Received January 16, 2020, accepted January 28, 2020, date of publication February 10, 2020, date of current version February 26, 2020.

Digital Object Identifier 10.1109/ACCESS.2020.2972606

A Scheme of Intelligent Traffic Light System Based on Distributed Security Architecture of Blockchain Technology

PENGJIE ZENG[1], **XIAOLIANG WANG**[1], **(Member, IEEE), HAO LI**[1], **FRANK JIANG**[2], **AND ROBIN DOSS**[2], **(Senior Member, IEEE)**

[1]School of Computer Science and Engineering, Hunan University of Science and Technology, Xiangtan 411201, China
[2]School of Info Technology, Deakin University, Geelong, VIC 3220, Australia

Corresponding author: Xiaoliang Wang (fengwxl@163.com)

This work was supported in part by the Cooperative Education Fund of China Ministry of Education under Grant 201702113002 and Grant 201801193119, in part by the Hunan Natural Science Foundation under Grant 2018JJ2138, in part by the H3C Fund of Hunan Internet of Things Federation under Grant 20180006, and in part by the Degree and Graduate Education Reform Project of Hunan Province under Grant JG2018B096.

ABSTRACT In recent years, under the background that the rapid development of traffic volume makes the current traffic lights far from meeting the urban traffic demand, intelligent traffic lights based on the centralized architecture began to appear. However, in the traffic network with complex structure and private data flow, there are many malicious attacks against the centralized architecture, such as Sybil and ghost car attacks, which undoubtedly brings great security risks to the traditional intelligent traffic lights. Blockchain technology is a popular security framework nowadays. Based on its outstanding characteristics in the distributed architecture and the development of Edge Intelligence (EI) technology, this paper proposes a distributed security architecture scheme based on blockchain technology for the existing intelligent traffic light system. At the same time, based on the model cutting technology proposed by EI, the smart contract is improved to achieve redundant cutting of ledger data in the process of block consensus, which greatly reduces the pressure of blockchain ledger data transmission. In the end of this paper, the superiority of this scheme compared with the traditional intelligent traffic light scheme in communication cost and time cost is demonstrated by simulation experiment.

INDEX TERMS Blockchain, intelligent transportation, distributed architecture, edge intelligence.

I. INTRODUCTION

With the rapid development of social economy and technology, traffic congestion has become a major problem in the field of transportation. At the same time, the rapid development of traffic volume makes the current traffic lights far from meeting the demand of urban traffic, which also increases the traffic pressure in a disguised way, and makes the traffic predicament fall into a vicious circle. In order to maintain the road traffic and improve the urban traffic efficiency, it is urgent to analyze the existing traffic system conditions, use intelligent algorithm to update the traffic light timing scheme in real time, thus giving birth to the concept of intelligent traffic lights. In the complex and changeable traffic network, intelligent traffic lights can connect with other intelligent traffic lights in the scope to a regional server for networking. Through image recognition algorithm, edge detection algorithm and machine learning algorithm, the collected traffic image data can be processed cooperatively [1]. Based on the data of traffic flow and people flow at each intersection, a standardized model is established, and a large number of existing traffic data are used to test the model, finally the optimal traffic light timing scheme is generated. However, the centralized network architecture of traditional intelligent traffic lights is vulnerable to malicious attacks from Internet of Vehicles (IoV), such as Sybil attacks and ghost car attacks. If an intelligent traffic light node in the network is maliciously attacked, the rest of the intelligent traffic light nodes in the network area will be threatened and affected, and even the whole traffic light network will be paralyzed, resulting in

The associate editor coordinating the review of this manuscript and approving it for publication was Honghao Gao.

serious traffic congestion and traffic accidents. Therefore, in order to improve the safety and feasibility of intelligent traffic lights and maintain a good intelligent traffic ecology, this paper introduces the block chain technology with the characteristics of decentralization [2], distributed ledger and consensus mechanism. With the aid of edge intelligence technology, a distributed security framework is established for the intelligent traffic light system, aiming to maintain the data authenticity and behavior security of the intelligent traffic light system through the distributed architecture.

II. LITERATURE REVIEW

At present, many scholars at home and abroad have carried out quite in-depth research in the field of intelligent traffic lights, and there are still some security schemes combining blockchain technology. In this section, we will outline the progress of intelligent traffic lights research and some solutions based on blockchain technology, focusing on their advantages and disadvantages.

When the concept of intelligent traffic is still in its infancy, Maram *et al.* proposed an Intelligent Traffic Light Control algorithm (ITLC) [3], which can make the intelligent traffic lights of each road intersection coordinate with each other and maintain the effective scheduling of road traffic. Li *et al.* later proposed a new control system based on real-time traffic flow [4], which can intelligently set the duration of traffic lights by sensing the number of vehicles through the sensor network. In the same year, with the rise of artificial intelligence technology, Zaid *et al.* [5] developed an automatic algorithm to control the time of traffic lights based on artificial intelligence technology and images on traffic lights, which can significantly increase the reliability and stability of intelligent traffic lights; according to Jin's team [6], a group based framework algorithm with adaptive learning ability can change the adaptive learning ability according to the traffic demand in real time and play a greater role in coordination; in the following year, Jin's team proposed a multi-level stage control scheme based on collective learning [7], emphasizing the use of reinforcement learning algorithm to train the system model, so as to improve the traffic performance. After that, intelligent transportation began to introduce the concept of Fog Computing (FC) [8]. Wu *et al.* [9] proposed an intelligent traffic light control system based on fog computing, which can calculate and share the traffic flow status of the intersection through the fog computing platform. Compared with the scheme of Maram *et al.*, it has made great progress. At the same time, Liu's team realizes safe intelligent traffic light control based on Fog Computing [10], which opens up the safety field of intelligent traffic lights, and can also be more friendly to compatible atomization equipment. Dorin [11] believes that some optimization tools can be used to update intelligent traffic lights. Vilarinho *et al.* innovatively focused on pedestrians, put forward a traffic light control strategy based on people at Isolated Intersections [12], adding people flow to the model, which can make the intelligent traffic light model more in line with the actual situation. In the latest research, Yousef *et al.* put forward a new reconfigurable history based traffic management algorithm [13], which optimizes performance indicators such as AQL and AWT through a robust heuristic method. The traffic network is dynamic and complex, and the perception of intelligent traffic lights to vehicles needs sufficient accuracy. Gao's team proposed a neural collaborative filtering QoS prediction scheme based on context awareness [14], and proved that the scheme can effectively improve the accuracy of the perception system. At the same time, when considering the type processing of exchange information, Gao's team also proposed a method of type processing of multimedia resources based on transformation [15], which can ensure the consistency of the collected traffic data in the exchange process and improve the reliability of decision-making. The team also made an in-depth discussion on the path planning of the intelligent transportation system, integrating the probability model test technology [16], Yin *et al.* further proposed a group travel planning scheme in the temporary mobile social network [17], which solved the existing path planning problems of the intelligent transportation system. Yin *et al.* proposed that service recommendation service quality prediction based on deep feature learning can be used in edge computing environment [18], thus promoting a cost driven service mix [19] in uncertain environment, so as to realize low coupling among entities of intelligent traffic light system. When collecting the information of traffic flow and people flow, it is necessary to improve the existing image recognition algorithm to obtain more accurate data information. Yu's team proposed a multi-mode converter for multi view visual representation of image caption display [20] and a layered depth selection feature prediction scheme for fine-grained image recognition [21], which can be used in combination. Experiments show that the accuracy of recognition can be improved effectively. For the position recognition errors in the image recognition process, Yu's team proposed a space pyramid enhanced netvlad position recognition algorithm based on weighted triple loss [22], which solved this problem well. With distributed architecture, it is bound to use edge computing technology to exchange and feedback data in time. Wang *et al.* proposed a CPCS trust evaluation crowdsourcing mechanism based on intelligent mobile edge computing [23] and an edge based sensor cloud differential privacy computing scheme [24], which improved the computing power of edge devices and could better coordinate the operation of intelligent traffic light system. In addition, we need to pay attention to the privacy of data in edge computing. In view of this, Wu *et al.* proposed a risk prevention method based on micro state prediction for part of information social network [25] and a security protection and recovery strategy based on incentive mechanism for big data in social network [26], which effectively improved the security in edge computing field. In addition, Wang *et al.* also proposed a mobile edge computing based industrial sensor cloud big data cleaning [27], which promotes the accuracy of decision-making formed by edge computing. Generally speaking, with the efforts of the above scholars, the intelligent traffic lights have been improved in function and performance, but at the same time, the security as a data carrier is ignored, which is also easy to be broken by malicious attacks, resulting in serious consequences. The security technology provided by blockchain technology can solve this problem well. Thakre *et al.* [28] proposed a novel secure publishing model based on blockchain technology, which is used to regulate and encourage academic publishing. Helo and Hao [29] developed a technical framework of bogistics monitoring system by using blockchain technology, and skillfully used the immutable distributed ledger to complete the information security work of supply chain. Longo *et al.* [30] also added the blockchain to the cooperation and trust of the supply chain, designed and developed a software connector based on the blockchain to connect the Ethereum blockchain with the enterprise information system, so as to share information with partners of different visibility levels. Yu's team research has given the realization of an online fair contract exchange protocol without a trusted third party, based on blockchain technology and certainty. At the same time, it has changed the one-way trust relationship of the current transaction type blockchain technology, and established a multi-directional trust relationship among the participating nodes of the blockchain through additional protocols [31]. In order to solve the security of centralized management of large-scale IoT devices, Xu's team proposed a scalable management framework for lightweight IoT devices based on blockchain technology [32], which improved transaction throughput, shortened transaction delay and reduced communication costs. There are also many scholars who have developed many security algorithms according to the characteristics of blockchain. Wei's team has proposed a forward security SSE scheme based on blockchain [33], which is proved to be four times faster than the latest forward private SSE scheme through experiments. Phan's team proposed an incremental hash function [34] based on the block link through the research of the blockchain ledger, which can calculate the hash value of the update message faster, but there will be some conflicts with the original hash function. Sachin's team [35] is able to achieve more efficient and effective goals and reflect sustainability in SC practice by studying blockchain technology. Ren *et al.* [36] proposed a sequential aggregate signature scheme (DVSSA) with designated verifier combined with blockchain technology to ensure that the user's health data can only be seen by the designated person, protect the privacy of WBAN users, and also compress the size of blockchain storage space. In addition, Ren's team also built a blockchain based identity and certificate management mechanism [37], which can provide a strong data security guarantee for the industrial Internet of things. In addition, it also proposed a mechanism that combines blockchain and regeneration coding [38], to improve the security and reliability of data stored under edge computing. Wang *et al.* proposed several intelligent data collection scheme [39]–[41] based on data fusion and a multi-source transmission scheme [42], which can better serve edge computing. The team also proposed a low complexity adaptive unloading scheme [43] based on Hungarian algorithm, which can effectively reduce the unloading delay of edge servers. He *et al.* proposed a light intelligent algorithm for edge computing [44]. Whether it is applied to solve practical problems or to develop more secure algorithms, the status of blockchain technology can not be shaken. In the development process of intelligent transportation and blockchain technology, we have summed up many experiences and lessons and integrated them into this paper.

The main contribution of this paper is to propose an improved security solution in the field of intelligent traffic lights, put forward a distributed intelligent traffic light architecture based on the decentralized characteristics of blockchain technology, and improve and innovate the existing intelligent contract by using the redundant cutting technology proposed by edge intelligence, effectively reducing the communication load in the consensus process in the block network.

III. PRELINARY KNOWLEDGE

A. OVERVIEW OF BLOCKCHAIN TECHNOLOGY

Blockchain is a kind of chained data structure which combines data blocks in chronological order in a way of sequential connection, and it is a distributed ledger that can not be tampered and forged guaranteed by cryptography [45].

In the intelligent traffic light architecture environment, which highly relies on the information of other nodes and maintains high frequency data exchange, new requirements are also put forward for the authenticity and privacy of data information: in order to prevent the real-time data of each intersection from being tampered with or used maliciously, the four core technologies of blockchain technology for the trust and security of transaction information can be adopted.

1) DECENTRALIZED ARCHITECTURE

In blockchain technology, decentralization means that in a system with many nodes, each node has a high degree of autonomy. Each node can choose to connect freely with each other to form a new connection unit. Any node may become a periodic center, but it does not have the mandatory central control and intervention function. The impact between nodes will form a non-linear causal relationship through the network. This open, flat and equal system architecture is called decentralized architecture.

2) DISTRIBUTED LEDGER

As the basis of blockchain to ensure the information security of account books, the most important implementation process of distributed account books is to make multiple nodes distributed in different places jointly complete the transaction bookkeeping, and the complete transaction account books will be dynamically stored in each node participating in the transaction. Therefore, all nodes can supervise and testify the legitimacy of transactions.

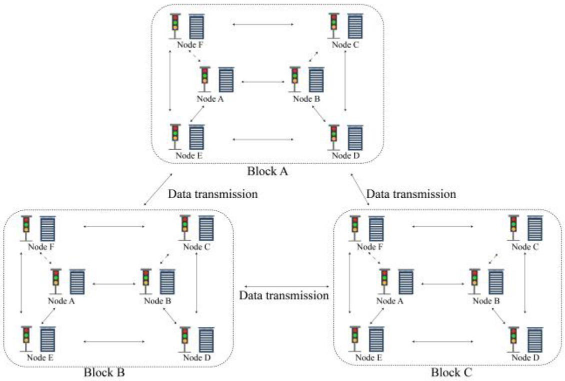

FIGURE 1. Schematic diagram of distributed ledger.

Different from the traditional distributed storage, the uniqueness of the blockchain distributed storage is mainly reflected in two aspects. First, each node of the blockchain stores complete data according to the block chain structure, while the traditional distributed storage generally stores data in multiple parts according to certain rules. Second, each node of blockchain is independent and equal in status, and the storage consistency is guaranteed by consensus mechanism, while the traditional distributed storage generally synchronizes data from the central node to other backup nodes. There is no single node that can record the account data separately, thus avoiding the possibility of single bookkeeper being controlled or being bribed to record false account. Because there are enough accounting nodes, in theory, unless all nodes are destroyed, accounts will not be lost, thus ensuring the security of account data [45].

3) SMART CONTRACT TECHNOLOGY

Ethereum's smart contract is a blockchain based digital asset control program. In a narrow sense, smart contract is a set of program codes involving relevant logic and algorithms, which can program the complex relationship among people, legal agreements and networks. In a broad sense, smart contract is a kind of computer protocol. Once deployed, self execution and self verification can be achieved. At present, it has been applied in distributed computing, Internet of things and other fields.

4) CONSENSUS MECHANISM

The consensus mechanism exists in the consensus layer of the blockchain infrastructure model. It takes Proof of Work (PoW) and Proof of Stake (PoS) as the consensus basis, and then uses Byzantine and Rayleigh wave consensus algorithms as auxiliary consensus methods to complete the consensus work of adding accounting nodes in the block and confirming the validity of transaction records. Taking PoW as an example, only when a block accounting node controls more than 51% of the accounting nodes in the block, can a record be forged without considering the huge number of nodes in the whole blockchain and the loss of their own rights and interests. As more and more nodes are added to the blockchain, the possibility of successful forgery approaches zero. This can effectively prevent information from being tampered with illegally or used by malicious nodes.

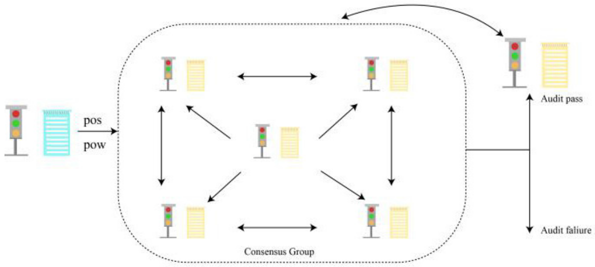

FIGURE 2. Schematic diagram of consensus working mechanism.

The consensus mechanism has two basic characteristics of ''The minority is subordinate to the majority'' and ''Everyone is equal'' [45]. The principle of ''The minority is subordinate to the majority'' does not necessarily refer to the number of block accounting nodes, but also refers to the computing power of nodes, the number of equity of nodes or the comparable characteristics of some other nodes. ''Everyone is equal'' emphasizes that when the block accounting nodes meet the conditions of participating in consensus, all the block accounting nodes have the priority to put forward consensus voting. If the consensus of other nodes is obtained, the consensus result may become the final consensus result.

B. OVERVIEW OF EDGE INTELLIGENCE

Edge Intelligence (EI) refers to terminal intelligence, which is an open platform integrating network, computing, storage and application core capabilities, and provides edge intelligence services to meet the key needs of industry digitalization in agile connection, real-time business, data optimization, application intelligence, security and privacy protection [46]. It can deploy intelligent attributes on edge devices, make terminal intelligence closer to users, and provide intelligent services to users in a faster and more accurate way.

In the intelligent traffic light system, there are cameras, remote data centers and other terminal equipment. As the edge terminal equipment node, it is difficult to meet the huge data computing needs in the process of algorithm training, such as machine learning, in computing capacity and information storage capacity. The edge cloud collaboration, model cutting and redundant data reduction in the edge intelligence scheme can solve these problems well.

IV. SYSTEM MODEL

A. SYSTEM ARCHITECTURED

In order to make the system framework have higher safety factor, the loose coupling principle is adopted in this paper. It is composed of three main entities: Municipal Administration, Traffic Administration and Intelligent Traffic Lights, among which Intelligent Traffic Lights entity includes edge terminal equipment such as camera and data sub center. In this

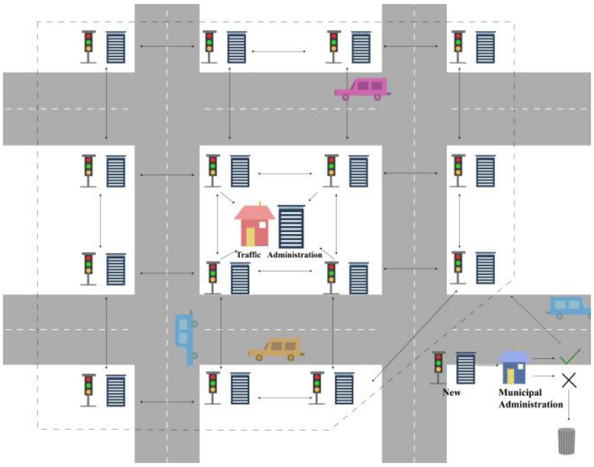

FIGURE 3. System frame diagram.

TABLE 1. Experimental configuration information.

Symbol	Definition
MA	Municipal Administration
TA	Traffic Administration
ITL	Intelligent Traffic Lights
$K_{pub\text{-}TA}$	The public key of *TA*
$K_{priv\text{-}TA}$	The private key of *TA*
$K_{pub\text{-}ITL}$	The public key of *ITL*
$K_{priv\text{-}ITL}$	The private key of *ITL*
ID	Unique identification of *ITL* node
Certificate	Digital certificate with *TA* key signature
timestamp	Current timestamp
$Message_{pre\text{-}p}$	Pre-prepared message
$Message_{prep}$	Prepared message
$Message_{comm}$	Confirmation message

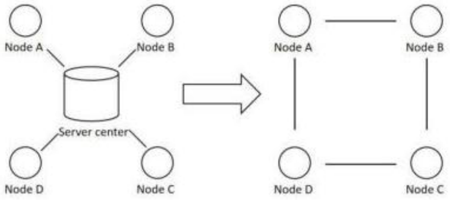

FIGURE 4. Schematic diagram of decentralized distributed architecture.

paper, under the background of intelligent traffic light system using blockchain structure and Edge Intelligence technology, the feasibility of an intelligent traffic light system with data privacy and malicious attack resistance is studied. In order to facilitate the elaboration of the system framework and principle, *MA*, *TA* and *ITL* will be used to refer to Municipal Administration, Traffic Administration and Intelligent Traffic Lights.

The framework adopts the principle of loose coupling in order to reflect that the main entities need to complete data exchange in a low degree of dependence, and at the same time guarantee the realization of system functions in a form similar to "separation of three powers": *MA* has the power to establish, add and abolish *ITL* nodes, but it can not obtain sensitive data including pedestrian characteristics and vehicle characteristics collected by terminal equipment. This is to prevent abuse or corruption within *MA*, resulting in a threat to ledger information. In addition to obtaining all *IT*L collection data and decision-making results, *TA* also has the authority to temporarily control and intervene*ITL*, which is only granted when individual *ITL* nodes fail or cities hold large-scale events and processions. At the same time, as a limitation, *TA* will not be able to add or remove *ITL* nodes. As an *ITL* node, in addition to the authority of collecting and processing data and decision-making scheme, it can also act as a member node in the blockchain to make consensus decision on the new *ITL* node added by *MA*. After obtaining the Proof of Work or Proof of Stake of the new node, it can decide whether it is allowed to join through consensus mechanism. This kind of mutual cooperation and checks and balances architecture can improve the safety of the intelligent traffic light framework to a greater extent. The specific system framework is shown in the Figure 3.

V. OUR SCHEME

Based on the system framework described in the previous section, this paper will propose a distributed security scheme based on blockchain technology in the following, and make a detailed description of the flow of the scheme. At the same time, in order to avoid the huge overhead load caused by the introduction of blockchain mechanism, we will use edge intelligence technology to improve the smart contract used by the system, complete the appropriate redundant cutting of the block, reduce the communication cost of the scheme on the premise of ensuring security, so that it can be better compatible with the original intelligent traffic light system architecture.

A. DECENTRALIZED DISTRIBUTED ARCHITECTURE BASED ON BLOCKCHAIN

Different from the traditional intelligent traffic light system in which the data is uploaded to the central server for processing, the intelligent traffic light architecture in this scheme adopts the decentralization scheme in the characteristics of blockchain, and the data collection, processing and transmission will be completed by each independent intelligent traffic light node, without relying on the server to participate in decision-making. At the same time, under the coordination and supervision of *MA* and *TA*, the safety of this way will be more solid. The advantage of the distributed scheme is to avoid the threat of being vulnerable to malicious attacks in the centralized scheme: in the centralized scheme, if there is a camouflaged traffic light node or ghost car attack, it is easy to upload the wrong information to the server, and then make the server processing decision confusion, and ultimately lead to the paralysis of the entire traffic system. The decentralized distributed architecture is shown in Figure 4.

In the distributed architecture based on blockchain, all blocks made up of nodes will maintain a common ledger, and the hash value of each block jointly proves the authenticity of the ledger. When one *ITL* makes a decision, it needs to obtain the unique bookkeeping right in the blockchain to add new data records, and generate new blocks through hash processing, broadcast and wait for the consensus of other nodes. The public ledger can only be added after the consensus is verified. This mode effectively prevents the whole intelligent traffic light system from being paralyzed due to malicious attacks on individual *ITL* nodes in the system. If some *ITL* nodes in the system suffer from multi-point attack at the same time, as long as the number of necrotic nodes is less than half of the number of block nodes, under the supervision of *MA* and *TA*, it can be intervened to some extent, for example, restart the node system or temporarily cancel the nodes. These methods can be adjusted quickly before the dead nodes affect the existing traffic conditions, which is also the necessity of *MA* and *TA* in this framework.

B. SPECIFIC IMPLEMENTATION PROCESS OF SAFETY SCHEME

1) INSTALLATION OF ITL NODE

ITL node has storage and computing functions, and it needs high security when it is put into use. Therefore, *MA* and *TA* are required to supervise its process when installing and establishing *ITL* node in this scheme, so as to prevent the creation *ITL* node from being maliciously attacked.

The new *ITL* node must be constructed and added by *MA* under the supervision of *TA*. The completed *ITL* node will receive a small amount of PoW from *TA* to assist it to add blocks in the subsequent process. Currently, it is only used as the creation node, not formally added to the block.

At this stage, *TA* will select global parameters for all *ITL* nodes in the system. On the newly installed *ITL* node, the public key (K_{pub-TA}), *ITL*'s own key ($K_{priv-ITL}$) and digital certificate with *TA* key signature are stored. Other installed *ITL* nodes will also obtain the public key ($K_{pub-ITL}$) of the new *ITL* node from *TA*. *TA* stores the public key ($K_{pub-ITL}$) of the new *ITL* node and its own private key ($K_{priv-TA}$).

2) REGISTRATION OF ITL NODES

In the registration phase, all new *ITL* nodes must be registered in *TA*. After confirming the construction process specification and registering the *TA* under the premise that the exchange information is normal, the *TA* will assign the unique *ID* to the new *ITL* node. At this time, the information stored by each *ITL* node is the unique identification *ID*, the public key of *TA* (K_{pub-TA}) and the digital certificate with *TA* key signature.

3) AUTHENTICATION PROCESS OF ITL NODE

- Broadcasting

The formation of block depends on hash function, which can transform the original information such as time, operation data and records stored in entity into a short summary information. Any slight change of the original information will make the hash value transformed by the hash function totally different, and also make it unable to reverse.

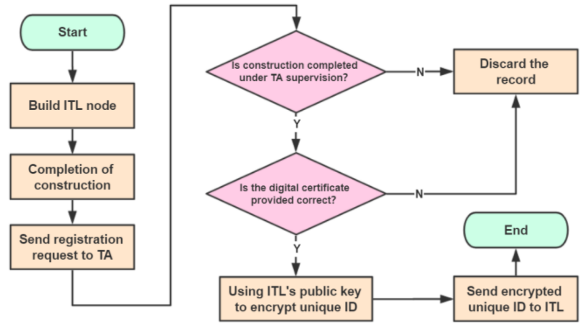
Start
Build ITL node
Completion of construction
Send registration request to TA
Is construction completed under TA supervision?
N
Discard the record
Y
Is the digital certificate provided correct?
N
Y
Using ITL's public key to encrypt unique ID
Send encrypted unique ID to ITL
End

FIGURE 5. ITL node installation and registration process.

In the above-mentioned *ITL* node that completes the installation and registration process, the original information stored with the current timestamp needs to be converted into a hash value through the hash function:

$$H_1 = Hash(ID, K_{pub-TA}, Certificate, timestamp) \quad (1)$$

After the conversion is successful, the *ITL* node uses its own key ($K_{priv-ITL}$) to encrypt the hash value H_1 to form a message and broadcast the rest of the installed *ITL* nodes:

$$Message = E\_K_{priv-ITL}(H_1) \quad (2)$$

- Consensus and verification

After receiving the request message broadcast by the new *ITL* node, the rest of the installed *ITL* nodes enter the consensus and verification stage. The main task of this stage is to use the consensus mechanism to complete the consensus and verification of new *ITL* nodes. At the same time, at this stage, *TA* and *MA* are unable to impose unfair intervention on their block.

In the consensus process, the installed *ITL* node needs to decrypt the request information using the public key ($K_{pub-ITL}$) of the new *ITL* node to obtain the initial hash value H_1:

$$H_1 = D\_K_{pub-ITL}(Message) \quad (3)$$

In *ITL* system, the number of *ITL* nodes in each block is limited, usually between 16 and 36, which also avoids the disadvantage of higher network communication complexity of Byzantine Fault Tolerance algorithm (*PBFT*) and achieves better consensus results. The key process of consensus includes three stages: pre prepare, prepare and confirm.

a: PRE-PREPARATION STAGE

$TA \rightarrow ITL_i$ (i =1,2,3,…, n): S_ $Message_{pre-p}$, where S is the sending operation. *TA* will assign a sequence number m to the request information and send the $Message_{pre-p}$ to all *ITL* nodes with consensus authority. The format of the $Message_{pre-p}$ is ≪*PRE-PREPARE, v, m, d*>δH_1>, where *v* is the view number, $H_1$is the request message sent by the new *ITL* node, and *d* is the summary of the request message H_1.

ITL nodes participating in consensus need to be confirmed:

a) Whether the signatures of the request and the $Message_{pre-p}$ are correct, and whether the summaries of d and H_1 are consistent;

b) Whether the current view number is v;

c) Whether the current *ITL* node implementing the consensus has never accepted message H_1 with sequence number m but different from its digest d in view v;

d) Whether the sequence number m of the $Message_{pre-p}$ is between the upper and lower limit h and H of the watermark, so as to prevent a failed *ITL* node from using a large sequence number to consume the sequence number space.

After each *ITL* node participating in the consensus completes the above confirmation, it will enter the preparation stage.

b: PREPARATION STAGE

TA→*ITL*$_i$(i =1, 2, 3, …, n): S_$Message_{prep}$. After the *ITL* node accepts the $Message_{pre-p}$: *≪PRE-PREPARE, v, m, d>δH*$_1$>, it enters the preparation stage. In this stage, *TA* sends preparation message $Message_{prep}$: *<PREPARE, v, m, d, ID>* to all *ITL* nodes (excluding request *ITL* nodes), where *v*, *m*, *d* have the same meaning as the preparation process, and *ID* is the unique identification number of *ITL* nodes. At the same time, the *ITL* node writes the $Message_{pre-p}$ to its message log.

At this stage, the *ITL* node needs to confirm:

a) Whether the signature of the $Message_{pre-p}$ and the $Message_{prep}$ is correct;

b) Whether the view number *v* is consistent;

c) Whether the message sequence number meets the waterline limit.

When the confirmation is passed, $Message_{prep}$ is written to the message log.

The flag of completion of the preparation stage is: the *ITL* node will record (*H*$_1$*, v, m, ID)* in its message log, where H_1 is the request content, the number *m* of the $Message_{pre-p}$ in view *v*, as well as *n*-1 $Message_{prep}$ received from different *ITL* nodes consistent with the $Message_{pre-p}$.

The preparation stage and the preparation stage ensure that all normal nodes agree on the request sequence number in the same view.

$$\begin{aligned} &\mathit{if}\ \mathit{prepared}(H_1, v, m, ID) == \mathit{TRUE}\ :\\ &\mathit{prepared}(H_1', v, m, ID)\ \mathit{NOT\ EXISTENCE};\end{aligned}$$

This means that at least (n−1)/2+1 normal nodes send message H_1 with sequence number m in the pre-preparation stage or preparation stage of view *v*.

c: CONFIRMATION STAGE

ITL$_1$ →*ITL*$_i$(i =2, 3, …, n): S_$Message_{comm}$. When the (*H*$_1$*, v, m, ID)* condition is true, each *ITL* node will broadcast the confirmation message $Message_{comm}$: *<COMMIT, v, m, D(H*$_1$*), ID>* to other *ITL* nodes to enter the confirmation stage.

In this stage, *ITL* nodes need to confirm:

a) Whether the signature of $Message_{pre-p}$, $Message_{prep}$ and $Message_{comm}$ is correct;

b) Whether the view number *v* of the message is consistent with the current view number of the node;

c) Whether the serial number *m* of the message meets the waterline condition.

When all the above conditions are met, the *ITL* node writes the confirmation message to the message log. It needs to be added that all received messages of a request are written to the log, which is allowed to exist in memory.

Define the conditions to confirm the completion of *committed (H*$_1$*, v, m)* as true:

$$\forall\ \mathit{ITL}(\mathit{from}1\ \mathit{ton}-1).\mathit{prepared}(H_1, v, m, ID) == \mathit{TRUE}$$

The conditions for local confirmation to complete *committed-local (H*$_1$*, v, m, ID)* are as follows:

$$\begin{cases} \mathit{prepared}(H_1, v, m, ID) == \mathit{TRUE} \\ \mathit{ITL}.\mathit{confirmation}[1, \dfrac{n-1}{2}] == Message_{pre-p} \end{cases} \tag{4}$$

The confirmation stage guarantees the following invariants:

$$\begin{aligned} &\mathit{if}\ \mathit{committed}-\mathit{local}(H_1, v, m, ID) == \mathit{TRUE}\ :\\ &\mathit{committed}(H_1, v, m) == \mathit{TRUE};\end{aligned}$$

This invariant and view change protocol ensure that all normal *ITL* nodes agree on the sequence number of local acknowledgment requests, even if the acknowledgment of these requests in each node is in a different view. Furthermore, this invariant ensures that any normal *ITL* node can finally confirm at least (n−1)/2+1 request nodes, and reduces the risk of malicious nodes disturbing the consensus results to a greater extent.

Each *ITL* node executes H_1 request after the *committed-local (H*$_1$*, v, m, ID)* is true, and the consensus state of *ITL* can reflect that all requests with number less than *m* are executed in order, which ensures that all normal *ITL* nodes execute all received requests in the same order, and ensures the correctness and order of consensus algorithm. After the consensus and verification operations are completed, each *ITL* node will send a reply to the requested *ITL* node. In this process, the *ITL* node will discard the reply with a smaller time stamp than the one with a reply, so as to ensure that the reply will only be executed once.

So far, the consensus and verification phase has been basically completed and will enter the decision-making phase.

- Policy decision

The *ITL* nodes participating in the consensus will sign in a round according to the results of the consensus and verification process. If the number of signatures is greater than or equal to 51%, the newly created *ITL* nodes will be allowed to join the block, otherwise, they will not pass, and the request record will be discarded. The decision results will be returned to the new *ITL* node, and the consensus will be fed back to the *TA*.

4) THE AUTHENTICATION OPERATION FLOW OF ITL NODE

Entity: ITL: Intelligent traffic lights; TA: Traffic Administration; MA: Municipal Administration.

Stage: Stage1: Broadcasting stage; Stage2: Preparation stage;
Stage3: Preparation stage; Stage4:Confirm stage;
Stage5: Decision-making stage.

```
       if the new ITL node has been installed and registered then
           $H_1$=Hash(ID, $K_{pub-TA}$, certificate, timestamp): Using hash function to convert original information into hash value $H_1$.
Stage1     Message=Encrypte_$K_{priv-ITL}(H_1)$: Encryption of hash value $H_1$ with ITL private key.
           The new ITL→other ITLs: Send_(Message): Broadcast the encrypted Message to other ITL nodes participating in the next stage.
       else
           Request broadcast failed.
       end if
```

```
       $H_2$=Decrypte_$K_{pub-ITL}$(Message)
       functionPRE_PREPARE($ITL_i$, n, $H_1$, $H_2$, h, H)
           Integer m=0
           if $ITL_i$(i=1, 2, 3,..., n)received and completed decryption then
               for(i=1; i<=n; i=i+1)
                   if $H_1 = H_2$ then
                       TA→$Message_{pre-p}$:Send_(m): Assign a serial number m to the pre-prepared information
                       TA→$ITL_i$ : Send_($Message_{pre-p}$:, ≪PRE-PREPARE v, m, d>δ$H_1$>)
Stage2                 m=m+1
                   else
                       delete $ITL_i$: Remove the failed ITL node.
                       continue
                   end if
               end for
           end if
       if $d = H_1$ and current view number = v and (h<m<H) then
           PREPARE($H_1$, v, m, d, h, H, ID)
       else
           return"Pre-preparatory failure"
       end if
```

```
       function PREPARE($H_1$, v, m, d, h, H, ID)
           if $ITL_i$(i=1, 2, 3,..., n) received $Message_{pre-p}$ then
               for (i=1; i<=n; i=i+1)
                   TA→$ITL_i$:Send_($Message_{prep}$:<PREPARE, v, m, d, ID>)
                   Write the pre-prepared message to$ITL_i$'s own message log
Stage3         end for
               if $signature_{pre-p}$=$signature_{prep}$ and current view number = v and (h<m<H)then
                   Write($H_1$, v, m, ID)to$ITL_i$'s own message log
                   if prepared($H_1$, v, m, ID) = TRUE then
                       prepared($H_1$', v, m, ID) NOT EXISTENCE
                       COMMIT($H_1$, v, m, ID)
                   else
                       return"Preparatory failure"
                   end if
               end if
       end if
```

```
       function COMMIT($H_1$, v, m, ID)
           if ($H_1$, v, m, ID)=TRUE then
               for(i=1; i<=n; i=i+1)
                   for(j=1; j<=n; j=j+1)
                       if i! = j then
                           $ITL_i$ →$ITL_j$:Send_($Message_{comm}$: <COMMIT, v, m, D($H_1$), ID>)
                       else
Stage4                     continue
                       end if
                   end for
               end for
       if ($signature_{pre-p}$ =$signature_{prep}$=$signature_{comm}$) and current view number = v and (h<m<H) then
           Writethe confirmed message to $ITL_i$'s own message log
           committed($H_1$, v, m)=TRUE
           prepared($H_1$, v, m, ID)=TRUE
           for(q=1; q<=n; q=q+1)
                   if $ITL_q$.prepared($H_1$, v, m, ID)=FALSE then
                       committed($H_1$, v, m)=FALSE
                       return "confirmation failure"
```

```
                    end if
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
          if $prepared(H_1, v, m, ID)=TRUE$
              and $ITL_q$,
              $getConfirmation$
              $(from\ 1\ to\ (n-1)/2, do\ not\ include$
            $ITL_q)=Message_{pre-p}$ then
                  $committed\text{-}local(H_1, v, m, ID)=TRUE$
              else
                  $committed\text{-}local(H_1, v, m, ID)=FALSE$
Stage4            $committed(H_1, v, m)=FALSE$
                  return "confirmation failure"
              end if
            end for
                if $committed\text{-}local(H_1, v, m, ID)=TRUE$ and
                  $committed(H_1, v, m)=TRUE$ then
                    return "Success"
            end if
          end if
      end if
- - - - - - - - - - - - - - - - - - - - - - - - - - - - - - -
      INPUT: number of signature
      if number of signature≥51% then
Stage5    Authentication pass
      else
          Authentication failed
      end if
```

C. REDUNDANT CUTTING PROCESS BASED ON SMART CONTRACT

When the authority of data collection, processing and transmission is distributed to each independent *ITL* node, it needs to be used as an edge terminal device to complete data calculation, processing, storage and other operations, that is, Edge Intelligence, in order to achieve the purpose of decentralization. At the same time, *ITL* as a bookkeeping node, its consensus election process for new nodes and decision-making operations for data need to be recorded in the blockchain ledger, and circulated in the blockchain in the form of public ledger. Each independent node needs to store the copy of the circulation account book, which is a huge test for the communication cost of the whole network, which also requires the blockchain to introduce the mechanism of smart contract to maintain the stability of the network.

In this paper, based on the consideration of security and the performance of the system, we will combine the model cutting scheme proposed in the Edge Intelligent technology to change the algorithm, so as to form a redundant cutting technology for information, and add it to the existing smart contract. The advantage of this improvement is to solve the problem of high redundancy of account information in the consensus process, which leads to the soaring communication cost. The improved smart contract framework is shown in Figure 6:

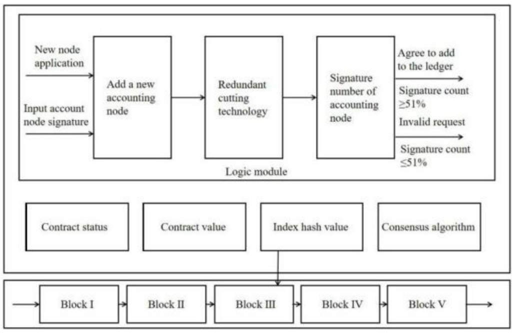

FIGURE 6. Smart contract based on redundant cutting technology.

1) INITIALIZATION

The smart contract includes necessary consensus modules, such as Byzantine algorithm [45], Ripple consensus algorithm, data management module, user management module, contract management module, legal text and parameters.

Redundancy cutting technology is often used in the field of edge intelligence. Its purpose is to cut the training model adaptively without affecting the data accuracy and data conclusion, so as to reduce the pressure of communication load. In the traffic light network with large amount of data, each independent *ITL* node needs to store the copy of the circulation account book, which will cause great pressure on the data storage of the node. Therefore, in the design of the smart contract, a redundant cutting process is added to the logic module of the smart contract. Initialization is the first step in the redundant cutting process. In the initialization stage, it is necessary to select global parameters for *ITL* nodes, zero the original information in the block, retain the initial hash value of each *ITL* node's account book, and clear the blacklist set by *MA* and *TA*.

2) BLOCK NODE WEIGHT CALCULATION AND REDUNDANT CUTTING

In Section V, this paper introduces the whole process of adding new *ITL* nodes into blocks in detail. In the consensus and verification stage, the main scheme of this paper is the current mainstream pbft algorithm. Unfortunately, in the process of *PBFT* algorithm consensus, it is necessary to repeatedly verify the pre prepared message, prepared message and confirmed message. This verification process will also require more communication resources in the process of consensus promotion.

Based on this dilemma, the second step of redundant cutting process needs to calculate the weight of the information generated by the consensus process in the block. The *ITL* nodes participating in the consensus in the block are analyzed by weight. Each *ITL* node has different contribution to the improvement of traffic environment in the area after entering the block, and its PoW and regional reputation are naturally different. We call this part of the value involved in the calculation as reputation product score, from low to high score as N_1, N_2, N_3, N_4 $(0 < N_1 < N_2 < N_3 < N_4 < 1)$.

At the same time of consensus mechanism in reality, each ITL node must maintain its current working state continuously, which leads to the loss of computing power of nodes, which is also different, which affects the decline of "loyalty" of normal *ITL* nodes participating in consensus process, although the decline of loyalty is inevitable. We record the "loyalty" lost due to maintaining the existing working state as μ, the original "loyalty" of *ITL* node as x, then the "loyalty" of a single node is finally recognized as $\lambda = x - \mu$, and the total "loyalty" of this block is:

$$\lambda_{sum} = \sum_{i=1}^{n} (x_i - \mu_i) \tag{5}$$

By integrating the reputation score and "loyalty" of each node, the weight of each *ITL* node is finally calculated as follows. It should be noted that $\sigma \in (0, 1)$ in the formula is the standard deviation of the node reliability recognized by *TA*:

$$Y = \sum_{i=1}^{n} (\frac{4(N_1\lambda_i|N_2\lambda_i|N_3\lambda_i|N_4\lambda_i)}{N_1 + N_2 + N_3 + N_4} \pm \sigma) \tag{6}$$

After completing the weight calculation of *ITL* nodes, for *ITL* nodes with high weight, when other *ITL* nodes receive the pre-preparation message and preparation message from this node, they can directly skip the verification stage, and the default content is the authenticity of their views. At the same time, if the pre-preparation message and the preparation message broadcast by the *ITL* node with high weight are verified by one of the *ITL* nodes participating in the consensus, and there are still some *ITL* nodes that have not yet processed the received broadcast (the message is in the processing queue), then the verified *ITL* node can send broadcast to the other *ITL* nodes participating in the consensus. Other *ITL* nodes traverse their own processing queue after receiving the broadcast. If there is a message whose serial number is verified by broadcast, the redundant message will be cut.

3) IMPACT ASSESSMENT

The redundant cutting process is to selectively cut the pre preparation stage and preparation stage in the consensus process, and give a few *ITL* nodes with high trust the privilege of broadcasting messages from being repeatedly checked. However, in order to ensure that the final consensus results will not be affected by information cutting, we do not carry out this cutting process in the confirmation stage of PBFT algorithm. In this stage, each participating *ITL* node is treated equally, and the whole process of broadcasting, receiving and processing must be completed. Therefore, the results of information cutting in the first two stages will receive a complete verification evaluation in the confirmation stage. If the evaluation result is not ideal, even if it does not cause the fundamental error of the consensus result, it will be required to carry out the consensus process again, and punish the *ITL* node that bears the main weight in the last two stages, and *TA*will reduce the credibility of this node.

TABLE 2. Experimental configuration information.

Device information	Parameter
CPU	Intel(R)Core(TM)i7-7700HQ @2.80GHz 2.80GHz
RAM	16.0GB
Operating system	Ubuntu(R)16.04(virtual machine)

VI. EXPERIMENT ANALYSIS

In this paper, we use the simulation platform of VISSIM-Excel VBA-MATLAB [48] to simulate the security solution proposed in this paper. VISSIM is a general-purpose traffic simulation modeling software [49], whose simulation time interval is 0.1 seconds, which can simulate various traffic conditions in reality, so it can comprehensively and effectively evaluate various traffic schemes [50], [51]. In order to verify the feasibility of the scheme, the experiment will use the traditional intelligent traffic light scheme to compare with the scheme in this paper, and finally analyze the simulation results.

A. SIMULATION ENVIRONMENT

B. SIMULATION ANALYSIS

1) COMMUNICATION COST ANALYSIS

Based on the characteristics of intelligent traffic lights, the setting of intersection parameters built in VISSIM in this paper is shown in Table 3, and all indicators of communication are taken into account. As the measurement of the traffic road condition mainly depends on the throughput of the intersection, and the simulation block is large in the process of the experiment, the analysis of the group arrival rate during the operation will produce large errors. Therefore, we finally choose the throughput of intersections and packet loss rate of runtime packets as the analysis indicators of this section. At the same time, all the experiments below will be compared with the traditional intelligent traffic lights proposed in [47].

In order to make the experimental results more close to the performance of intelligent traffic lights, the following experiments will respectively simulate the changes of throughput and packet loss rate of intelligent traffic lights when they operate normally in peak hours, which is to avoid the measurement and analysis data when the traffic is scarce, that is, when the intelligent traffic lights do not play the real performance, which will cause a certain degree of error to the correct results of the experiment.

TABLE 3. VISSIM simulation parameter settings.

Setup unit	Parameter
Intersection shape	Cross
Number of lanes	Two way single lane
Number of vehicles per lane	0~2000
Simulation duration	1000 s
Random seed	20
Intelligent traffic light nodes	0~100
Flow detector	Parking line location for each lane

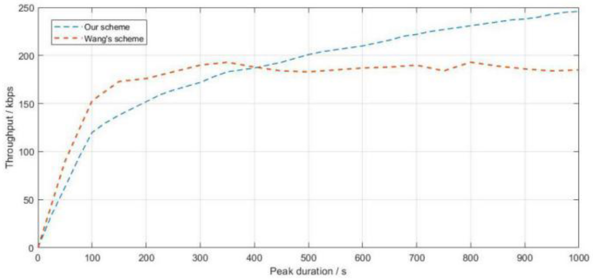

FIGURE 7. Impact of peak operation duration on throughput.

As shown in Figure 6, abscissa represents the duration of intelligent traffic light peak operation, in seconds(s), and ordinate represents real-time intersection throughput, in kbps. It can be clearly seen that before the peak operation duration of the traditional intelligent traffic light scheme reaches 400s, the real-time traffic throughput gradually increases while tends to be flat, which is better than the scheme in this paper. However, with the duration exceeding 400s, due to the advantages of ITL block distribution in this scheme, the ledger information transmission has adapted to the real environment, and because of the existence of redundant cutting technology, the system can complete the decision-making task of larger throughput, which makes the real-time intersection throughput of this scheme surpass the traditional scheme. At the same time, it can maintain a certain degree of upward trend. However, the throughput of the traditional scheme can only be kept below 200kbps, and there is a upper limit of throughput.

As shown in Figure 8, abscissa represents the duration of peak operation of intelligent traffic lights, in seconds(s), and ordinate represents the packet loss rate in $\times\ 10^{-4}\%$ of account books in blockchain. It can be seen from the figure that before the peak operation time of intelligent traffic lights reaches 600s in the traditional scheme, the overall curve shows an upward trend. However, in the second half of the curve, due to the adaptive influence of the system environment, it slightly fell back, and finally kept close to the level of $5\times10^{-4}\%$. The account packet loss rate caused by the scheme in this paper tends to be stable after the peak operation time is about 350s. In addition to the help of the system's own adaptive ability to the environment, it is more because the improved smart contract in the scheme in this paper is gradually playing a role, making the packet loss rate finally fall below $4\times10^{-4}\%$.

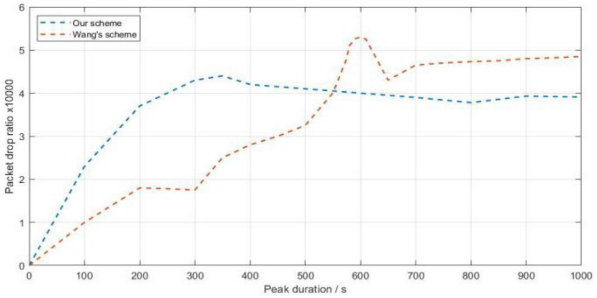

FIGURE 8. Impact of peak operation duration on packet loss rate.

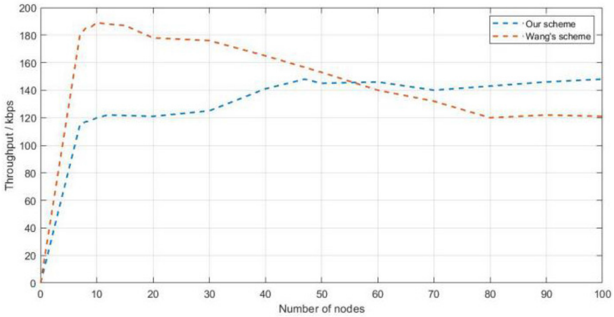

FIGURE 9. Impact of intelligent traffic light nodes on throughput.

At the same time of maintaining the peak operation of intelligent traffic lights, this paper also carried out repeated simulation experiments for the same indicators of the nodes of intelligent traffic lights.

As shown in Figure 9, the abscissa represents the number of nodes of intelligent traffic lights, and the ordinate represents the real-time intersection throughput, in kbps. It can be seen from the figure that with the increase of the number of intelligent traffic light nodes, the traditional scheme will reach a peak when the number of nodes is about 10. It is estimated that the throughput can reach 191kbps, but it will gradually fall back to around 120kbps later. The rising trend of the scheme in this paper will stop when the number of nodes reaches about 8, and then the redundant cutting technology starts to play a role. It optimizes the account book transmission process to make the throughput climb to about 145kbps stably, and when the number of nodes reaches 56, it will reverse the traditional scheme in throughput.

Similarly, as shown in Figure 10, the abscissa represents the number of nodes of the intelligent traffic light, and the ordinate represents the packet loss rate of the account book in the blockchain, with the unit of $\times\ 10^{-4}\%$. It can be seen from the figure that with the increase of the number of intelligent traffic light nodes, the rate curve of account packet loss in the blockchain shows a steady upward trend, both in the traditional scheme and in this scheme. When the number of

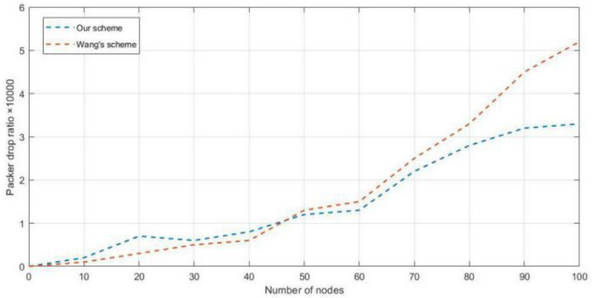

FIGURE 10. Impact of the number of intelligent traffic light nodes on packet loss rate.

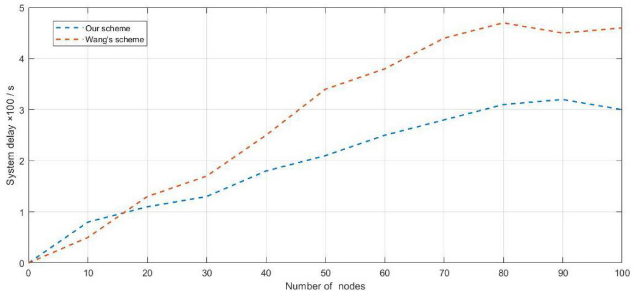

FIGURE 11. Impact of intelligent traffic light nodes on system delay.

intelligent traffic light nodes reaches 46, the account packet loss rate of this scheme gradually starts to play the powerful adaptive ability of block distribution, and the rising speed of packet loss rate slows down, and finally stays at about $3.2\times10^{-4}\%$. In the traditional scheme, the packet loss rate of account book keeps increasing at a linear speed, and breaks through $5\times10^{-4}\%$ before the end of simulation.

2) TIME COST ANALYSIS

In addition to analyzing the scheme architecture from the perspective of communication cost, it also needs to further analyze its feasibility from the perspective of time cost. Further simulation experiments are also carried out according to the parameter list in Table 3. In terms of time cost index, the reduction of system delay is often a necessary condition for a new scheme to be proposed. In the huge intelligent traffic light network, a system delay is needed to identify the feasibility of the scheme, so this paper selects the system delay in the analysis of time cost.

In Figure 11, the abscissa represents the number of nodes of the intelligent traffic light, and the ordinate represents the overall delay of the intelligent traffic light system, with the unit of $\times\ 10^{-2}$s. It can be seen from the figure that the delay curves of the two schemes increase slowly with the increase of the number of nodes of the intelligent traffic lights, and the difference is that when the number of nodes exceeds 16, the delay growth rate of the scheme in this paper has been greatly reduced. Even when the number of nodes reaches 90, the curve shows a downward trend. This is because with the increase of nodes in this scheme, the execution of smart contracts between nodes will become ''simplified'' because of the existence of information cutting. This ''simplification'' is through the adaptive stage of the system, rather than the formal simplification of the smart contract itself. This shows the superiority of the scheme in the control system delay.

C. SUMMARY OF SIMULATION EXPERIMENT RESULTS

According to the simulation experiment analysis in Section VI, it can be seen that this scheme has considerable advantages over the traditional intelligent traffic light scheme in terms of communication cost and time cost, especially in terms of real-time intersection throughput, account packet loss rate, system delay and other indicators. At the same time, this advantage will be more obvious when the traffic network becomes larger because of the characteristics of blockchain's own distributed architecture. The feasibility and effectiveness of the scheme are verified by simulation.

VII. CONCLUSION

Based on the in-depth discussion, analysis and verification of the security field of intelligent traffic lights, this paper proposes an intelligent traffic lights system under the distributed security architecture based on blockchain technology, which can prevent malicious attacks against some nodes from invading and resulting in the collapse of the whole system. In this scheme, the redundant cutting technology proposed by Edge Intelligence is also used to improve and innovate the existing smart contract, and through the simulation and comparative experiment of this scheme, it is proved that this scheme can effectively reduce the huge communication load and time cost caused by information transmission in the consensus process of intelligent traffic light block network. Intelligent traffic light system is an important component to realize intelligent traffic in the future. In view of the research of its combination with blockchain technology, we will continue to carry out a series of research work.

REFERENCES

[1] J. Zhang, W. Wang, C. Lu, J. Wang, and A. K. Sangaiah, ''Lightweight deep network for traffic sign classification,'' *Ann. Telecommun.*, to be published, doi: 10.1007/s12243-019-00731-9.

[2] J. Zhang, S. Zhong, T. Wang, H.-C. Chao, and J. Wang, ''Blockchain-based systems and applications: A survey,'' *J. Internet Technol.*, to be published.

[3] M. Bani Younes and A. Boukerche, ''Intelligent traffic light controlling algorithms using vehicular networks,'' *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 5887–5899, Aug. 2016.

[4] Z. Li, C. Li, Y. Zhang, and X. Hu, ''Intelligent traffic light control system based on real time traffic flows,'' in *Proc. 14th IEEE Annu. Consum. Commun. Netw. Conf. (CCNC)*, Las Vegas, NV, USA, Jan. 2017, pp. 624–625.

[5] A. A. Zaid, Y. Suhweil, and M. A. Yaman, ''Smart controlling for traffic light time,'' in *Proc. IEEE Jordan Conf. Appl. Electr. Eng. Comput. Technol. (AEECT)*, Aqaba, Jordan, , Oct. 2017, pp. 1–5.

[6] J. Jin and X. Ma, ''A group-based traffic signal control with adaptive learning ability,'' *Eng. Appl. Artif. Intell.*, vol. 65, pp. 282–293, Oct. 2017.

[7] J. Jin and X. Ma, ''Hierarchical multi-agent control of traffic lights based on collective learning,'' *Eng. Appl. Artif. Intell.*, vol. 68, pp. 236–248, Feb. 2018.

[8] S. H. He, K. Xie, X. Zhou, T. Semong, and J. Wang, ''Multi-source reliable multicast routing with QoS constraints of NFV in edge computing,'' *Electronics*, vol. 8, no. 10, p. 1106, Oct. 2019.

[9] Q. Wu, F. He, and X. Fan, ''The intelligent control system of traffic light based on fog computing,'' *Chin. J. Electron.*, vol. 27, no. 6, pp. 1265–1270, Nov. 2018.

[10] J. Liu, J. Li, L. Zhang, F. Dai, Y. Zhang, X. Meng, and J. Shen, "Secure intelligent traffic light control using fog computing," *Future Gener. Comput. Syst.*, vol. 78, no. 2, pp. 817–824, Jan. 2018.

[11] M.-D. Pop, "Traffic lights management using optimization tool," *Procedia Social Behav. Sci.*, vol. 238, pp. 323–330, Jan. 2018.

[12] C. Vilarinho, J. P. Tavares, and R. J. Rossetti, "Intelligent traffic lights: Green time period negotiaton," *Transp. Res. Procedia*, vol. 22, pp. 325–334, Jan. 2017.

[13] K. M. A. Yousef, A. Shatnawi, and M. Latayfeh, "Intelligent traffic light scheduling technique using calendar-based history information," *Future Gener. Comput. Syst.*, vol. 91, pp. 124–135, Feb. 2019.

[14] H. Gao, Y. Xu, Y. Yin, W. Zhang, R. Li, and X. Wang, "Context-aware QoS prediction with neural collaborative filtering for Internet-of-Things services," *IEEE Internet Things J.*, to be published.

[15] H. Gao, Y. Duan, L. Shao, and X. Sun, "Transformation-based processing of typed resources for multimedia sources in the IoT environment," *Wireless Netw.*, to be published, doi: 10.1007/s11276-019-02200-6.

[16] H. Gao, W. Huang, and X. Yang, "Applying probabilistic model checking to path planning in an intelligent transportation system using mobility trajectories and their statistical data," *Intell. Automat. Soft Comput. (Autosoft)*, vol. 25, no. 3, pp. 547–559, 2019.

[17] Y. Yin, J. Xia, Y. Li, Y. Xu, W. Xu, and L. Yu, "Group-wise itinerary planning in temporary mobile social network," *IEEE Access*, vol. 7, pp. 83682–83693, 2019.

[18] Y. Yin, L. Chen, Y. Xu, J. Wan, H. Zhang, and Z. Mai, "QoS prediction for service recommendation with deep feature learning in edge computing environment," *Mobile Netw. Appl.*, Apr. 2019, doi: 10.1007/s11036-019-01241-7.

[19] H. Gao, W. Huang, Y. Duan, X. Yang, and Q. Zou, "Research on cost-driven services composition in an uncertain environment," *J. Internet Technol.*, vol. 20, no. 3, pp. 755–769, 2019.

[20] J. Yu, J. Li, Z. Yu, and Q. Huang, "Multimodal transformer with multi-view visual representation for image captioning," *IEEE Trans. Circuits Syst. Video Technol.*, to be published.

[21] J. Yu, M. Tan, H. Zhang, D. Tao, and Y. Rui, "Hierarchical deep click feature prediction for fine-grained image recognition," *IEEE Trans. Pattern Anal. Mach. Intell.*, to be published.

[22] J. Yu, C. Zhu, J. Zhang, Q. Huang, and D. Tao, "Spatial pyramid-enhanced NetVLAD with weighted triplet loss for place recognition," *IEEE Trans. Neural Netw. Learn. Syst.*, vol. 31, no. 2, pp. 661–674, Feb. 2020.

[23] T. Wang, H. Luo, X. Zheng, and M. Xie, "Crowdsourcing mechanism for trust evaluation in CPCS based on intelligent mobile edge computing," *TISTACM Trans. Intell. Syst. Technol.*, vol. 10, no. 6, pp. 1–19, Oct. 2019.

[24] T. Wang, Y. Mei, W. Jia, X. Zheng, G. Wang, and M. Xie, "Edge-based differential privacy computing for sensor–cloud systems," *J. Parallel Distrib. Comput.*, vol. 136, pp. 75–85, Feb. 2020.

[25] Y. Wu, H. Huang, Q. Wu, A. Liu, and T. Wang, "A risk defense method based on microscopic state prediction with partial information observations in social networks," *J. Parallel Distrib. Comput.*, vol. 131, pp. 189–199, Sep. 2019.

[26] Y. Wu, H. Huang, N. Wu, Y. Wang, M. Z. Alam Bhuiyan, and T. Wang, "An incentive-based protection and recovery strategy for secure big data in social networks," *Inf. Sci.*, vol. 508, pp. 79–91, Jan. 2020.

[27] T. Wang, H. Ke, X. Zheng, K. Wang, A. K. Sangaiah, and A. Liu, "Big data cleaning based on mobile edge computing in industrial sensor-cloud," *IEEE Trans. Ind. Informat.*, vol. 16, no. 2, pp. 1321–1329, Feb. 2020.

[28] A. Thakre, F. Thabtah, S. R. Shahamiri, and S. Hammoud, "A novel block chain technology publication model proposal," *Appl. Comput. Inform.*, to be published, doi: 10.1016/j.aci.2019.10.003.

[29] P. Helo and Y. Hao, "Blockchains in operations and supply chains: A model and reference implementation," *Comput. Ind. Eng.*, vol. 136, pp. 242–251, Oct. 2019.

[30] F. Longo, L. Nicoletti, A. Padovano, G. D'atri, and M. Forte, "Blockchain-enabled supply chain: An experimental study," *Comput. Ind. Eng.*, vol. 136, pp. 57–69, Oct. 2019.

[31] Y. Lei, X. Zhao, Y. Sun, J. Zhang, H. Zhang, K. Wang, L. Jia, Y. Jin, and B. Hu, "FCSP blockchain: Fair contract exchange protocol based on blockchain technology," *Softw. J.*, vol. 2, no. 3, pp. 1–13, Oct. 2018, doi: 10.13328/j.cnki.jos.005880.

[32] X. Xu, X. Qi, J. Wang, Q. Li, and W. Sun, "Scalable management mechanism of Internet of Things based on blockchain," *Comput. Appl. Res.*, vol. 4, no. 3, pp. 1–5, 2019, doi: 10.19734/j.issn.1001-3695.2019.01.0022.

[33] Y. Wei, S. Lv, X. Guo, Z. Liu, Y. Huang, and B. Li, "FSSE: Forward secure searchable encryption with keyed-block chains," *Inf. Sci.*, vol. 500, pp. 113–126, Oct. 2019.

[34] R. C.-W. Phan and D. Wagner, "Security considerations for incremental hash functions based on pair block chaining," *Comput. Secur.*, vol. 25, no. 2, pp. 131–136, Mar. 2006.

[35] S. Yadav and S. P. Singh, "Blockchain critical success factors for sustainable supply chain," *Resour., Conservation Recycling*, vol. 152, Jan. 2020, Art. no. 104505.

[36] Y. Ren, Y. Leng, F. Zhu, J. Wang, and H.-J. Kim, "Data storage mechanism based on blockchain with privacy protection in wireless body area network," *Sensors*, vol. 19, no. 10, p. 2395, May 2019, doi: 10.3390/s19102395.

[37] Y. Ren, F. Zhu, J. Qi, J. Wang, and A. K. Sangaiah, "Identity management and access control based on blockchain under edge computing for the industrial Internet of Things," *Appl. Sci.*, vol. 9, no. 10, p. 2058, May 2019, doi: 10.3390/app9102058.

[38] Y. Ren, Y. Leng, Y. Cheng, and J. Wang, "Secure data storage based on blockchain and coding in edge computing," *Math. Biosci. Eng.*, vol. 16, no. 4, pp. 1874–1892, Mar. 2019, doi: 10.3934/mbe.2019091.

[39] J. Wang, Y. Gao, W. Liu, A. K. Sangaiah, and H.-J. Kim, "An intelligent data gathering schema with data fusion supported for mobile sink in wireless sensor networks," *Int. J. Distrib. Sensor Netw.*, vol. 15, no. 3, Mar. 2019, Art. no. 155014771983958, doi: 10.1177/1550147719839581.

[40] J. Wang, Y. Gao, X. Yin, F. Li, and H.-J. Kim, "An enhanced PEGASIS algorithm with mobile sink support for wireless sensor networks," *Wireless Commun. Mobile Comput.*, vol. 2018, pp. 1–9, Dec. 2018.

[41] J. Wang, X. Gu, W. Liu, A. K. Sangaiah, and H.-J. Kim, "An empower hamilton loop based data collection algorithm with mobile agent for WSNs," *Hum.-Centric Comput. Inf. Sci.*, vol. 9, no. 1, pp. 1–4, 2019, doi: 10.1186/s13673-019-0179-4.

[42] S. He, K. Xie, K. Xie, C. Xu, and J. Wang, "Interference-aware multi-source transmission in multi-radio and multi-channel wireless network," *IEEE Syst. J.*, vol. 13, no. 3, pp. 2507–2518, May 2019.

[43] J. Wang, W. Wu, Z. Liao, A. K. Sangaiah, and R. Simon Sherratt, "An energy-efficient off-loading scheme for low latency in collaborative edge computing," *IEEE Access*, vol. 7, pp. 149182–149190, 2019.

[44] S. He, Z. Li, Y. Tang, Z. Liao, F. Li, and S.-J. Lim, "Parameters compressing in deep learning," *Comput., Mater. Continua*, vol. 61, no. 3, pp. 321–336, 2019.

[45] Y. Yuan and F. Wang, "Current situation and prospect of blockchain technology development," *J. Autom.*, vol. 3, pp. 481–494, Mar. 2016.

[46] K. Li and C. Liu, "Edge intelligence: Current situation and prospect," *Big Data*, vol. 3, no. 1, pp. 69–75, 2019.

[47] A. Mitra and S. Sundaram, "Byzantine-resilient distributed observers for LTI systems," *Automatica*, vol. 108, Oct. 2019, Art. no. 108487.

[48] S. Lu, Q. Wei, and W. Shen, "Integrated simulation platform of VISSIM excel VBAMATLAB," *J. Transp. Syst. Eng. Inf. Technol.*, vol. 12, no. 4, pp. 43–48, 2012.

[49] P. Marc, "Blockchain technology: Principles and applications," in *Research Handbook on Digital Transformations* (Microscopic Traffic Flow of Traffic Simulation), M. Fellendorf, P. Vortisch, New York, NY, USA: Springer, 2010, pp. 63–93.

[50] G. Asaithambi, V. Kanagaraj, K. K. Srinivasan, and R. Sivanandan, "Study of traffic flow characteristics using different vehicle-following models under mixed traffic conditions," *Transp. Lett.*, vol. 10, no. 2, pp. 92–103, Mar. 2018.

[51] D. Wang and M. Li, "An intelligent traffic light control algorithm based on traffic flow," *Comput. Appl. Softw.*, vol. 32, no. 6, pp. 241–244, Mar. 2015.

PENGJIE ZENG is currently pursuing the bachelor's degree from the Hunan University of Science and Technology. His research field is the application of blockchain in the Internet of Things, cyberspace security, privacy protection, and large data processing and analysis. He received the Second Prize at the National College Students Innovative Electronic Design Competition and the Third Prize at the School-Level Financial Management Data Analysis Competition. He is currently in charge of leading the Technical Team to complete the development of a smart agriculture project and an intelligent traffic light project.

XIAOLIANG WANG (Member, IEEE) received the B.E. degree in computer engineering from Xiangtan University, China, and the master's degree of computer science from the joint education of Xiangtan University and the Institute of Computing Technology of the Chinese Academy of Sciences, China, and the Ph.D. degree from Hunan University, China. He has worked at Xiangtan University and the Nanjing Government of China, and has also worked as a postdoctoral Researcher at the University of Alabama, USA. He is currently a Professor of information technology and the Director of the Department of Internet of Things Engineering, Hunan University of Science and Technology, China. He leads a team of researchers and students in the areas of information security and the Internet of Things, such as VANET security, anonymous authentication in ad hoc networks. He has published more than 30 highly reputed SCI/EI indexed journals/conferences articles. His research has been funded by the Natural Science Foundation Committee and the Ministry of Education of China.

HAO LI is currently pursuing the bachelor's degree from the Hunan University of Science and Technology. His research interests are data analysis, algorithm design, and the Internet of vehicles security. He received the Second Prize of Hunan University from the Students Innovation and Entrepreneurship Competition and the Third Prize of "Challenge Cup" from Extracurricular Academic Research Competition. He is currently in charge of a National Innovation and Entrepreneurship Training Program for college students and applies for a software copyright. He is also the most Active Academic Student Organization Director of the School of Computer Science and Engineering, Hunan University of Science and Technology.

FRANK JIANG received the master's degree in computer science from the University of New South Wales (UNSW), Australia and the Ph.D. degree from The University of Technology Sydney, Australia. He gained three and a half years of postdoctoral research experience at UNSW. He is currently a Senior Lecturer of cyber security with the School of Info Technology Campus, Deakin University, Australia. He has published over 100 highly reputed SCI/EI indexed journal/conferences papers. His main research interests include data-driven cyber security, predictive analytics, biologically inspired learning mechanism, and its application in the complex information security systems.

ROBIN DOSS (Senior Member, IEEE) received the B.E. degree in electronics and communication engineering from the University of Madras, India, and the master's and Ph.D. degrees from the Royal Melbourne Institute of Technology (RMIT), Australia. He was a part of the Technical Services Group, Ericsson Australia, and a Research Engineer at RMIT University. He is currently a Professor of information technology and the Deputy Head of the School of Information Technology, Deakin University, Australia. He leads a team of researchers and Ph.D. students in the broad areas of communication systems and cybersecurity with a focus on emerging domains, such as the IoT, pervasive computing, applied machine learning, and ambient intelligence. His research has been funded by the National Security Science and Technology Branch of the Office of National Security in collaboration with the Defence Signals Directorate, the Australian Research Council, and industry partners. He is the Founding Chair of the Future Network Systems and Security Conference series. He is also an Associate Editor of the *journal of Cyber-Physical Systems*.