nepal, October 2018.

[36] C. Xu, K. Wang, P. Li et al., "Making big data open in edges: a resource-efficient blockchain-based approach," *IEEE Transactions on Parallel and Distributed Systems*, vol. 30, no. 4, pp. 870–882, 2018.

[37] J. Mirkovic and P. Reiher, "A taxonomy of DDoS attack and DDoS defense mechanisms," *ACM SIGCOMM Computer Communication Review*, vol. 34, no. 2, pp. 39–53, 2004.

[38] N.-W. Lo and J.-L. Tsai, "An efficient conditional privacy-preserving authentication scheme for vehicular sensor networks without pairings," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 5, pp. 1319–1328, 2015.

[39] J. Yu, K. Wang, D. Zeng, C. Zhu, and S. Guo, "Privacy-preserving data aggregation computing in cyber-physical social systems," *ACM Transactions on Cyber-Physical Systems*, vol. 3, no. 1, pp. 1–23, 2018.

[40] X. Wang, X. Wang, H. Su, and J. Lam, "Coordination control for uncertain networked systems using interval observers,"

IEEE Transactions on Cybernetics, vol. 50, no. 9, pp. 4008–4019, 2020.

[41] S. Popov, "The tangle," *White Paper*, vol. 1, p. 3, 2018.

[42] M. Du, K. Wang, Y. Liu et al., "Spacechain: a three-dimensional blockchain architecture for IoT security," *IEEE Wireless Communications*, vol. 27, no. 3, pp. 38–45, 2020.