A Blockchain-based Authentication Scheme and Secure Architecture for IoT-enabled Maritime Transportation Systems

Peiying Zhang, Yaqi Wang, Gagangeet Singh Aujla, Anish Jindal, Yasser D. Al-Otaibi

***Abstract*—Although modern Maritime Transportation Systems (MTS) have been extensively benefited from Internet of Things (IoT) technology, but still the risks and challenges in safety and reliability have increased substantially. The involvement of different maritime parties in the marine transportation flow scheduling and management further escalates these challenges. Thus, we need an IoT-based collaborative processing system that unifies the modular structure and integrates multiple modules involved in MTS. Moreover, the need for a shared and controlled access mechanism that cannot be manipulated or tampered by unauthorized parties is also essential requirement in MTS. Blockchain, as an emerging technology, has become a key tool in data security protection because of its non-tampering and non-forgery characteristics. Keeping in view of this aspect, in this paper, an IoT-based collaborative processing system based on blockchain is proposed for marine transportation flow scheduling and management. In addition, we propose a novel consensus mechanism based on Verifiable Random Function (VRF) and reputation voting to reduce the communication cost in blockchain consensus communication process. The proposed scheme has been validated in a simulated environment and the results illustrate that the scheme has obvious effect in resisting replay attack and camouflage attack. Furthermore, the optimized consensus mechanism improves the security by 8% and the transaction processing speed by 6% on the premise that the communication cost is basically unchanged.**

***Index Terms*—Maritime Transportation Systems, Internet of Things, Blockchain, Authentication Mechanism.**

I. Introduction

Intelligent Transportation Systems (ITS) have undergone a tremendous makeshift in their applications uncovering the areas that were not previously explored for general purpose such as space and underwater applications. This has been made possible with the recent advances in the communication and computation technologies where the data can be processed and transferred within the application-oriented quality of service demand requirements [1]. One of its impact is that it has led to the transformation in maritime systems in transportation making them more accessible and communicable. Then in turn, MTS are of vital significance for today's global business [2], [3]. The transportation of goods in large scale is being carried out by oil tankers, bulk carriers and container ships [4], [5]. Billions of tons of goods are transported on several major trade routes every year. With the increasing globalization of the market, world trade has increased more than three times since the last century [6]. As a result of this growth, ports and maritime traffic routes (known as regular itineraries) have become more crowded all over the world. Like most of the land /air transportation, the scope of maritime transportation is accredited through geographical (through its physical characteristics), commercial (by operation), and strategic (by command and control) dimensions spread over its own space. The geographical dimension is varied with respect to weather patterns but limited over the time as compared to strategic as well as commercial dimensions, i.e., much more dynamic considerations.

The popularity and deployment of 5G technology, has brought higher network communication efficiency. It has also promoted the rapid growth of the IoT in MTS [7], [8]. IoT provides various benefits to the transportation industry ranging from real-time tracking to remote management [9]. It is being used extensively in various application scenarios related to ITS [10], [11], which has attracted the attention of the marine transportation industry as well. This can be attributed to different possible autonomous technologies (such as computer-assisted navigation, global positioning systems, telematics, cargo racking, safety, etc) in MTS. With the development and growth of the maritime transportation industry, the marine traffic problem is becoming serious. Compared with the terrestrial communication system, the corresponding equipment of the ocean has lagged for decades. The development of IoT technology gives the marine transportation management system a new force [12]. More specifically, IoT equipment integrates the natural environment and the current situation of maritime transportation to provide more comprehensive and scientific decision-making for marine transportation scheduling and management [13], [14]. Moreover, IoT steadily drives

This work is partially supported by the Shandong Provincial Natural Science Foundation, China under Grant ZR2020MF006, partially supported by the Industry-university Research Innovation Foundation of Ministry of Education of China under Grant 2021FNA01001, partially supported by the Major Scientific and Technological Projects of CNPC under Grant ZD2019-183-006, partially supported by the Open Foundation of State Key Laboratory of Integrated Services Networks (Xidian University) under Grant ISN23-09, and partially supported by the Startup Fund provided by the Durham University, UK. (Corresponding authors: Gagangeet Singh Aujla and Peiying Zhang.)

Peiying Zhang is with the College of Computer Science and Technology, China University of Petroleum (East China), Qingdao 266580, China, and also with the State Key Laboratory of Integrated Services Networks, Xidian University, Xi'an 710071, China. (email: zhangpeiying@upc.edu.cn)

Yaqi Wang is with the College of Computer Science and Technology, China University of Petroleum (East China), Qingdao 266580, China. (email: wangyaqi.upc@qq.com)

Gagangeet Singh Aujla and Anish Jindal are with the School of Computing Science, Durham University, Durham DH1 3LE, UK. (email: gagangeet.s.aujla@durham.ac.uk, anish.jindal@durham.ac.uk)

Yasser D. Al-Otaibi is with the Department of Information Systems, Faculty of Computing and Information Technology in Rabigh, King Abdulaziz University, Jeddah 21589, Saudi Arabia (e-mail: yalotaibi@kau.edu.sa).

the maritime industry through digitization for better efficiency and greater transparency (just like it does in case of smart cities). It also supports satellite-inherent functionality that extends the current capability of MTS to remote areas by expanding its scale and extending its coverage. This transforms the traditional MTS into interoperable IoT-MTS ecosystems.

A. Motivation

Maritime technology is booming; however the maritime information security has lagged behind as compared with the land network security for decades. Therefore, many enterprises and experts all over the world began to pay attention to the network and information security of MTS including ships and ports. There is no doubt that the participation of IoT technology will greatly improve the speed and efficiency of information transmission [15], [16]. However, several information security issues are required to be tackled in order to realize the full potential of maritime industry. Some of these are highlighted below.

- The marine shipping industry is increasingly dependent on digital equipment and software. Many connected equipments can directly access sensitive information (like maritime route, safety plans), which increases the risk of information disclosure.
- At present, many safety standards and procedures followed in the shipping industry are out of date based on the old standards created in the past industrial era, which urgently needs to be upgraded and updated.
- The shipping industry supply chain is very long and involves many fields and participating entities. The information of all parties involved, including shipping agents, freight forwarders, shipping companies, ports, and other companies, is not well synchronized, which will bring opportunities for criminals to attack the systems.
- The integration of satellite services for monitoring purposes (like vessel monitoring), a huge amount of data (related to speed, position, etc.) is collected by different agencies (like fisheries) on a regular basis. But, the data is often utilized by other parties for effective decision making and processing and often moves through nonauthorized bodies. Thus, compliance of monitoring system regulations is also essential.
- The modern data MTS replace the conventional paper-based log books and adopt modern electronic ledgers that record the different operational and commercial activities. Even the monitoring data is logged for future use in case of any anomalies or misinterpretations. However, a shared and controlled log book that can be securely accessed by different MTS parties without being able to manipulate the records is very essential concern.

1) Research Questions: Summarizing all the above major concerns, there are many key research questions that must be resolved through adequate solutions. Some of these key Research Questions (RQ) are discussed below.

- **RQ1:** How to develop an IoT-based collaborative processing system that unifies the modular structure and integrates multiple modules (such as identity authentication, user management, information recording) for marine transportation flow scheduling and management.
- **RQ2:** How can we design and develop a shared and controlled ledger that cannot be manipulated or tampered by unauthorized parties and can be traceable and auditable if fabricated by any legitimate entity.
- **RQ3:** How to develop a mechanism that can secure the communications (including the personnel crew communications) to identify legitimate participants.

B. Research Approach and Contributions

In order to tackle these challenges and provide a controlled and shared access to the different involved parties in MTS, blockchain technique can be leveraged along with the use of IoT and advanced communication technologies. Undeniably, blockchain has been widely used in academia and industries because of its potential for distributed system management [17], [18]. The significant advantage of blockchain technology is that it maintains a distributed, authenticated, and synchronized transaction ledger without centralized management. Due to its advantages, it has been widely used in various sectors including healthcare, smart cities, financial, and transportation, for securing the underlying sector [19], [20]. Therefore, because of its main characteristics of decentralization, trust, and data encryption, blockchain makes it possible for the MTS to access massive terminals for identity authentication and solve the problem of information protection.

Based on the above discussion, the main contributions and ideas of this paper are as follows:

- An IoT-based collaborative processing system is presented for marine transportation flow scheduling and management. The system adopts a modular structure and integrates multiple modules such as identity authentication, user management, information recording, and so on.
- This paper analyzes the security problems and related research of marine equipment access and puts forward a new authentication mechanism. The authentication mechanism relies on blockchain technology and ensures data confidentiality and integrity in device access and information communication.
- Considering the characteristics of low bandwidth and high delay in marine system communication, we propose a blockchain consensus mechanism based on VRF algorithm and credibility voting mechanism to reduce the overall communication cost.

C. Organization of the Article

The rest of the paper is organized as follows. Section II discusses the existing literature on information security mechanisms and blockchain-based identity authentication for ITS. Section III presents the system model. In Section IV the proposed scheme for access authentication and collaborative processing system for MTS is presented. Section V highlights the simulation results and analysis and the paper is concluded in Section VI.

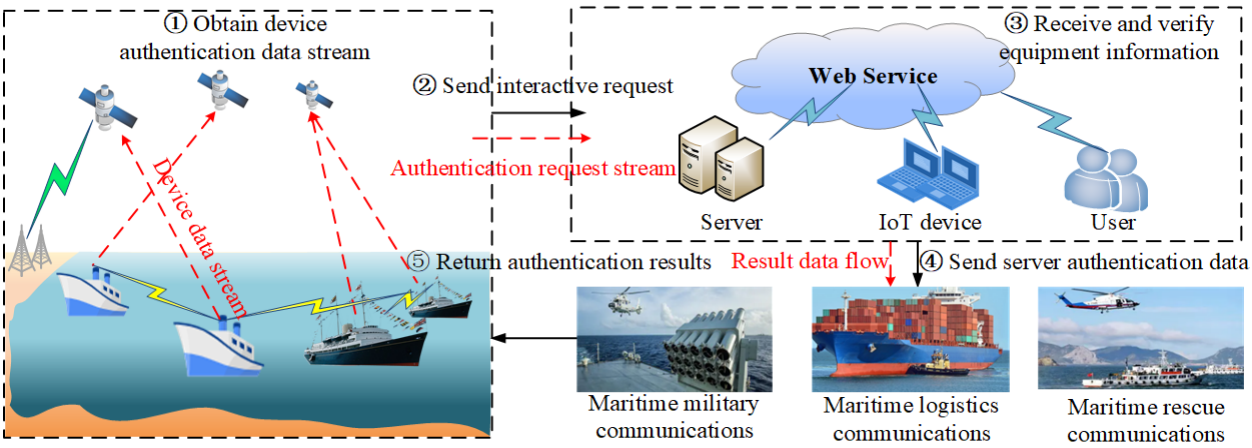

Fig. 1: Application scenario of access authentication in IoT-enabled MTS system.

II. Related Works

Various existing proposals have suggested solutions to the key research questions in ITS and related fields, although not specific to MTS. Some of these existing proposals are discussed below.

A. Information security mechanisms for ITS

For the information security of ITS, the authentication protocol based on privacy protection policy is the main method to ensure the integrity and reliability of message transmission and identity privacy security [21]. At present, the mainstream identity authentication mechanisms in the ITS are realized by using public key encryption technology based on a trusted third party, such as Public Key Infrastructure (PKI). For instance, in literature [22], on the basis of cryptography, location verification technology is used to reduce false attacks. The influence of forged location information is preliminarily analyzed. Thus, a more reliable train group network authentication scheme is adopted. The authors of literature [23] propose a privacy protection authentication scheme for vehicle network. The scheme combines Elliptic curve public key encryption and Software Defined Network (SDN). In literature [24], a privacy protected certificateless aggregate signature scheme is proposed to eliminate the complex certificate maintenance overhead. This scheme is suitable for lightweight vehicle networking.

However, with the increase of data volume and user demand in intelligent systems, there is an urgent need for a new mechanism that can not only meet the expanding demand of data volume and user demand, but also ensure the security of data and user privacy. Literature [25] introduces a real-time vehicle monitoring scheme based on blockchain. Among them, secure authentication is provided with the assistance of blockchain technology. The blockchain network architecture can promise that each node replicates and stores a database copy. Then if a node fails, the whole data will not be affected [26]. This characteristic sorts the thorny problems out in the current information security field, such as identity theft, data tampering and Distributed Denial of Service (DDoS). Therefore, the future development and application of blockchain technology can improve the network security index of the shipping industry.

B. Blockchain-based Identity Authentication in ITS

In essence, blockchain is a shared database wherein, the over-centralized IoT architecture makes the central server overloaded. This drawback not only causes system crash, but also leads to serious security risks. It is interesting to note that the decentralized feature of blockchain can reduce the pressure on the central server, prevent information from being tampered with and improve system security. Fig. 1 describes the application scenario of access authentication in IoT-enabled MTS system. The red dashed arrows represent the data flows and its direction, while the solid black arrows describe the interaction behaviors between the whole system. To some extent, the possibility of being attacked by hackers is directly proportional to the value of the target, so the shipping page should pay more attention to information security [27], [28]. Blockchain technology may bring new solutions to the network security of the shipping industry [29]. For instance, the authors of [30] group the nodes and then authorizes the blockchain. The aggregated authentication results were then uploaded to the central server to realize decentralized authentication. The mechanism proposed in [31] allows one node to apply different certificates. Then the blockchain network complete the encryption and information preservation of nodes. In [32], the authors use Elliptic Curve Cryptography (ECC) to realize the anonymous communication of vehicles. As a result, better performance and lower communication computing costs were obtained. The authors of literature [33] propose a decentralized data management system for intelligent and secure transportation. They apply blockchain and IoT in a sustainable intelligent urban environment to solve the problem of data vulnerability.

All these studies point to the applicability of blockchain in maritime industry to solve the issues related to authentication, data integrity and security. Based on the former researches, we hold the view that blockchain can provide decentralized security and privacy, providing a solution to the data security problems caused by over-reliance of systems on central servers.

C. Researches on blockchain consensus mechanism

A good consensus mechanism ought to ensure that the latest block is accurately added to a unique backbone, that nodes store the same block information, and that they can even resist malicious attacks. In the field of distributed systems, the consensus algorithm proposed by researchers is divided into two parts according to whether it supports Byzantine fault tolerance. One of the most important advantage of the Practical Byzantine Fault Tolerance (PBFT) consensus algorithm [34] is that it solves the low efficiency drawback of the original Byzantine fault-tolerant algorithm. Consequently, the complexity of the algorithm decreases from exponential level to polynomial level. The authors of [35] proposes to improve the Byzantine consensus mechanism with the help of credit authorization. The reputation value is added to the node attribute, so that the node with good reputation has a greater chance to obtain the block right. This idea not only retains the advantages of the original PBFT, but also reduces the probability of abnormal nodes participating. It also provides a new idea for us to solve the participation of unreliable nodes in the Internet of vehicles. In literature [36], the authors propose a multi-layer consensus mechanism based on PBFT to realize the application of PBFT mechanism in large-scale systems. The nodes are grouped hierarchically, so as to narrow the range of communication nodes. The mechanism has proved that the poor node problem scalability is solved by grouping mechanism. Hence, the improvement of PBFT consensus algorithm in the previous researches give us new inspiration in solving application problem of large-scale networks. Moreover, they make it possible for the consensus algorithm to be applied in practical scenarios.

III. Systerm Model for IoT-based Collaborative Processing in Maritime Transportation

In this section, we propose the architectural system model for access authentication and collaborative processing system for IoT-MTS ecosystem. Also, it is an IoT collaborative processing system for marine transportation flow scheduling and management. As illustrated in Fig. 2, the system adopts modular structure and integrates multiple modules. On the whole, the system is divided into three layers: the maritime IoT layer, the virtual node layer and the blockchain layer. The functionality these layers is discussed below.

Maritime IoT layer: This layer consists of several marine physical equipment, including sensor subsystem and IoT subsystem. The sensor subsystem is mainly deployed on the ship and in the channel. It is used to identify and collect the real-time information of the current ship, including the name, position, heading, speed, tonnage, etc. At the same time, combined with some environmental monitoring sensors, such as ocean current sensors and wind speed sensors, and integrating the natural environment and the current situation of shipping, it provides more comprehensive and scientific decision-making for marine transportation scheduling and management. In addition, the IoT subsystem connects each subsystem to the unified IoT through standardized protocols, so as to complete data transmission and collection. The control subsystem mainly maintains various sensors in the marine transportation IoT data processing system, simultaneous interpreting the current state of the sensor, unifying different sensor subsystems and accessing the interface of the IoT devices. The transmission layer mainly completes the data transmission and sends the data to the data collection equipment and shore based control center according to the transmission protocol specified by the control layer.

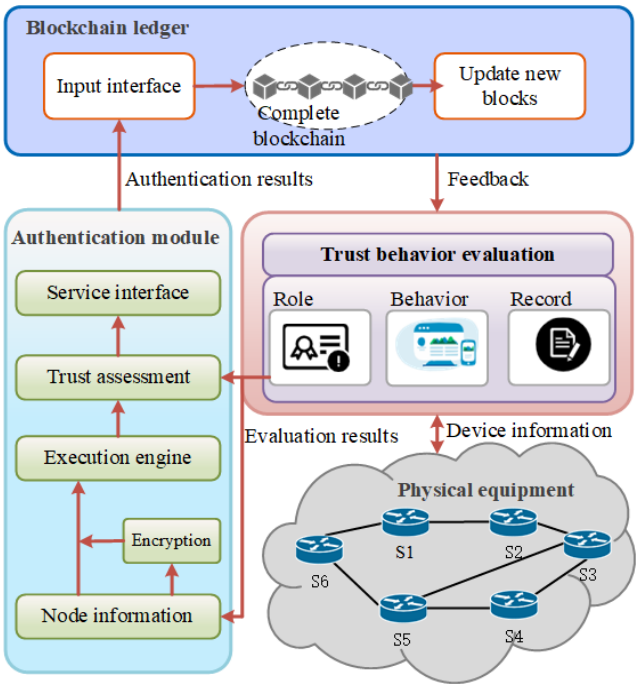

Fig. 2: The architecture of the collaborative processing system.

Virtual node layer: In this layer, the marine physical equipment is mapped as virtual nodes. The virtual nodes are divided into different virtual type according to the trust behavior authentication mechanism we proposed. The whole transportation network is abstracted as a virtual network composed of several nodes. Each node carries its important data, including identification, physical identification, authentication key or password.

Blockchain layer: Blockchain is connected by multiple blocks in the form of chain, and the later block will store the header hash value of the previous block. The essence of a block is the log data recorded in a consensus process, which represents the consensus result of the current round of consensus transactions. The consistent result is stored in Merkle tree and encrypted by hash algorithm. Then the hash value of the block is obtained by encrypted hash. Each block has the hash of the previous block, which helps the blockchain to achieve the invariance of its content. If the hacker tries to change the contents of the previous block, its original hash value will become invalid. Due to domino effect, hash values in subsequent blocks are also invalid.

In each layer of the architecture, several modules are included to cooperate to complete the information transmission and node authentication. In the maritime IoT layer, the intelligent terminal sensors collect data from the node itself and the

environment. The data is then sent to the security module in the second layer. Additionally, the security module senses the security of data and terminal operating environment, and finally submits the processing results to the communication module. The node authentication protocol, key information and security context will be delivered to the security module. Then the trust behavior authentication module comprehensively evaluates the service-oriented behavior trust value of the vehicle node according to its own attributes, perception information, interaction information and context environment provided by the vessel node. Finally, the third layer blockchain network receives node information and trust value to complete classification and security authentication.

IV. The proposed scheme

In this section, we present the proposed scheme that intends to address the research problem and questions raised concerning the IoT-MTS collaborative system. The different methods involved in the proposed scheme are discussed in the subsequent sections.

A. Behavior trust evaluation authentication method

The trust evaluation model proposed in this paper is measured by the role and behavior of nodes. The construction of traditional trust concept takes the legitimacy verification results of entity identity and access attributes by certification authority as a reference. However, the ship nodes involved in maritime transportation need frequent message communication, and its reliability is uncertain. The behavior centered trust relationship should reflect the credibility of the data itself, which needs to be rebuilt frequently due to the continuous changes of the network and perceived environment. Therefore, this method is more suitable for marine scenes with frequent changes in environment. $\Omega = \{\alpha_1, \alpha_2, \alpha_3, ..., \alpha_n\}$ is defined as the standard event library, which records maritime transportation information such as "traffic congestion". The ship information set is $\Psi = \{\gamma_1, \gamma_2, \gamma_3, ..., \gamma_n\}$, and the node type set is $V = \{v_1, v_2, v_3, ..., v_n\}$. Moreover, $s(v_i)$ represents the matching degree between the information and the standard events in the information base. We classify ships into six classes based on different categories and behaviors of maritime transportation business. They are assigned different levels of trust $\rho \in [0, 1]$. We are based on the assumption that vehicles with fixed business or official certification have a low probability of error. Table 1 shows one of our classification simulation schemes. In practical application, the management department can classify and assign values according to the actual situation of ships and current sea areas. Based on the different roles of nodes and individual behaviors in the MTS, we use the node type $\rho \in [0, 1]$, the reliability of information f and the safety state of nodes $\lambda \in [0, 1]$ as the reliability calculation index. Based on the above definition, when the vehicle node v_i sends event information e_i^j. The event corresponds to event a_j in the standard information base. The calculation formula of information reliability is as follows:

$$T(e_i^j) = F(f(\alpha_i, \lambda_j), s(v_i), \rho) \rightarrow [0, 1], \tag{1}$$

TABLE I: Mapping relationship between equipment type and information credibility.

Grade	Equipment type	Credibility range	Quantitative value
Q1	System server	(0.8, 1]	ρ=1
Q2	Traffic control vessel	(0.6, 0.8]	ρ=0.8
Q3	Public transport	(0.4, 0.6]	ρ=0.6
Q4	Repair vessel	(0.2, 0.4]	ρ=0.4
Q5	Private vessel	(0, 0.2]	ρ=0.2
Q6	Faulty vessel	(0, 0.1]	ρ=0.1

where $T(e_i^j)$ represents the confidence level. As for the trust degree of nodes, we consider the long term trust value of the platform and the short term trust vector calculated from the historical interaction behavior between nodes. The short term trust of nodes depends on the interaction behavior between nodes. Once there is interaction behavior between nodes, there will be short term trust between nodes. The short term trust vector ST_{ij} is obtained by the system checking the cumulative trust value f_i of nodes in this period.

$$ST_{ij} = \begin{cases} 1 & , \prod_{i=1}^{m} f_i \neq 0 \\ 0 & , f_i = 0 \end{cases} . \tag{2}$$

The long term trust vector LT_{ij} is derived from the vessel history interaction behavior, and the time attenuation factor γ^{n-k} is used in its calculation. This is based on the assumption that the earlier the interaction between nodes, the smaller the trust contribution between nodes.

$$LT_{ij} = \sum_{k=1}^{n} ST_{ik} \times \gamma^{n-k}, \tag{3}$$

where v_j is the interactive target node. Finally, the comprehensive score of the node is weighted by the short term trust value ST_{ij} and the long term trust value LT_{ij}.

$$CT_{ij}^n = \eta ST_{ij} + (1 - \eta) LT_{ij}, \tag{4}$$

where, η is determined according to the node role, and its range is between 0 and 1.

The feedback trust degree TF is calculated according to the node topology connection of the shipping network. Suppose that node p is connected to several nodes on the topology. Then nodes set $\{k_1, k_2, k_3, ..., k_t\}$ are the feedback nodes of p. The calculation of feedback trust is based on the assumption that the more nodes interact, the higher the feedback trust. Check the number of interactions between node p and each feedback node and calculate the weighting factor according to the following formula.

$$TF(k_i) = \begin{cases} 1 & , times = 0 \\ \prod_{i=1}^{m} CT_{mn} & , times > 0, \end{cases} \tag{5}$$

where, $times$ represents the number of interactions between nodes. Additionally, CT_{mn} is the comprehensive score weighted by the short term and long term trust value. The comprehensive trust degree is calculated according to the following formula, which needs to combine short term trust value, long term trust value and feedback trust value.

$$T(ij) = \alpha CT_{ij}^n + (1 - \alpha) TF(k_i). \tag{6}$$

B. Authentication mechanism of blockchain network

Before nodes join the blockchain network, identity authentication is an essential link. Elliptic Curve Digital Signature Algorithm (ECDSA) is a Digital Signature(DS) algorithm based on ECC. This algorithm has the characteristics of fast speed, high intensity and short signature, which is suitable for MTS with high real-time requirement. Algorithm 1 describes the signature process in detail, where d_A represents the private key and z is the positive integer intercepted by the hash. After receiving the message m and signature value

Algorithm 1 ECDSA signature process.

Input: Elliptic curve $Ep(a, b)$, base point G and random integer k.
Output: Signature value $< r, s >$.

Calculate public key P ;
$P \leftarrow k * G$;
Generates a random integer r $(r < n)$ and another k;
if $r == 0$ **then**
    Return to the Step 1;
else
    $s \leftarrow k^{-1}z + rd_A \ mod \ n$;
    if $s == 0$ **then**
        Choose another k and return to the Step 3;
    end if
end if
return $< r, s >$

$< r, s >$, the receiver performs the following operations to verify the signature. ECDSA works on the hash of encrypted information, not the information itself. The choice of hash function is determined by the user. Obviously, in order to ensure security, password level secure hash function is still required.

As for the verification process, we first need to obtain the public key H_A and the intercepted hash value z. Then calculate P according to the following formula, where u_1 and u_2 are the two intermediate variables involved in the calculation.

$$u_1 = s^{-1}z \quad mod \quad n, \tag{7}$$

$$u_2 = s^{-1}r \quad mod \quad n, \tag{8}$$

$$P = u_1G + u_2H_A. \tag{9}$$

Finally, verify whether the following equation is true, that is, whether the signature is valid.

$$r = x_P \quad mod \quad n. \tag{10}$$

Compared with other digital signature algorithms, its security performance is higher under the same key length. In addition, due to the small amount of computing and low storage space requirements, it is very suitable for mobile Internet.

C. Consensus verification algorithm based on VRF algorithm and credibility

In view of the limitation of network traffic, we propose an improved VRF consensus scheme based on credit voting. The VRF scheme cannot effectively deal with the false evaluation and collusion behavior of malicious nodes. And credibility of the voting process can reduce abnormal behavior node credit score, keeps it from being added to the consensus. In this way, interference with the normal consensus process is avoided. The improvement of this consensus algorithm is based on PBFT consensus algorithm.

G, V and F are three polynomial time algorithms included in VRF algorithm. G is a key generation algorithm, which can generate public key PK and private key SK. The input of F algorithm includes random value α and private key SK. And its output is the final random selection result $\beta = F_1(SK, \alpha)$ and the proof of the result $Proof = F_2(SK, \alpha)$. The function of V is to verify that β is based on the correct output under α. The input of V algorithm includes random value α, public key PK and $Proof$. Then it will output the judgment of whether the result is correct or not. In the proposed scheme, the VRF algorithm uses RSA digital signature algorithm and hash function to ensure the verifiability and uniqueness of the algorithm. The specific flow of algorithm is shown in Algorithm 2.

Algorithm 2 Verifiable random function process based on RSA.

Input: Two unequal large prime numbers p and q, an integer e and Euler function $\psi(x)$.
Output: public key $< e, n >$, private key $< d, n >$ and Output value b.

$n \leftarrow p \times q$;
$\psi(n) \leftarrow \psi(p-1) \times \psi(q-1)$;
Calculate d, where $d \times e \equiv 1 \ mod \ \psi(n)$.
Generates $< e, n >$ and $< d, n >$;
$h \leftarrow hash \ (SK, \alpha)$;
$Proof \leftarrow h^d \ mod \ n$;
if $Proof' = hash \ (SK') \ mod \ n$ **then**
    Random number is valid, $b \leftarrow true$;
else
    Random number is invalid, $b \leftarrow false$;
end if
return b

With the addition of VRF, PBFT has made a new breakthrough in scalability and security. The characteristics of VRF ensure that no user can generate a fictitious r to join the voting committee under the premise that the α is determined. The value of α will change with the result of the previous round of blocks. Therefore, it is difficult for malicious users to predict the α random value of the next round. VRF can control the number of nodes drawn, which makes the nodes in the consensus stage process not exceed the threshold. Furthermore, it ensures more flexibility in network expansion and change than the original PBFT. In terms of security, VRF improves the master selection mode. The remainder method of PBFT is easy to expose the order of the master node, affecting the packaging block of the master node. After the introduction of VRF, the attackers cannot know the master node in advance. Therefore, the security of the packaging process is improved. In addition, in each round of consensus process, the proposal

node, verification node and confirmation node are randomly selected by VRF, which is difficult for attackers to predict, thus greatly enhancing the overall anti attack ability of the consensus algorithm.

V. Simulation Experiment and Analysis

In this section, we analyze the simulation results of the proposed model and evaluate its performance comprehensively. The system is evaluated with simulator in Matlab. We set up nodes in the system for testing, and the memory capacity of each node is 50MB, which contains 2MB source information of the node itself. All the experiments are completed on a personal computer with 4 gigabytes memory and Intel i5 quad core CPU.

A. Identity authentication protocol simulation experiment

In this paper, we propose a behavior trust authentication mechanism (BTEA) for MTS based on the blockchain network to ensure data confidentiality and integrity in device access and information communication. In order to highlight the performance advantages of the authentication mechanism proposed in this paper, we choose three authentication models to compare the authentication time. These three models are all discussed for vehicle certification in the IoT-enabled transportation scenario. The first authentication mechanism (VGKM) is proposed in literature [37]. This dual authentication mechanism of dual key management can join and remove vehicle nodes in a brief way. The second scheme is Vehicular Ad-hoc Network (VANET) local authentication and roaming authentication (PPAS) based on bilinear pair in literature [38]. The last one [39] is a lightweight anonymous scheme (VAAS) based on bilinear pairing, which eliminates the bilinear pairing operation and significantly reduces the computational complexity of vehicles.

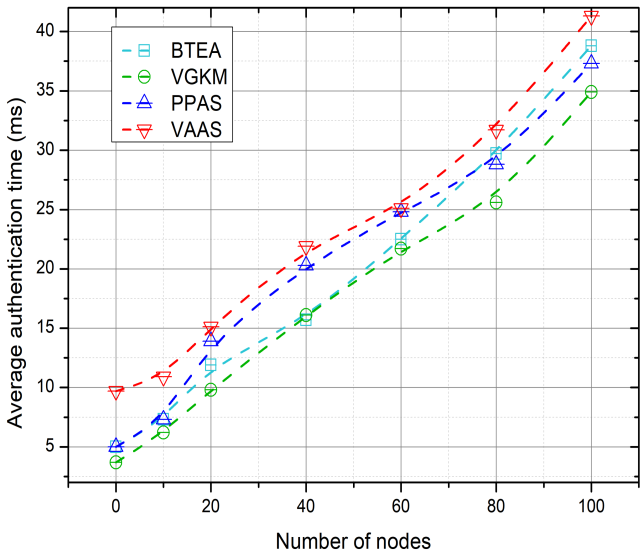

Fig. 3: Average authentication time.

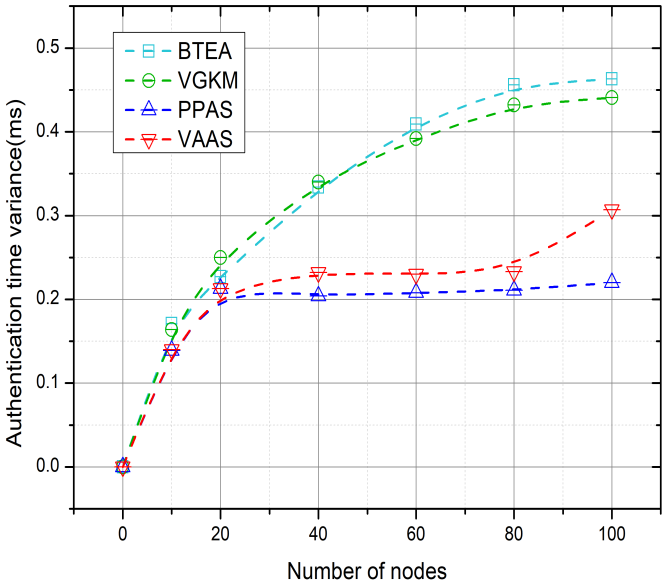

Fig. 4: Authentication time variance.

Fig. 3 describes the average value of node authentication time in each system with the increasing number of participating nodes. Fig. 4 illustrates the curves of authentication time variance of the four systems respectively. It can be seen from the two charts that compared with the other three models, the time average value of node authentication in our proposed scheme is at a lower level. Although the model VGKM performs best in the average value, its variance level is significantly higher than that of other models when the number of nodes increases to more than 20. In addition, it carries the certificate information of both sides in the authentication interaction information, resulting in high load problem and data loss. The scheme in this paper is close to VGKM, but the effect is not stable as PPAs and VAAs. As for resisting security attacks, VAAs and VGKM have the same security problems, and PPAs is vulnerable to replay attacks. Therefore, the proposed BTEA scheme is similar to other models in authentication time, but the security of authentication process is improved.

B. Time performance experiment of consensus algorithms

TPS is the detection standard for the operating efficiency of the blockchain system. The definition of throughput is the average of the number of transactions packed into a block in a unit time. It is calculated as follows:

$$TPS = B_{transaction}/\Delta t, \tag{11}$$

where, Δt represents the block generation time and $B_{transaction}$ is the quantity of transactions packed into the block during the Δt time period. In the test phase, we compare the improved PBFT algorithm based on VRF and credibility (VC-PBFT) proposed in this paper with traditional PBFT, Dynamic Practical Byzantine Fault Tolerance (DPBFT) [40], and the Geographic Practical Byzantine Fault Tolerance (GPBFT) [41] algorithm. PBFT algorithm can completely separate the blockchain from the reward mechanism of tokens on the chain.

It solves the Byzantine problem with limited nodes and ensures certain performance at the same time. However, there are still some problems, such as security vulnerabilities in the selection of master nodes. Based on PBFT, the DPBFT protocol introduces the concept of participation to measure whether nodes are active enough. By adding screening conditions to ensure the effectiveness of participating nodes, so as to effectively improve the system security. Additionally, GPBFT is based on the assumption that fixed IoT devices have a low probability of becoming malicious nodes. GPBFT uses the geographic information of fixed IoT devices to reach a consensus, so as to avoid Sybil attack. Taking the number of nodes as the

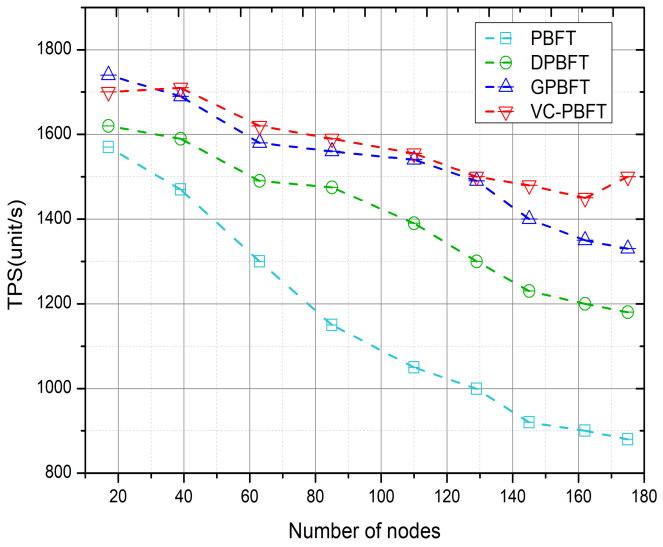

Fig. 5: Comparison of system TPS.

independent variable, we observe the change of TPS value of each model with the increase of node number. It can be seen from Fig. 5, the consensus algorithm proposed in this paper has the highest computational efficiency in the blockchain system. And this advantage becomes more obvious with the increase of the number of nodes.

In order to prove that VRF improves the consensus efficiency of the system, we apply the four models to the network with 180 nodes. Fig. 6 shows how the generation time of each block changes as the number of rounds increases. Compared with PBFT, DPBFT and GPBFT, the communication cost of the proposed VC-PBFT scheme decreases in the process of reaching a stable state.

There is no doubt that the addition of VRF algorithm simplifies the consensus process, resulting in an increase in the number of transactions adding blocks per unit time. More importantly, with the increasing number of nodes, the performance of the consensus mechanism will not decline significantly. It can be verified that the output of VRF has good randomness, so it ensures the randomness of extracting consensus nodes in non interactive mode. Therefore, the centralization of the system is greatly reduced. On the whole, the output randomness of VRF ensures that the transaction is evenly distributed to all candidate nodes. It reduces the

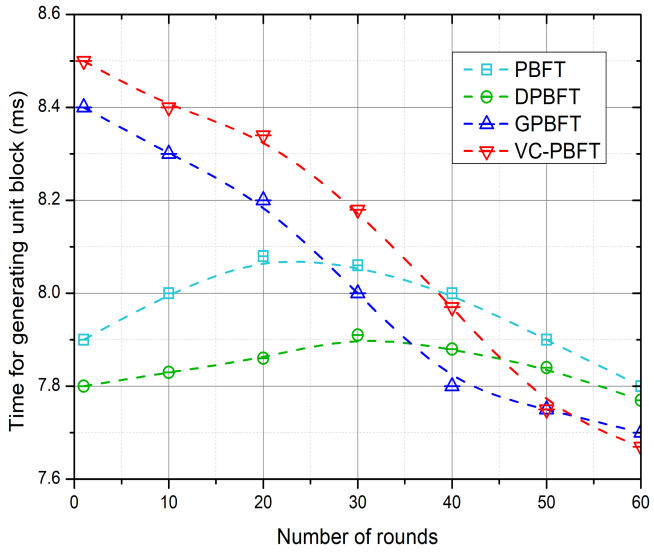

Fig. 6: Time for generating unit block.

workload of each node and improves the concurrent processing ability of the transaction. For the other three comparison schemes, because of the lack of node filtering mechanism, the number of transactions will decrease significantly with the increase of node points. However, for the shipping system with changing environmental facts, the joining and launching events of nodes are frequent. Therefore, the proposed VC-PBFT mechanism is more suitable for IoT-enabled MTS application.

C. Fault tolerance performance and safety analysis

This section shows experimental studies for the Byzantine fault tolerance performance of the proposed consensus algorithm and conducts security analysis. In the initial blockchain system with 1500 nodes, there exist 480 labeled Byzantine nodes. Fig. 7 illustrates that after about 15 rounds, the proposed VC-PBFT algorithm can more obviously eliminate the Byzantine fault nodes, while the security of PBFT algorithm is lower.

That is because PBFT has the security vulnerability of randomly selecting the main section for view switching and the problem of low consensus efficiency when consensus nodes increase. It is difficult to apply PBFT to networks with more than 100 nodes, because of the $O(n^2)$ messaging complexity. If you want to reliably broadcast a message in a network where Byzantine nodes (malicious nodes) exist, at least $O(n^2)$ message complexity is required accordingly. When the proposed consensus algorithm greatly reduces the number of broadcast participants, the consensus efficiency will be improved naturally, and the fault tolerance and security will be enhanced. The problem of transaction performance is solved by using VRF and credibility mechanism. For all candidate nodes, each candidate node has a different private key. Different random numbers will be generated after using the same seed as the input of the node identity extraction algorithm. For the same node, different random numbers will be generated. Therefore, each candidate node will process the

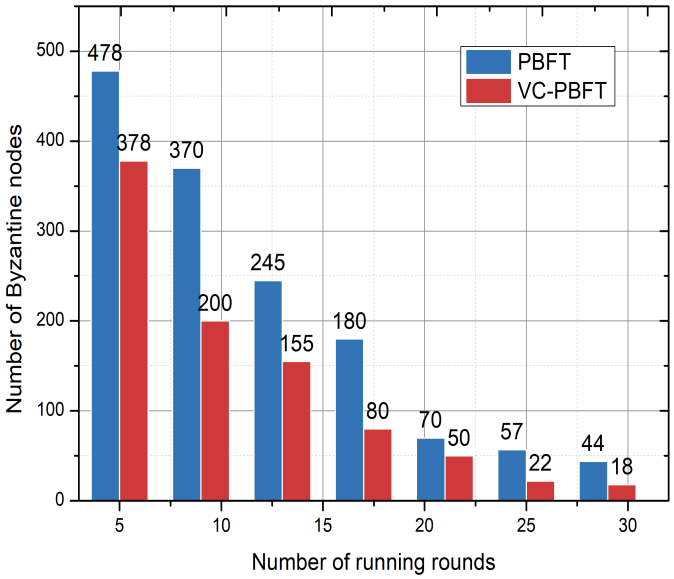

Fig. 7: Byzantine node number comparison.

transactions of some clients in the whole network. The union of the transactions processed by the candidate node is all the transactions in the whole network. In this way, all the transactions in the whole network are allocated to different nodes, reducing the number of transactions processed by a single node.

This scheme adopts blockchain technology as the support, and multiple nodes form a blockchain network. Even if some nodes go down or betray, it will not affect the normal operation of other nodes in the network and avoid the single point of failure of the system. In the system security experiment, we change the original fixed consensus node into a set of candidate nodes, and then use the lottery algorithm based on VRF algorithm to determine the final nodes. The adversary node cannot obtain the private key of the candidate node, so it is difficult to determine the attack target. Even if the opponent's proposal controls some candidate nodes, it may not be able to participate in the subsequent consensus process because it is not selected, which increases the difficulty of the opponent's attack and improves the security of the consensus mechanism. Moreover, the business system is vulnerable to replay attacks, causing economic losses to the shipping industry. In the proposed system, the core of the VRF algorithm for blockchain is to sign the message using the RSA digital signature algorithm, and then use the hash function to calculate the hash value of the digital signature. It ensures that different digital signatures can be obtained for different messages, and then different random numbers can be obtained. Therefore, replay attacks can be defended with the help of random numbers of both sides of communication. Thus the model has a good defense effect against the camouflage attacks, denial of service attacks and replay attacks.

VI. Conclusion

With the wide application of IoT technology in all aspects of MTS, the risks and challenges in safety and reliability have also increased significantly. Aiming at reducing the risk of information leakage in maritime transportation, this paper puts forward an IoT collaborative processing system for marine transportation flow scheduling and management. The system takes the blockchain mechanism as the guarantee for system authentication and secure transmission. Additionally, we propose an improved PBFT consensus algorithm based on VRF and credibility mechanism to adapt to the frequent environmental changes. The proposed mechanism ensures that the transactions are evenly distributed to all candidate nodes, and improves the concurrent processing ability of the system.

In fact, as a future work, we will continue to pay attention to the development of marine information industry. We plan to use the proposed architecture within the context of the Cloud Computing to augment our solution. We will explore more concise and lightweight authentication methods, so as to further improve the information transmission mechanism of MTS. Last, our work has not addressed the problem of detecting possible conflicts between messages. In fact, the messages submitted by the two terminal devices may be opposite or conflict with each other. In this case, how to filter reliable messages is our next research direction.

References

[1] K. Z. Ghafoor, L. Kong, S. Zeadally, A. S. Sadiq, G. Epiphaniou, M. Hammoudeh, A. K. Bashir, and S. Mumtaz, "Millimeter-wave communication for internet of vehicles: Status, challenges, and perspectives," *IEEE Internet Things J.*, vol. 7, no. 9, pp. 8525–8546, 2020.

[2] J. Wu, D. Zhang, and C. Wan, "Resilience assessment of maritime container shipping networks - a case of the maritime silk road," in *2019 5th International Conference on Transportation Information and Safety (ICTIS)*, pp. 252–259, 2019.

[3] L. Zhu, L. Zhang, X. Li, and R. Zhou, "Maritime safety assessment in the 21st-century maritime silk road under risk factors coupling," in *2019 5th International Conference on Transportation Information and Safety (ICTIS)*, pp. 411–415, 2019.

[4] I. S. Shipunov, A. P. Nyrkov, M. U. Ryabenkov, E. V. Morozova, and K. P. Goloskokov, "Investigation of computer incidents as an important component in the security of maritime transportation," in *2021 IEEE Conference of Russian Young Researchers in Electrical and Electronic Engineering (ElConRus)*, pp. 657–660, 2021.

[5] A. Munusamy, M. Adhikari, M. A. Khan, V. G. Menon, S. N. Srirama, L. T. Alex, and M. R. Khosravi, "Edge-centric secure service provisioning in iot-enabled maritime transportation systems," *IEEE Transactions on Intelligent Transportation Systems*, pp. 1–10, 2021.

[6] A. P. Nyrkov, N. B. Glebov, R. O. Novoselov, O. M. Alimov, and S. G. Chernyi, "Databases problems for maritime transport industry on platform highload," in *2018 IEEE International Conference "Quality Management, Transport and Information Security, Information Technologies" (IT QM IS)*, pp. 132–135, 2018.

[7] P. Zhang, Y. Wang, N. Kumar, C. Jiang, and G. Shi, "A security and privacy-preserving approach based on data disturbance for collaborative edge computing in social iot systems," *IEEE Transactions on Computational Social Systems*, vol. PP, no. 99, pp. 1–1, 2021.

[8] P. Zhang, C. Jiang, X. Pang, and Y. Qian, "Stec-iot: A security tactic by virtualizing edge computing on iot," *IEEE Internet of Things Journal*, vol. 8, no. 4, pp. 2459–2467, 2021.

[9] G. Raja, A. Ganapathisubramaniyan, S. Anbalagan, S. B. M. Baskaran, K. Raja, and A. K. Bashir, "Intelligent reward-based data offloading in next-generation vehicular networks," *IEEE Internet Things J.*, vol. 7, no. 5, pp. 3747–3758, 2020.

[10] A. Jindal, G. S. Aujla, N. Kumar, R. Chaudhary, M. S. Obaidat, and I. You, "Sedative: Sdn-enabled deep learning architecture for network traffic control in vehicular cyber-physical systems," *IEEE Netw.*, vol. 32, no. 6, pp. 66–73, 2018.

[11] S. A. Hussain, M. Iqbal, A. Saeed, I. Raza, M. H. Raza, A. Ali, A. K. Bashir, and A. Baig, "An efficient channel access scheme for vehicular ad hoc networks," *Mob. Inf. Syst.*, vol. 2017, pp. 8246050:1–8246050:10, 2017.

[12] X. Xu, X. Yan, C. Sheng, C. Yuan, D. Xu, and J. Yang, "A belief rule-based expert system for fault diagnosis of marine diesel engines," *IEEE Trans. Syst. Man Cybern. Syst.*, vol. 50, no. 2, pp. 656–672, 2020.

[13] L. Lyu, Y. Dai, N. Cheng, S. Zhu, X. Guan, B. Lin, and X. Shen, "Aoi-aware co-design of cooperative transmission and state estimation for marine iot systems," *IEEE Internet Things J.*, vol. 8, no. 10, pp. 7889–7901, 2021.

[14] M. Cai, Y. Wang, S. Wang, R. Wang, Y. Ren, and M. Tan, "Grasping marine products with hybrid-driven underwater vehicle-manipulator system," *IEEE Trans Autom. Sci. Eng.*, vol. 17, no. 3, pp. 1443–1454, 2020.

[15] P. Zhang, C. Wang, N. Kumar, and L. Liu, "Space-air-ground integrated multi-domain network resource orchestration based on virtual network architecture: a drl method," *IEEE Transactions on Intelligent Transportation Systems*, vol. PP, no. 99, pp. 1–1, 2021.

[16] T. Zhou, J. Shen, Y. Ren, and S. Ji, "Threshold key management scheme for blockchain-based intelligent transportation systems," *Secur. Commun. Networks*, vol. 2021, pp. 1864514:1–1864514:8, 2021.

[17] L. Hirtan, C. Dobre, and H. González-Vélez, "Blockchain-based reputation for intelligent transportation systems," *Sensors*, vol. 20, no. 3, p. 791, 2020.

[18] P. Zhang, C. Wang, C. Jiang, and A. Benslimane, "Security-aware virtual network embedding algorithm based on reinforcement learning," *IEEE Transactions on Network Science and Engineering*, vol. 8, no. 2, pp. 1095–1105, 2021.

[19] G. S. Aujla and A. Jindal, "A decoupled blockchain approach for edge-envisioned iot-based healthcare monitoring," *IEEE J. Sel. Areas Commun.*, vol. 39, no. 2, pp. 491–499, 2021.

[20] A. Jindal, G. S. Aujla, N. Kumar, and M. Villari, "GUARDIAN: blockchain-based secure demand response management in smart grid system," *IEEE Trans. Serv. Comput.*, vol. 13, no. 4, pp. 613–624, 2020.

[21] M. A. Javed, N. S. Nafi, S. Basheer, M. A. Bivi, and A. K. Bashir, "Fog-assisted cooperative protocol for traffic message transmission in vehicular networks," *IEEE Access*, vol. 7, pp. 166148–166156, 2019.

[22] A. A. Celes and N. E. Elizabeth, "Verification based authentication scheme for bogus attacks in vanets for secure communication," in *2018 International Conference on Communication and Signal Processing (ICCSP)*, pp. 0388–0392, 2018.

[23] J. Huang, Y. Qian, and R. Q. Hu, "Secure and efficient privacy-preserving authentication scheme for 5g software defined vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 8, pp. 8542–8554, 2020.

[24] C. Yan, Y. Zhang, H. Wang, and S. Yu, "A safe and efficient message authentication scheme in the internet of vehicles," in *2020 International Conference on Information Science, Parallel and Distributed Systems (ISPDS)*, pp. 10–13, 2020.

[25] S. Guo, X. Hu, Z. Zhou, X. Wang, F. Qi, and L. Gao, "Trust access authentication in vehicular network based on blockchain," *China Communications*, vol. 16, no. 6, pp. 18–30, 2019.

[26] P. Zhang, X. Pang, N. Kumar, G. S. Aujla, and H. Cao, "A reliable data-transmission mechanism using blockchain in edge computing scenarios," *IEEE Internet of Things Journal*, vol. PP, no. 99, pp. 1–1, 2020.

[27] Z. Xiao, X. Fu, L. Zhang, and R. S. M. Goh, "Traffic pattern mining and forecasting technologies in maritime traffic service networks: A comprehensive survey," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, no. 5, pp. 1796–1825, 2020.

[28] P. Zhang, C. Wang, G. S. Aujla, N. Kumar, and M. Guizani, "Iov scenario: Implementation of a bandwidth aware algorithm in wireless network communication mode," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 12, pp. 15774–15785, 2020.

[29] M. B. Mollah, J. Zhao, D. Niyato, Y. L. Guan, C. Yuen, S. Sun, K. Lam, and L. H. Koh, "Blockchain for the internet of vehicles towards intelligent transportation systems: A survey," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4157–4185, 2021.

[30] H. Liu, P. Zhang, G. Pu, T. Yang, S. Maharjan, and Y. Zhang, "Blockchain empowered cooperative authentication with data traceability in vehicular edge computing," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 4, pp. 4221–4232, 2020.

[31] Z. Lu, Q. Wang, G. Qu, H. Zhang, and Z. Liu, "A blockchain-based privacy-preserving authentication scheme for vanets," *IEEE Transactions on Very Large Scale Integration (VLSI) Systems*, vol. 27, no. 12, pp. 2792–2801, 2019.

[32] M. Zang, Y. Zhu, R. Lan, Y. Liu, and X. Luo, "Bavc: Efficient blockchain-based authentication scheme for vehicular secure communication," in *2021 13th International Conference on Advanced Computational Intelligence (ICACI)*, pp. 346–350, 2021.

[33] K. Abbas, L. A. Tawalbeh, A. Rafiq, A. Muthanna, I. A. Elgendy, and A. A. A. El-Latif, "Convergence of blockchain and iot for secure transportation systems in smart cities," *Secur. Commun. Networks*, vol. 2021, pp. 5597679:1–5597679:13, 2021.

[34] M. Castro and B. Liskov, "Practical byzantine fault tolerance," in *Proceedings of the Third USENIX Symposium on Operating Systems Design and Implementation (OSDI), New Orleans, Louisiana, USA, February 22-25, 1999* (M. I. Seltzer and P. J. Leach, eds.), pp. 173–186, USENIX Association, 1999.

[35] Y. Wang, S. Cai, C. Lin, Z. Chen, T. Wang, Z. Gao, and C. Zhou, "Study of blockchains's consensus mechanism based on credit," *IEEE Access*, vol. 7, pp. 10224–10231, 2019.

[36] W. Li, C. Feng, L. Zhang, H. Xu, B. Cao, and M. A. Imran, "A scalable multi-layer pbft consensus for blockchain," *IEEE Transactions on Parallel and Distributed Systems*, vol. 32, no. 5, pp. 1146–1160, 2021.

[37] P. Vijayakumar, M. Azees, A. Kannan, and L. Jegatha 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, 2016.

[38] H. Zhu, T. Liu, G. Wei, and H. Li, "PPAS: privacy protection authentication scheme for VANET," *Clust. Comput.*, vol. 16, no. 4, pp. 873–886, 2013.

[39] H. Zhu, W. Pan, B. Liu, and H. Li, "A lightweight anonymous authentication scheme for vanet based on bilinear pairing," in *2012 Fourth International Conference on Intelligent Networking and Collaborative Systems*, pp. 222–228, 2012.

[40] H. Xu, Y. Long, Z. Liu, Z. Liu, and D. Gu, "Dynamic practical byzantine fault tolerance," in *2018 IEEE Conference on Communications and Network Security, CNS 2018, Beijing, China, May 30 - June 1, 2018*, pp. 1–8, IEEE, 2018.

[41] L. Lao, X. Dai, B. Xiao, and S. Guo, "G-pbft: A location-based and scalable consensus protocol for iot-blockchain applications," in *2020 IEEE International Parallel and Distributed Processing Symposium (IPDPS)*, pp. 664–673, 2020.