frontiers | Frontiers in Sustainable Cities

TYPE Original Research
PUBLISHED 07 August 2024
DOI 10.3389/frsc.2024.1426036

OPEN ACCESS

EDITED BY
Krishna Kumar Mohbey,
Central University of Rajasthan, India

REVIEWED BY
Ioannis Karamitsos,
Rochester Institute of Technology Dubai, United Arab Emirates
Saha Reno,
Ahsanullah University of Science and Technology, Bangladesh

*CORRESPONDENCE
Ling-Chun Liu
d110056004@mail.nchu.edu.tw
Hsing-Chung Chen
cdma2000@asia.edu.tw;
shin8409@ms6.hinet.net

RECEIVED 30 April 2024
ACCEPTED 04 July 2024
PUBLISHED 07 August 2024

CITATION
Chen C-L, Tu C-Y, Deng Y-Y, Huang D-C, Liu L-C and Chen H-C (2024) Blockchain-enabled transparent traffic enforcement for sustainable road safety in cities.
Front. Sustain. Cities 6:1426036.
doi: 10.3389/frsc.2024.1426036

Blockchain-enabled transparent traffic enforcement for sustainable road safety in cities

Chin-Ling Chen[1,2], Cheng-Yang Tu[2], Yong-Yuan Deng[2], Der-Chen Huang[3], Ling-Chun Liu[3]* and Hsing-Chung Chen[4,5]*

[1]School of Information Engineering, Changchun SciTech University, Changchun, China, [2]Department of Computer Science and Information Engineering, Chaoyang University of Technology, Taichung, Taiwan, [3]Department of Computer Science and Engineering, National Chung-Hsing University, Taichung, Taiwan, [4]Department of Computer Science and Information Engineering, Asia University, Taichung, Taiwan, [5]Department of Medical Research, China Medical University Hospital, China Medical University, Taichung, Taiwan

With the progress of the times, cars have become an important means of transportation in our lives. However, with new cars of all kinds, road safety issues still cannot be effectively improved. While countries have responded by enforcing traffic laws and using electronic technology to enhance enforcement, challenges still need to be addressed, including blurred images and misjudgments by police agencies, and even exploiting loopholes in traffic enforcement frameworks to evade consequences through bribery or connections. exacerbating an accident and leaving victims and families in the lurch of the aftermath. To solve this problem, we proposed a data traceability law enforcement system based on blockchain and InterPlanetary File System (IPFS). The system ensures rapid traceability and protects law enforcement data from external attacks. The goal of leveraging blockchain's decentralized nature and smart contracts is to instill accountability and fairness in road safety measures, mitigate the effects of corruption, and pave the way for a safer and more just transportation environment. Our experimental results show that under our stress test of 50 transactions per second, the throughput can be as high as 300 and the maximum delay can reach 2.01s, which is enough to experimentally prove that our system is feasible. Our approach is designed to solve the data corruption problem caused by the centralized server being paralyzed. It applies to all technology enforcement, with high flexibility and scalability for all participants to join or set privileges. we also provide an automated traffic law enforcement system in a smart city. To make the data storage more secure and fair, and not easily damaged by malicious people or tampered with by intentional attackers. This brings a breakthrough to the country's program security.

KEYWORDS

Hyperledger fabric blockchain, traffic law enforcement, security, smart contract, traceability

1 Introduction

Road safety is a global concern for nations, driving the deployment of cross-border traffic law enforcement systems. Despite their pivotal role in curbing reckless driving and reducing accidents, a glaring issue threatens the effectiveness of these systems. The shadow of corruption looms, casting doubt on the integrity of mechanisms designed to protect lives on our roads. According to the statistical data provided by the World Health Organization (WHO) on road

safety, nearly 1.3 million people die in car accidents worldwide each year, and 20 to 50 million people suffer non-fatal injuries (World Health Organization, n.d.). The latest annual report of the European Union (E.U.) Road Safety reported that 18,800 fatalities were attributable to major car accidents in 2020, including 12,561 deaths caused by motor vehicles (European Commission, 2022). According to the latest public report of the National Highway Traffic Safety Administration (NHTSA) in the United States (U.S.), 42,915 people died due to major car crashes in 2021 (National Center for Statistics and Analysis, 2022). In Japan, 2,101 people died in major crashes, according to a report from the Japanese Police Department Traffic Bureau in 2021 (Japan National Police Agency, n.d.). Many cases of heavy road crashes are related to the speed of people driving, so no timely response to avoid danger, out of control, and regret. Car speed affects the distance required to break in an emergency. The faster the speed, the higher the chance of an accident.

The World Health Organization (WHO) released a report in 2004 (Peden et al., 2004) to urge countries to pay more attention to road safety, raise awareness of traffic accidents, and solve them effectively. Many countries have taken steps to introduce traffic laws and regulations, intending to penalize violators through fines. This measure aims to decrease the frequency of risky driving behaviors, making roads safer for everyone. With the rapid development of technology and the rise of the Internet of Things (IoT), countries have also begun to use electronic technology to assist traffic enforcement, such as speed cameras, red light cameras, and closed circuit television, which are everywhere we can see in our daily lives. For example, artificial intelligence or machine learning can optimize videos or images, improve the identification rate, and help the road police catch and track illegal vehicles. In recent years, researchers have used conventional neural networks (CNN) multi-tasking to identify and track motorcycle riders with or without a helmet to collect road safety data in 2020 (Lin et al., 2020). Some studies have used three-dimensional visualization techniques to identify driving violations at urban intersections and to collect data on vehicles during peak hours to prevent violations and improve intersection safety (Li et al., 2020). Some scholars have also proposed new license plate recognition technology designs to improve the recognition of license plates by cameras in different environments during daytime and night, allowing a major step forward in technological enforcement (Rademeyer et al., 2020).

Although these studies have significantly improved the hardware and software functions of law enforcement systems, the blurring of images can be significantly improved, and the rate of misjudgment by police agencies can be reduced. However, people often exploit the vulnerabilities within the traffic law enforcement framework. The disconcerting reality is that some can sidestep consequences for their actions through bribery or connections, undermining the intended legal repercussions. This exacerbates the severity of accidents and leaves victims and their families grappling with the aftermath.

A critical reevaluation and fortification of our approach to road safety are imperative. Innovative solutions are needed to address the shortcomings of existing systems and fundamentally transform the landscape, making it resistant to corruption and ensuring justice prevails on our roads.

Therefore, we propose implementing a data traceability enforcement system, utilizing blockchain technology and the InterPlanetary File System (IPFS). This system will ensure that law enforcement data can be quickly traced to its source and protected from external malicious attacks and tampering. By leveraging blockchain technology's decentralized, transparent, and tamper-resistant characteristics, we aim to instill a new level of accountability and fairness in road safety initiatives. The goal is not only to mitigate the impact of corruption but also to pave the way for a safer, more just transportation landscape for all.

Blockchain network system technology, which is the future trend, can be broadly classified into four distinct types: public blockchain, private blockchain, consortium blockchain, and hybrid blockchain. The blockchain network system collectively maintains a database by using peer-to-peer decentralization and trust. It also features anonymity, non-tamper ability, traceability, and scalability. Different types of blockchain systems are used in various situations. For example, public blockchain is used for cryptocurrency transactions to ensure all transaction information is open, fair, and transparent. A private blockchain is used for enterprise internal information security, and it is closed to public networks to avoid data leakage. The production supply chain uses consortium blockchain, where many stakeholders will cooperate to form a consortium to ensure that the information among members of the consortium is open and transparent, while non-members cannot enter and obtain information. Blockchain technology has also found widespread application across numerous professional domains in recent years. For example, production management in the supply chain traceability and verification (Chen et al., 2021b), online traceable insurance system (Chen et al., 2021a), sharing of private medical information of hospital patients (Huang et al., 2022a), the subscription management system of digital media platforms (Huang et al., 2022b), and digital identity management of road vehicles (Feng et al., 2022). All witness to the application status of blockchain network technology in the future.

To address the limitations of the previous system, this study aims to achieve the following objectives:

(1) *Decentralized system architecture*: A blockchain network system is a decentralized network system that can prevent attacking servers and causing damage to the entire network system from malicious people. At the same time, it can also avoid improper information leakage.
(2) *Information non-repudiation*: We use ECDSA as a signature for users to upload data to ensure non-repudiation. Therefore, when any information is uploaded to the blockchain network system, the signature can be used to know who sent the information.
(3) *Traceability and transparency of information*: A blockchain system is like a chain of chains. In a consortium chain blockchain system, everyone who participates in the system is a beneficiary. Therefore, everyone has the same right to access any data on the blockchain, thus achieving information traceability and information.
(4) *Dispute resolution issues*: The issuance of fines for traffic violations often causes car owners to be dissatisfied with the fines. This study uses blockchain technology to cooperate with traffic law enforcement and proposes a feasible dispute resolution mechanism.

(5) *Replay attack*: Malicious people will use repetitive packet transmission to paralyze the target server. In our proposed blockchain system, there is a consensus mechanism: whenever someone wants to upload data, they will first send the data to other participants for verification. To ensure the legitimacy of transactions, it is essential that the information can be uploaded to the blockchain center. Otherwise, any unauthorized information will be promptly deleted and discarded.

(6) *Man-in-the-middle attack*: Hackers will tamper with the transmitted messages or put malicious code on the network by intercepting packets. Our system uses asymmetric cryptography, public key encryption, and private key decryption. Therefore, if a hacker intercepts the information, it will not be able to tamper with the information because there is no private key.

We will present our work in the following sections. Section 2 discusses the basic background knowledge relevant to this article. In Section 3, we detail the methodology of our framework and the system protocol. Section 4 provides a comprehensive overview of the security measures of the system. Section 5 presents the performance analysis and evaluation of the server after installation. Finally, we conclude the article.

2 Preliminary

2.1 Literature review

There are some blockchain applications in various fields in the past literature; we organized them in Table 1. Blockchain technology is a breakthrough technology that solves the trust problem in online transactions.

2.2 Traffic law enforcement

Traffic law enforcement utilizes automatic detection and measurement technology to capture traffic violations or traffic accidents, transmitting the network to transmit information back to the relevant traffic departments for data analysis and processing (Fisher, 1980). Cameras play an essential role in the traffic law enforcement system. Standard speed cameras can be divided into three major categories: radar speed systems, laser speed systems, and S induction coil speed systems. The radar speed system is the most commonly used method, based on the Doppler Effect (Eckart, 1968). It transmits radio waves to a target object and calculates the time to send and receive them. The relative movement speed between the radar and the target object is then determined. If the target is stationary, the wavelength of the reflected radio wave remains unchanged. If the target object is moving, the wavelength of the reflected radio wave changes. Conversely, intelligent cameras combine machine learning and recognition to identify traffic violations and issue penalties automatically.

2.3 Blockchain

Blockchain technology originated from Nakamoto's Bitcoin (Nakamoto, 2019), which uses peer-to-peer methods to collectively maintain databases in a decentralized and trusted manner. Blockchain technology operates independently of third-party intermediaries by utilizing decentralized nodes to store, verify, transmit, and communicate network data. Each interconnected block contains the hash value of the preceding block, ensuring data immutability once linked. Refer to Figure 1 for an illustration of the fundamental blockchain architecture.

Blockchain technology has several key characteristics, including decentralization, anonymity, immutability, traceability, and extensibility.

2.4 Hyperledger fabric

There are four different types of blockchain: public blockchain, private blockchain, consortium blockchain, and hybrid blockchain. In a public blockchain, data are entirely transparent and accessible to all participating nodes, unlike in a private blockchain, which maintains a

TABLE 1 Review past articles and current applications in various fields.

Authors	Year	Objective	Method and results
Chen et al. (2021b)	2021	Production management in the supply chain traceability and verification	Blockchain can be used in the production supply chain to achieve the purpose of traceability and effective anti-counterfeiting of tobacco products.
Chen et al. (2021a)	2021	Online traceable insurance system	Design traceability for insurance policy systems. This allows the insurance company to enforce the rights and interests of the policy through the system when it encounters an injury and prevents the insurance company from denying the bill.
Huang et al. (2022a)	2022	Sharing of private medical information of hospital patients	Solve the personal information security hazard caused by electronic medical data being used by the hospital for other experiments or leaked without the patient's knowledge.
Huang et al. (2022b)	2022	The subscription management system of digital media platforms	In the digital media era, protect creators' intellectual property rights and avoid being persecuted by media companies or platforms for their interests.
Feng et al. (2022)	2022	Digital identity management of road vehicles	Under the Internet of Vehicles technology, all cars will share road information with each other and use blockchain for digital verification to avoid attacks on the Internet of Vehicles system, thus protecting the safety of every passerby.

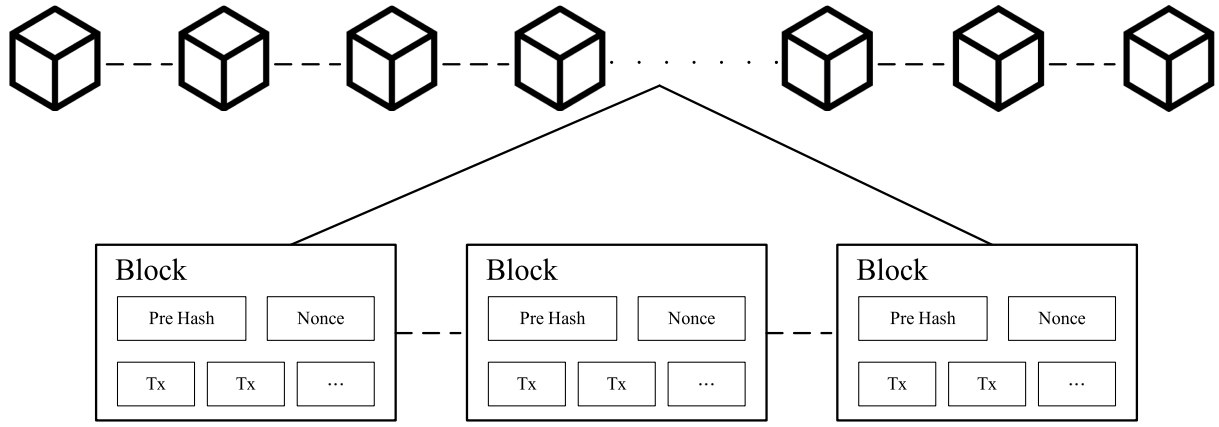

FIGURE 1
The basic blockchain architecture.

level of confidentiality. Private chains exhibit a high degree of centralization, catering solely to the internal data management needs of a single organization. The consortium blockchain is the most flexible one. As long as the participating nodes can form a consortium, the data will only circulate in this consortium. Hyperledger Fabric is a kind of consortium blockchain. Hyperledger Fabric is an open-source system, a project created and managed by the Linux Foundation, dedicated to building a transparent, secure, and decentralized enterprise blockchain solution (Hyperledger Fabric Docs, n.d.; The Linux Foundation, n.d.). Hyperledger Fabric is less costly, more efficient, more architecturally flexible, scalable, and confidential than public and private chains.

2.5 Smart contract

A smart contract is a computer command stored in a blockchain center that includes the logic to create and modify ledgers. It can be written in various programming languages, such as Solidity, Java, Python, C++, and Golang (Buterin, 2014; Amin et al., 2020). Smart contracts are just like automated programs that execute content and enable applications when triggered by conditions within the blockchain, such as production supply chain management (Chen et al., 2021b), policy benefits tracking (Chen et al., 2021a), and medical information sharing (Huang et al., 2022a).

In Hyperledger Fabric, chaincode functions as the smart contract. Chaincode is created and executed through peer nodes and comes in two main types: endorsement system chaincode (ESCC) and validation system chaincode (Androulaki et al., 2018).

2.6 InterPlanetary File System (IPFS)

InterPlanetary File System is a kind of protocol called peer-to-peer. It was proposed by Juan Benet in 2014 to achieve decentralized storage, sharing, and persistence of files (Benet, 2014).

When the user uploads data to the storage in IPFS, IPFS will first compute the hash function by SHA-256, which becomes the file storage address, and return it to the user. Anyone who wants to access a file must use this address to download it. Nowadays, IPFS has been applied and analyzed in many ways, such as the application of IPSF in the industrial IoT (Shahjalal et al., 2022), the analysis of decentralized applications of IPFS (Casino et al., 2019), and the application in decentralized web pages (Antelmi et al., 2022), which are all contributions of IPFS in the technology.

2.7 Elliptic Curve Digital Signature Algorithm (ECDSA)

Elliptic Curve Digital Signature Algorithm (ECDSA) combines Elliptic Curve Cryptography (ECC) and Digital Signature Algorithm (DSA) (Johnson et al., 2001). With the same level of security as Rivest-Shamir-Adleman (RSA), ECDSA can provide smaller keys and relatively faster computation speed.

3 The proposed scheme

3.1 System architecture

(1) *Smart Camera (SC)*: Responsible for taking pictures and recording the images of violating vehicles.
(2) *Traffic Control Center (TCC)*: Responsible for handling traffic-related events, including traffic signal control, traffic accident handling, and automatic detection of weather and road conditions. The photos uploaded by the smart camera will be automatically signed and certified by the smart contract, and a timestamp will be added to achieve the non-repudiation of the violation information.
(3) *Roadside Unit (RSU)*: Assist smart camera to calculate and transmit the photo data taken, or transmit real-time information between vehicles, so that the incoming information is kept at zero time difference and the network information flows smoothly.
(4) *Police Agency (PA)*: To report and send fines to vehicle owners for traffic violation events.
(5) *Department of Motor Vehicle (DMV)*: Responsible for vehicle inspection, licensing, and registration review and management

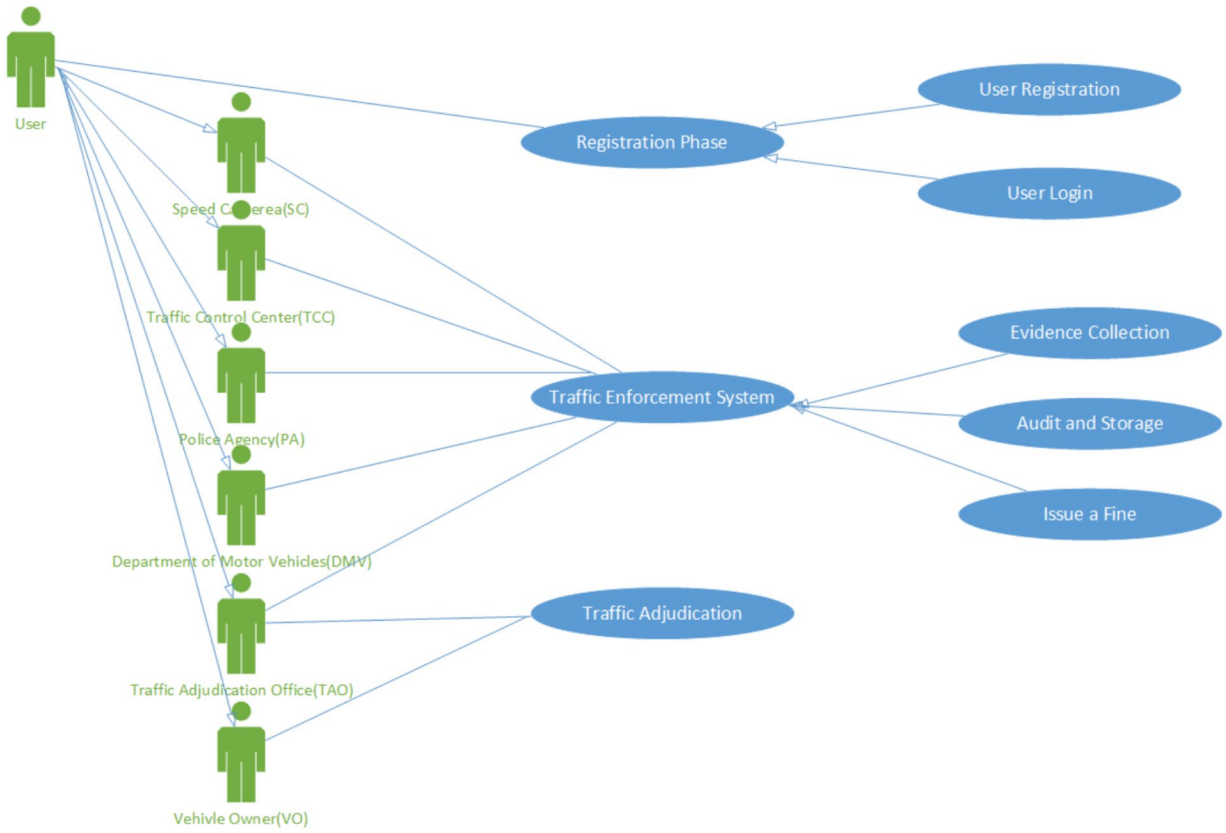

FIGURE 2
System UML diagram.

of the inspection plant, as well as the penalty, complaint, and relief for violations of highway law, road traffic management, and mandatory automobile liability insurance.

(6) *Traffic Adjudication Office (TAO)*: Assist in the arbitration of traffic violations, complaints, administrative litigation, and refund cases. If a vehicle owner has any problems after receiving a ticket, he/she can file a complaint with the Traffic Adjudication Office.

(7) *Vehicle Owner (VO)*: A person who owns a car or other motor vehicle.

(8) *Competent Authorities (CA)*: Responsible for the registration and certification of organizations and issuance of public and private keys.

(9) *Blockchain Center (BCC)*: Blockchain Center will store the file address of each IPFS return to achieve no tampering, traceability, and high security to avoid lobbying.

(10) *InterPlentary File System (IPFS)*: Responsible for storing photos, time, and smart camera ID of traffic violations with a P2P feature to prevent data deletion by malicious people. Unlike traditional centralized databases, it provides faster and more secure storage space.

Figure 2 shows the system UML diagram. The characters in the figure can be subdivided into Smart Camera (SC), Traffic Control Centre (TCC), Police Agency (PA), Department of Motor Vehicle (DMV), Police Unit (PA), and Traffic Adjudication Office (TAO), and the relationship between all characters in the method, and the function of the system. It can be seen in the figure that all characters are involved in the system. When the offenders appear, the Smart Camera will start a new event and go from the chain center to the center of the blockchain.

Figure 3 illustrates the System Architecture, delineating scenarios depicting the journey of evidence transmission from smart cameras to vehicle owners. This process involves several entities, including the traffic control center, roadside unit, police agency, and Department of Motor Vehicles. Further elaboration on this process is provided below:

Step 1: Traffic Control Centre (TCC), Police Agency (PA), Department of Motor Vehicle (DMV), Police Agency (PA), and Traffic Adjudication Office (TAO) must register with the Blockchain Center. After applying for registration, it will be certified by CA and issued public–private key pairs. It will be considered a node in the blockchain and join the organization to form a federation chain with other organizations.

Step 2: When someone's speeding violation is captured by a Smart Camera (SC), the captured photo will be transmitted to the control center via RSU.

Step 3: After receiving the photos, the control center will use artificial intelligence or manual audit to identify the license plate. Then, the photo, smart camera number, location, and vehicle-related information will be transferred to IPFS for storage and ECDSA signature with a time stamp through a smart contract.

Step 4: The Police Agency (PA) is notified when a new record is available on the blockchain. The PA can get the hash value from

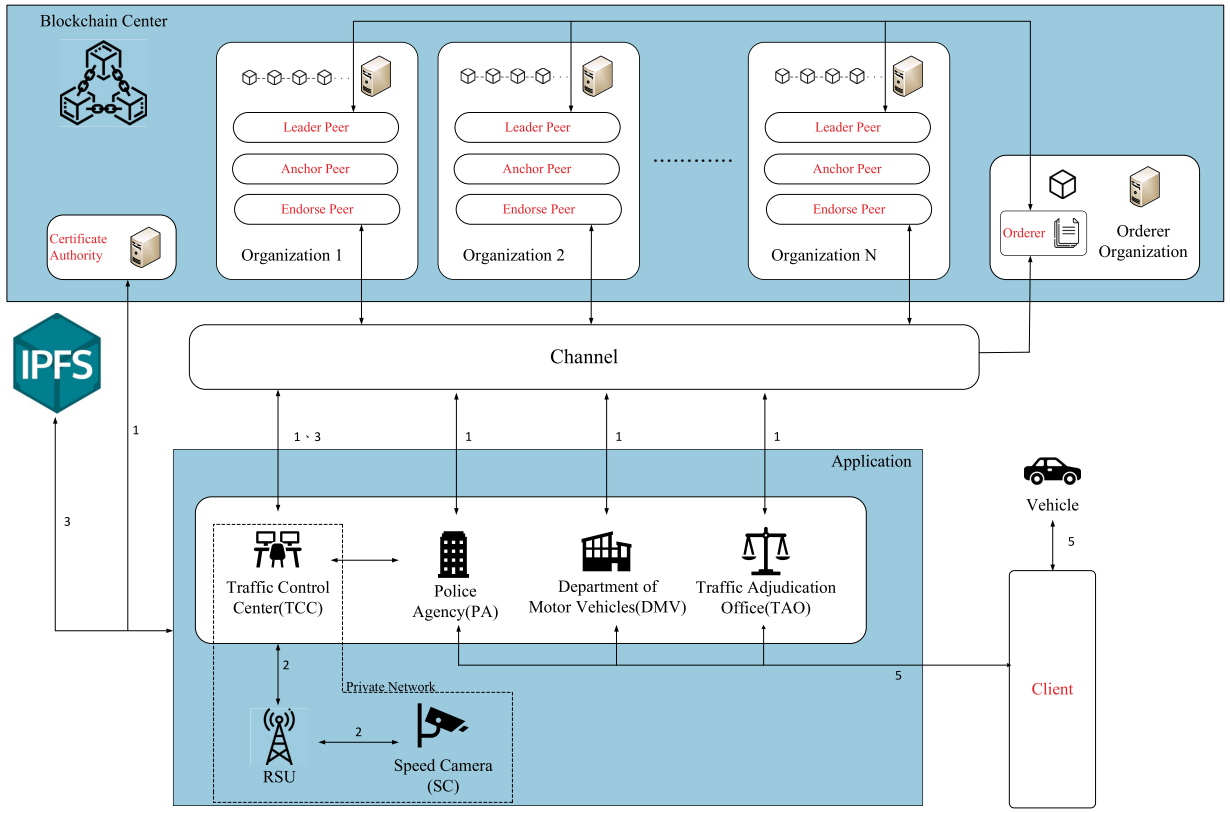

FIGURE 3
System architecture diagram. The figure shows the process and work order of the entire system.

the blockchain and download the related prosecution evidence from IPFS to issue a fine to the owner.

Step 5: Vehicle Owner (VO) receives the fine and can directly pay the fine to the supervisory station or appeal to the traffic incident arbitration office if he/she is not satisfied.

3.2 Notation

M_P	The photo is captured by a smart camera
M_i	The ith unencrypted information
M_{vo}	The information from the vehicle owner
M_{Fine}	Relevant violation information (e.g., fine amount, reason).
$Fine$	Fine
ID_x	The x's account number is recorded in the blockchain center
ID_{SC}	The number of smart cameras
ID_{LPN}	License plate number
ID_{Fine}	Fine number
Adr	Location of smart camera

d_x	ECDSA private key of the party x
Q_x	ECDSA public key of the party x
G	A generating point based on the elliptic curve E
k_i	The ith ECDSA random number
v	The variable is defined in the verification function.
T_x	The time recorded by x
T_i	The ith timestamp
$"\tau$	The valid range of the timestamp
C_i	The number of i ciphertext
$H(\ )$	One-way hash function, used in the ECDSA signature
h_i	The ith hash value
h_{IPFS}	The IPFS hash value and location of the data
$(r_{\mathrm{Xi}}, s_{\mathrm{Xi}})$	The number of i ECDSA signature value of X
$(x_{\mathrm{Xi}}, y_{\mathrm{Xi}})$	The number of i Elliptic curve signature value of X
$E_{Puk_x}(M) / D_{Prkx}(M)$	Encrypt/decrypt message M with a public key or private key of the party x
$F1 \overset{?}{=} F2$	Verify that F1 is equal to F2 or not

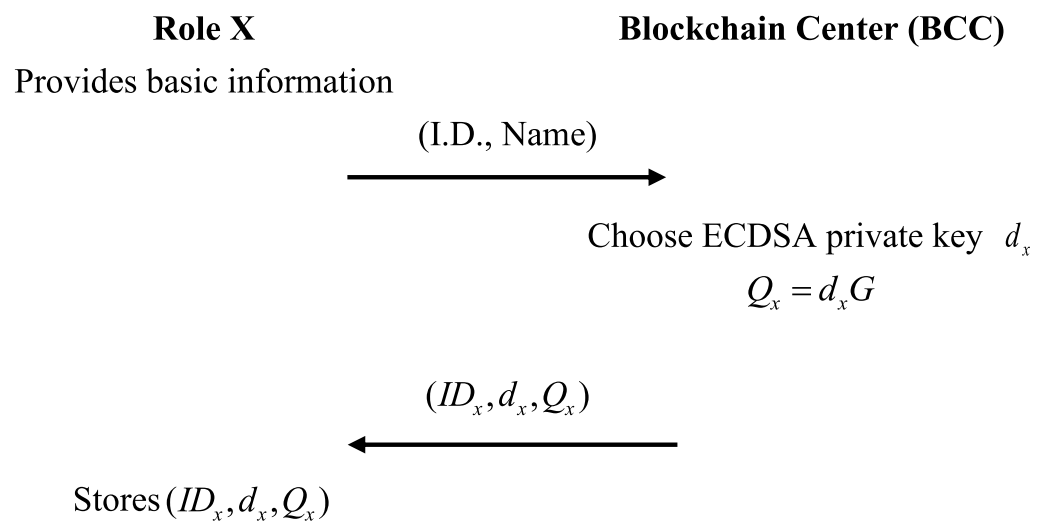

FIGURE 4
The flowchart of the registration phase. All participants need to register in the system.

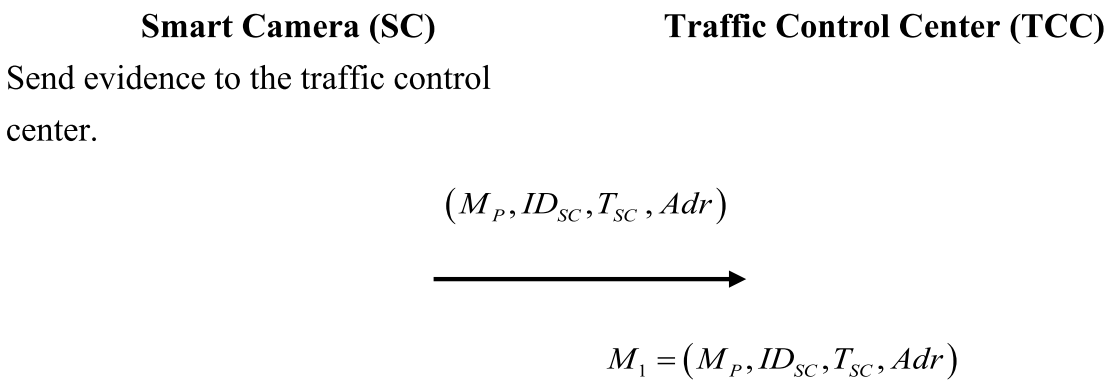

FIGURE 5
The flowchart of the evidence-collection phase. The evidence is sent to TCC from the SC.

3.3 Registration phase

All roles in the framework must first register as participants with the Blockchain Center. The participant must provide basic information, and the Blockchain Center will use the ECDSA signature to generate the private key and calculate the public key, which is then returned to the applicant. The flowchart of the registration phase is shown in Figure 4.

Step 1: Role X provides the blockchain center basic information (e.g., name, role, ID, and address).

Step 2: The blockchain center will use the private key d_x to calculate the public key Q_x, showns in Equation (1):

$$Q_x = d_x G \tag{1}$$

Role X must be authenticated by CA when registering. If the CA approves the application of role X, it will execute the register function of Algorithm 1. The blockchain center will then send (ID_x, d_x, Q_x) back to Role X.

Step 3: Role X receives (ID_x, d_x, Q_x) and stores it.

ALGORITHM 1 *func register (name string, role string, ID string, adr string)*

```
(name string, role string, id string, adr string){
    AP = AP_information{
        ID: id,
        Name: name,
        Role: role,
        Address : adr
    }
}
```

3.4 Evidence collection phase

After the smart camera captures the violation, it transmits it to the traffic control center through the dedicated network of roadside unit connections. Figure 5 shows the flowchart of the evidence-collection phase.

Step 1: The smart camera will send the photo that was taken, as well as the number, time, and location, to the traffic control center through a dedicated network. The computation is shown in Equation (2):

$$M_1 = (M_P, ID_{SC}, T_{SC}, Adr) \tag{2}$$

3.5 Audit and storage phase

When the traffic control center receives evidence from the smart camera, it automatically identifies the license plate and obtains relevant vehicle owner information through image recognition. The collected data will then be transferred to IPFS for storage, where a hash value is calculated to serve as the data storage address. This hash value is then sent back and uploaded to the blockchain. Figure 6 shows the flowchart of the audit and storage phase.

Step 1: After receiving the message, TCC will check the timestamp first in Equation (3):

$$T_{NOW} - T_{SC} \le \Delta\tau \tag{3}$$

Obtain license plate and owner information through image recognition in Equation (4):

$$M_2 = (M_1, ID_{LPN}, M_{vo}) \tag{4}$$

Select a random number k_1 and timestamp T_1 to calculate the hash value of the message, it is shown in Equation (5):

$$h_1 = H(M_2, T_1) \tag{5}$$

Execute Algorithm 2, call the Sign function, and make a signature. It is shown in Equation (6):

$$(r_{TCC}, s_{TCC}) = Sign(h_1, k_1, d_{TCC}) \tag{6}$$

Use PA's public key to the crypto messenger. It is shown in Equation (7):

$$C_1 = E_{Puk_{PA}}(M_2) \tag{7}$$

Finally, upload $(ID_{TCC}, C_1, (r_{TCC}, s_{TCC}), T_1)$ to IPFS and store it.

Step 2: Equation (8), IPFS receives the stored message from TCC:

$$M_3 = (ID_{TCC}, C_1, (r_{TCC}, s_{TCC}), T_1) \tag{8}$$

Compute IPFS hash value of M_3, It is shown in Equation (9):

$$h_{IPFS} = H(M_3) \tag{9}$$

Return h_{IPFS} to TCC

Step 3: After receiving h_{IPFS}, TCC will get the timestamp T_2 and license plate ID_{LPN}. Last, upload $(h_{IPFS}, T_2, ID_{LPN})$ to BCC and send to PA.

Step 4: In Equation (10), the PA uses the V.O.'s license plate number ID_{LPN} to find the data in the block on the blockchain.

$$(h_{IPFS}, T_2, ID_{LPN}) \tag{10}$$

Additionally, use the hash value h_{IPFS}, download M_3 from IPFS.

Step 5: After PA gets M_3. In Equation (11), PA will check the timestamp. In Equation (12), it checks the timestamp:

$$M_3 = (ID_{TCC}, C_1, (r_{TCC}, s_{TCC}), T_1) \tag{11}$$

$$T_2 \overset{?}{>} T_1 \tag{12}$$

Decrypt C_1 Equation (13), get M_2:

$$M_2 = D_{\Pr k_{PA}}(C_1) \tag{13}$$

In Equation (14), compute the hash value of M_2 then get h_1':

$$h_1' = H(M_2, T_1) \tag{14}$$

Execute Algorithm 3 and call the function Verify to ensure the integrity of data sources. Finally, check if v is legal or illegal to r_{TCC}. If legal, it means that the data source is correct, and returns Valid; otherwise, it returns Invalid. As shown in Equation (15).

$$\text{Call } func\ Verify(h_1', r_{TCC}, s_{TCC}), \text{verify}, v \overset{?}{=} r_{TCC} \tag{15}$$

ALGORITHM 2 *func Sign(h string, k string, d string)*

```
(r string, s string){
    (x, y) = k * G
    r = x mod n
    s = k^-1 (h + r * d) mod n
    return r, s
}
```

ALGORITHM 3 *func Verify (h string, r string, s string)*

```
(result string){
    u1 = h * s^-1 mod n
    u2 = r * s^-1 mod n
    X = (x, y) = u1 * G + u2 * Q
    v = x mod n
    if v == r{
        return "valid"
    }else{
        return "invalid"
    }
}
```

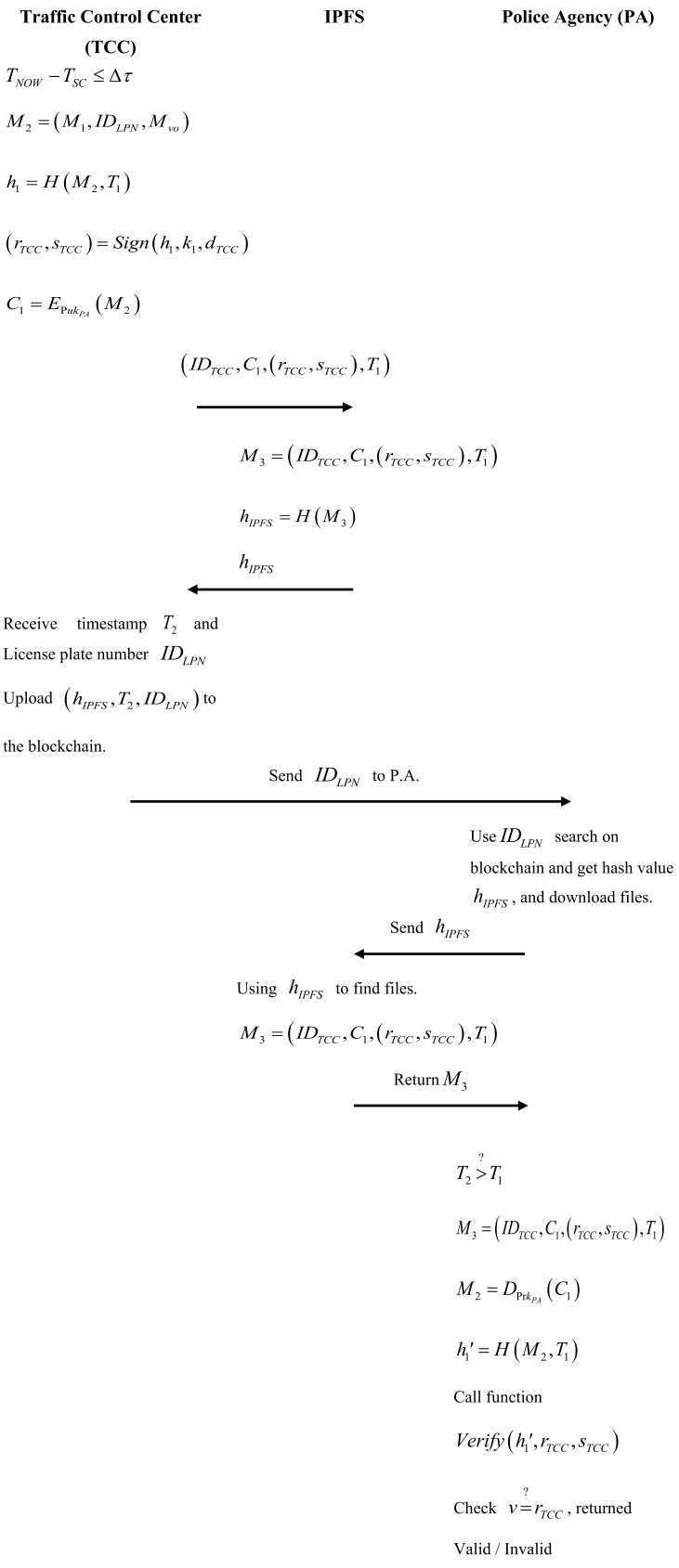

FIGURE 6
The flowchart of the audit and storage phase. TCC storage evidence and forward to the PA.

3.6 Issue a fine phase

When a new block is created in the blockchain, all participants can access the data in the blockchain center. After receiving the information from the traffic control center, the PA can search data addresses h_{IPFS} through the license plate ID_{LPN} and download the data stored in IPFS. The data are decrypted, and its signature is verified to ensure its integrity and legality.

When the return is legal, the police will issue a fine based on the data, then sign a signature to the data and upload it to the IPFS. Getting the address of the IPFS hash value, the PA will upload it to the blockchain center and send the fine to the VO Figure 7 shows the flowchart of issuing a fine.

Step 1: In Equation (16), after confirming that the information is legal, the PA will issue a fine based on the information:

$$Fine = \left(ID_{Fine}, M_2, M_{Fine}\right) \tag{16}$$

Select a random number k_2 and timestamp T_3. Then, compute hash values of *Fine* Equation (17):

$$h_2 = H\left(Fine, T_3\right) \tag{17}$$

In Equation (18), execute Algorithm 2 and call function Sign to generate signature:

$$\left(r_{PA}, s_{PA}\right) = Sign\left(h_2, k_2, d_{PA}\right) \tag{18}$$

In Equation (19), encrypt messenger by TAO's public key:

$$C_2 = E_{\mathrm{Pu}k_{TAO}}\left(Fine\right) \tag{19}$$

Finally, upload $\left(ID_{PA}, C_2, \left(r_{PA}, s_{PA}\right), T_3\right)$ to IPFS.

Step 2: In Equation (20), after IPFS receives data to be stored by the PA:

$$M_4 = \left(ID_{PA}, C_2, \left(r_{PA}, s_{PA}\right), T_3\right) \tag{20}$$

Equation (21), compute the hash value of data:

$$h_{IPFS} = H\left(M_4\right) \tag{21}$$

Step 3: The IPFS data storage address h_{IPFS} is received by the PA The PA will upload $\left(h_{IPFS}, T_4, ID_{Fine}\right)$ to the blockchain center and send the fine to VO

Step 4: When receiving a fine, the VO will compute the hash value of the fine Equation (22):

$$h_2^{'} = H\left(Fine, T_3\right) \tag{22}$$

Execute Algorithm 3 caLL function Verify. Verify messages to ensure the integrity of data sources. Finally, check if v is legal or illegal to r_{PA}. If legal, it means that the data source is correct, and returns Valid; otherwise, returns Invalid.

$$Call\ \ func\ Verify\left(h_2^{'}, r_{PA}, s_{PA}\right), \text{verify} \overset{?}{v = r_{PA}} \tag{23}$$

3.7 Arbitration phase

If VO has any problems or is dissatisfied after receiving the fine. VO can proceed with a complaint with TAO. Submit the fine number and vehicle information to the TAO.

When the TAO conducts a complaint and receives information from the VO, it will compare the information from the Blockchain Center to evaluate, enforce, or revoke the violation. Figure 8 displays the flowchart of the arbitration phase.

Step 1: Verification of the authenticity and legality of the information. VO has to submit $Fine^{'} = \left(ID_{Fine}, M_1, M_{Fine}\right)$ and the VO's information M_{VO} to TAO. TAO uses ID_{Fine} search and gets the address h_{IPFS} where the data are stored in the blockchain center. Then, download data in Equation (24) and Equation (25) and verify Equation (26), the PA's signature $\left(r_{PA}, s_{PA}\right)$ on the fine information:

$$M_3 = \left(ID_{PA}, C_2, \left(r_{PA}, s_{PA}\right)\right) \tag{24}$$

$$h_2^{'} = H\left(Fine, T_3\right) \tag{25}$$

$$\text{Call}\ func\ Verify\left(h_2^{'}, r_{PA}, s_{PA}\right) \text{verify} \overset{?}{v = r_{PA}} \tag{26}$$

If the PA's signature verification is illegal, it means that the information provided by the VO was wrong and the VO complaint failed; if the verification is successful, the process advances to the next step.

Step 2: After confirming the legitimacy of the PA's signature, TAO will decrypt the C_2 form $M_3 = \left(ID_{PA}, C_2, \left(r_{PA}, s_{PA}\right)\right)$, and then get *Fine* by Equation (27):

$$Fine = D_{\mathrm{Pr}k_{TAO}}\left(C_2\right) \tag{27}$$

Compare the information, Equation (28) provided by the VO and the data information.

$$\overset{?}{Fine = Fine}^{'} \tag{28}$$

If the information *Fine* matches M_3, it means that VO violates the law, and VO must accept the penalty.

4 Analysis

4.1 Decentralization

Many system architectures commonly use the cloud for data storage, but many cloud databases are provided through third-party organizations. If a cloud provider is attacked, it may lead to irreversible data corruption due to the centralized nature of the server.

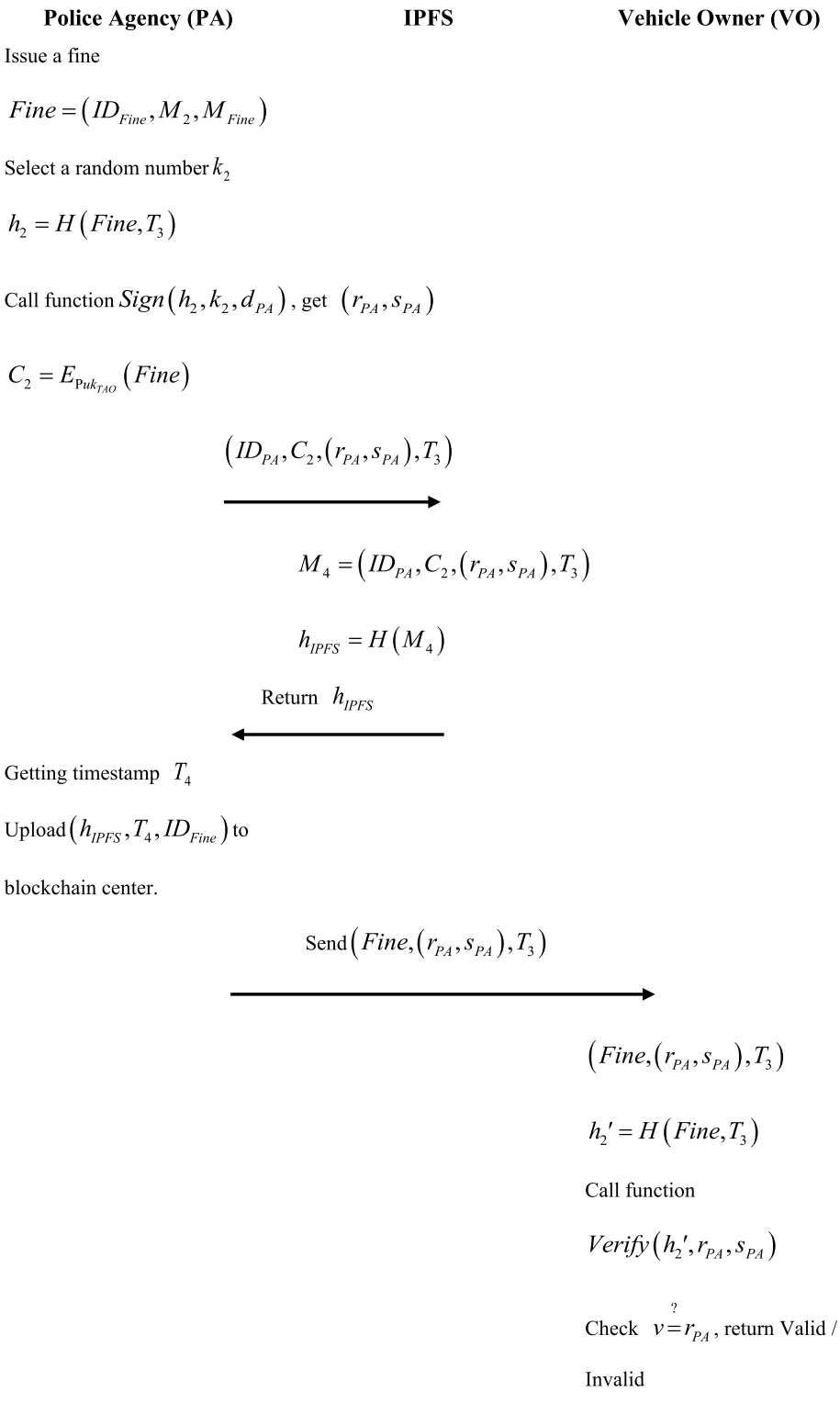

FIGURE 7
The flowchart of the issue is a fine phase. PA issue a fine to illegal CO.

Therefore, we use a blockchain network in our scheme. It relies on the P2P network mechanism, so there is not need to verify the data transmission through a third-party organization. In addition to avoiding improper information outflow. The transmission can also avoid the security concerns of centralized servers.

4.2 Non-repudiation

In this study, our framework uses EDCSA to digitally sign and verify the information to achieve a message that cannot be tampered with. When TCC sends important data to PA, TCC

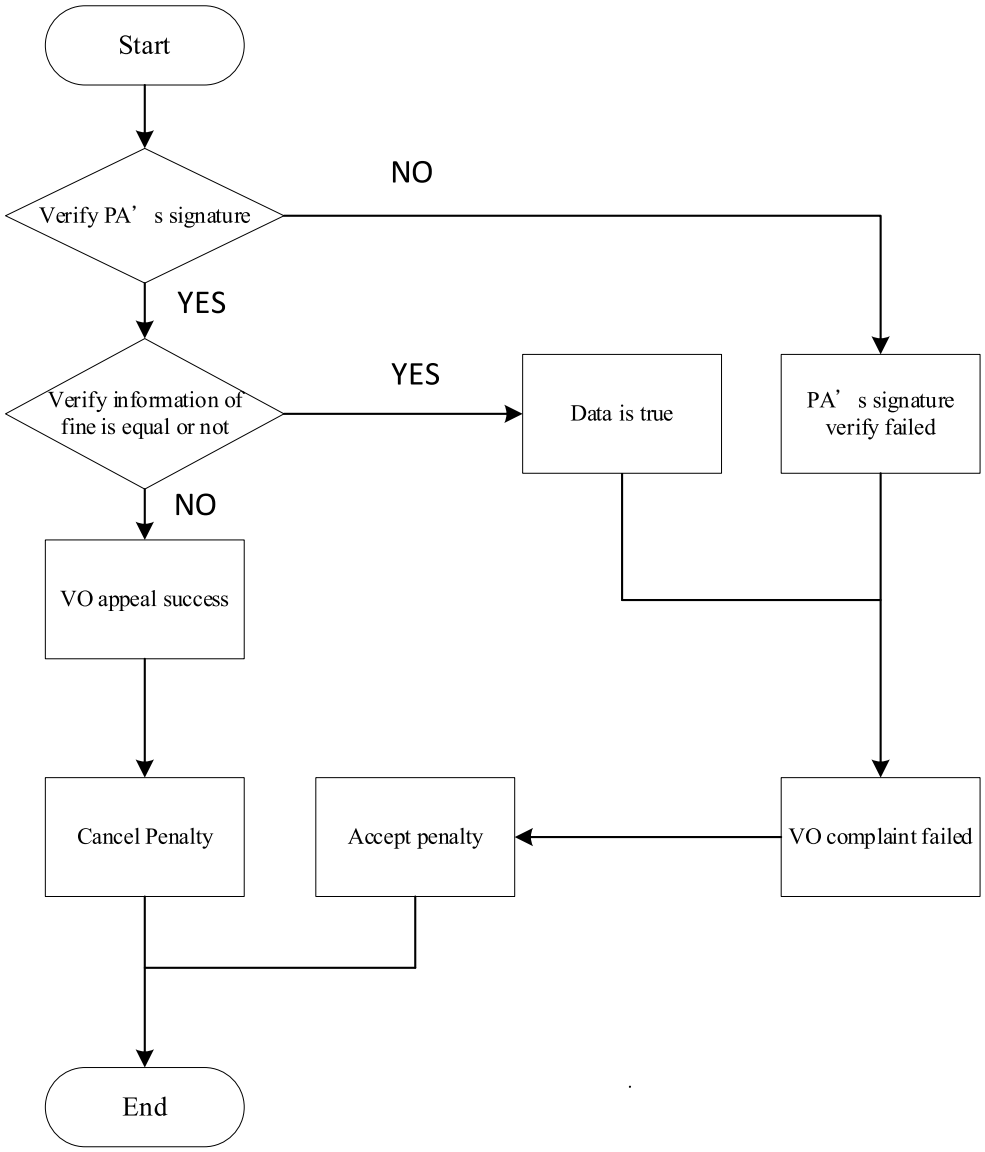

FIGURE 8
Flowchart illustrating the arbitration phase.

TABLE 2 Non-repudiation verification in each phase of this study.

Phase	Message	Sender	Receiver	Verify signature
Audit and storage phase	$(ID_{TCC}, C_1, (r_{TCC}, s_{TCC}), T_1)$	TCC	PA	$v \overset{?}{=} r_{TCC}$
Issue a fine phase	$(Fine, (r_{PA}, s_{PA}), T_3)$	PA	VO	$v \overset{?}{=} r_{PA}$

will use a private key (r_{TCC}, s_{TCC}) to sign it. P.A. receives data, and the public key is sent by TCC for signature verification $v=r_{TCC}$ to confirm that the message is sent from TCC. Similarly, PA sends the same information to ensure the information is non-repudiation. Table 2 illustrates the non-repudiation verification process of each phase in the framework:

4.3 Traceability and transparency

Upon uploading data to the blockchain center, it will include the previous block's hash value, forming a blockchain. During the audit storage stage, TCC will link $(h_{IPFS}, T_2, ID_{LPN})$ to the blockchain center, allowing the PA can use the ID_{LPN} to check the

data in the blockchain center. After the PA issues a fine, $(h_{IPFS}, T_4, ID_{Fine})$ will be linked to the blockchain center.

VO proposes an appeal to TAO that can check data by ID_{Fine}. Anything linked to the blockchain center, cannot be changed by anyone. Hence, data traceability and transparency have been achieved.

4.4 Reply attack

A reply attack is a malicious attempt to send large-flow packets, causing the target host server to be paralyzed or maliciously manipulated, thereby affecting the entire network system In the Hyperledger Fabric blockchain network system used in this study, Practical Byzantine Fault Tolerant (PBFT) is used to effectively resist such attacks, called consensus mechanism.

As shown in Figure 9, whenever a new block upload is done. It will be across to each node in the blockchain center for verification. Therefore, if a malicious person wants to use a reply attack to paralyze a server, it may only harm a few peer servers, and it is extremely difficult to bring down the whole blockchain network system.

All members must certify new blocks on the chain and confirm them as legal blocks before uploading them to the blockchain center.

4.5 Man-in-the-middle (MITM)

To prevent man-in-the-middle attacks, each important message is encrypted in our scheme.

When a malicious individual intercepts the message, they are unable to make unauthorized alterations to the decrypted message as they lack the necessary private key for decryption. In the audit and storage phase, when TCC wants to send the message to PA, it will encrypt it with PA's public key. PA will decrypt it with its private key after receiving the message. Because the private key is only owned by the PA, when a malicious person intercepts the message, there is no private key to decrypt the message. So, no malicious modification can be made to the message. Table 3 shows the encrypted communication messages of each phase.

4.6 Arbitration mechanism

In the previous arbitration process, the VO had to prepare numerous documents and wait for a long time for examination. Therefore, we propose a mechanism in which the first step is to use the PA's signature to compare the fine of the information by VO uploaded. If it matches, the next step is to make a judgment, or the fine will be returned to VO because the information on the fine does not match. In the second step, we will conduct data matching to confirm VO's license plate number, VO's name, fine, and fine number

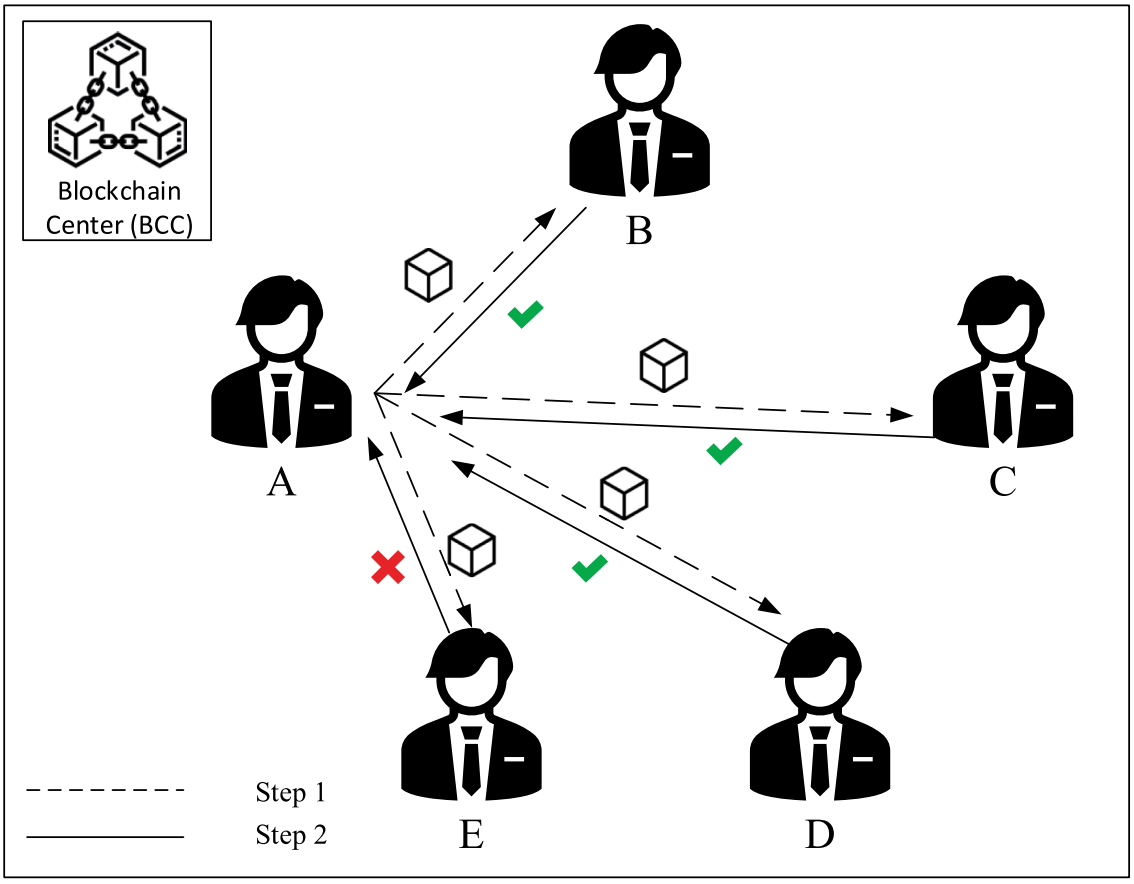

FIGURE 9
Consensus mechanism in blockchain.

for comparison. The related verification is presented in Table 4. The arbitration mechanism has been automatically determined in this article.

5 Results and discussion

5.1 Computation cost

Table 5 shows the computation costs of the proposed scheme and summarizes computational costs at each phase, focusing on asymmetrical encryption, comparison, hash functions, and multiplication operations.

5.2 Communication performance

As shown in Table 6, we compare the communication cost of each stage in 4G and 5G environments. In the 4G environment, the maximum transmission speed reaches up to 100Mbps, while in the 5G environment, it can reach 20Gbps.

5.3 Performance analysis

In this section, we assess the performance of chain code contract deployment within the system architecture of this study. The evaluation utilizes a test tool compatible with Hyperledger Fabric version 0.42, while the blockchain platform operates on Hyperledger Fabric version 2.3. The server environment comprises an Intel Core i9 9920X CPU running at 4.5 GHz with 32 GB of RAM. Configuration includes a Certificate Authority (C.A.) node, a contract node, and four peer nodes running on Ubuntu 20.04 servers. We have created a core chain code to act as the central component for submitting and retrieving transaction data from the blockchain network. In evaluating its performance, we employed Calliper v0.42 to gauge both transaction latency, which denotes the duration for chain code interaction with the ledger, and throughput, representing the rate at which transactions are committed to the ledger,

TABLE 3 Critical communications messages are encrypted at all stages of this article.

Phase	Sender	Receiver	Encrypt function	Decrypt function
Audit and storage phase	TCC	PA	$C_1 = E_{Puk_{PA}}(M_2)$	$M_2 = D_{Prk_{PA}}(C_1)$
Issue a fine phase	PA	TAO	$C_2 = E_{Puk_{TAC}}(Fine)$	$Fine = D_{Puk_{TAC}}(C2)$

TABLE 4 The arbitration mechanism has been automatically determined in this article.

Phase	Sender	Receiver	Message	Data	Verification
Arbitration phase	VO	T.A.O.	$Fine' = (ID_{Fine}, M_1, M_{Fine})$	$M_3 = (ID_{PA}, C_2, (r_{PA}, s_{PA}))$	$\overset{?}{v = r_{PA}}$
				$Fine = D_{Prk_{TAO}}(C_2)$	$\overset{?}{Fine = Fine'}$

TABLE 5 Computation costs of the proposed scheme.

Phase	TCC	PA	VO	T.A.O.
Audit and storage phase	$T_{asy} + T_{cmp} + T_h + 5T_{mul}$	N/A	N/A	N/A
Issue a fine phase	N/A	$2T_{asy} + 2T_{cmp} + 2T_h + 11T_{mul}$	N/A	N/A
Arbitration phase	N/A	*N/A*	N/A	$T_{asy} + 2T_{cmp} + T_h + 6T_{mul}$

T_{asy}: The process time for an asymmetrical signature/verifying a signature. T_{cmp}: The process time for a comparison operation. T_h: The process time for a one-way hash function. T_{mul}: The process time for a multiplication operation.

TABLE 6 The communication cost associated with the proposed scheme.

Phase	Message Length	4G (100Mbps)	5G (20Gbps)
Evidence collection phase	T_{other} = 80 bits	$80/100*10^6 = 0.8$ us	$80/20*10^9 = 0.004$ us
Audit and storage phase	$2T_{sig} + 2T_{asy} + 3T_{othe} + 2T_h = 2*512 + 2*1024 + 3*80 + 2*368 =$ 4,048 bits	$4048/100*10^6 = 0.040$ ms	$4048/20*10^9 = 0.202$ us
Issue a fine	$2T_{sig} + 1T_{asy} + 2T_{othe} + 1T_h = 2*512 + 1{,}024 + 2*80 + 2*368 =$ 2,944 bits	$2944/100*10^6 = 0.029$ ms	$2944/20*10^9 = 0.147$ us

T_{sig}: The process time to transmit an ECDSA signature (512 bits). T_{asy}: The process time to transmit an asymmetric message (1,024 bits). T_{other}: The process time to transmit information (80 bits). T_h: The process time to transmit hash value (368 bits).

measured in transactions per second (tps). These metrics are pivotal for effectively executing read and write operations across the network.

In Figure 10, we examine the sending rate and throughput. For the test, we selected 9 sending rate groups, with intervals of 50 transactions per second (tps) ranging from 300 to 700. Each tps test lasted for 2 s.

In Figure 11, we analyze the relationship between sending rate and latency. The minimum delay for writing data is 1.12 s, and the

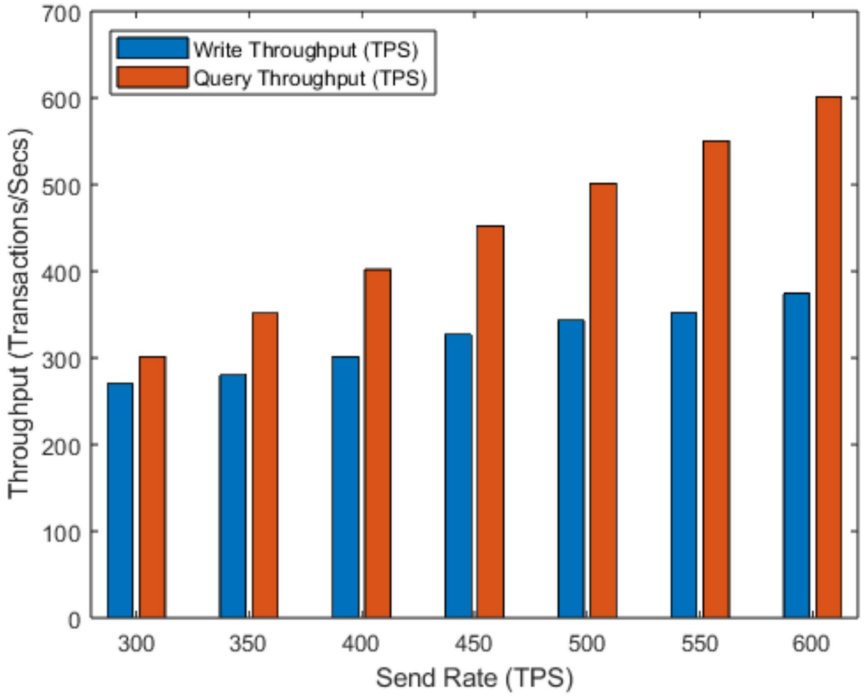

FIGURE 10
Throughput in Hyperledger Fabric environment under different workloads.

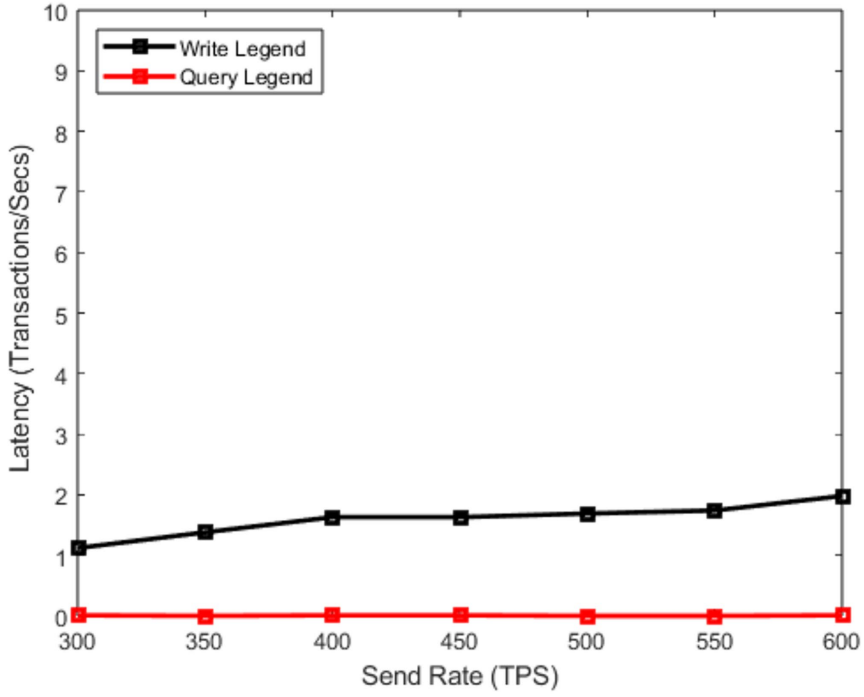

FIGURE 11
Latency time in Hyperledger Fabric environment under different workloads.

maximum delay is 2.01 s. It can be seen that the designed system is feasible.

Consequently, the proposed system demonstrates significant storage capability. The throughput is sufficiently high to support writing and reading operations during the audit, storage, and finalization phases.

6 Conclusion

In the future, smart cities will play a critical technological role. It will bring a lot of convenience on traffic roads, but at the same time, information security will be a significant issue. In this paper, we propose a data-traceable traffic law enforcement system based on blockchain and IPFS to solve the danger of speeding to other road users. We also make the violators unable to lobby. The contributions of this study are described as follows:

(1) The architecture designed in this paper uses a consortium blockchain so that all participating members can have the data. It also solves the data corruption problem caused by the centralized server being paralyzed. Unlike the current cloud backup approach, the decentralized ledger feature of the blockchain allows for continuous backup updates. The framework applies to all technology enforcement, with high flexibility and scalability for all participants to join or set privileges.
(2) This framework provides an automated traffic law enforcement system in a smart city. This makes the data storage more secure and fair, and not easily damaged by malicious people or tampered with by intentional attackers, and prevents the suspicion of gossip.
(3) In addition to the advantages brought by P2P, we also use the data address returned from the interstellar file system to upload all the data to the blockchain with the simplified hash value, which greatly reduces the burden of blockchain uploading.
(4) Unlike traditional arbitration systems, which used to take a long time from appeal to cancelation, the architecture provided in this study automatically performs discrimination testing and improves the time-consuming problem of data processing and comparison.

The future goal is to use blockchain network technology, smart city initiatives, IoT infrastructure, and artificial intelligence to build a more efficient, sustainable, and connected world. We envision a future where decentralized systems empower communities, smart cities optimize resources, IoT devices enhance daily life, and AI advances human potential, all while prioritizing privacy, security, and ethical considerations.

Data availability statement

The raw data supporting the conclusions of this article will be made available by the authors, without undue reservation.

Author contributions

C-LC: Conceptualization, Methodology, Supervision, Writing – review & editing, Formal analysis, Funding acquisition. C-YT: Conceptualization, Methodology, Software, Writing – original draft, Writing – review & editing, Resources, Validation. Y-YD: Formal analysis, Methodology, Validation, Writing – original draft, Investigation, Resources. D-CH: Investigation, Validation, Writing – review & editing, Resources. L-CL: Data curation, Software, Writing – original draft, Formal analysis, Resources. H-CC: Conceptualization, Investigation, Resources, Writing – review & editing.

Funding

The author(s) declare financial support was received for the research, authorship, and/or publication of this article. This study was supported in part by the National Science and Technology Council, Taiwan, R.O.C., under contract NSTC 112-2410-H-324-001-MY2, and contract MOST 111-2218-E-002-037. This work was also supported by the Chelpis Quantum Tech Co., Ltd., Taiwan, under the Grant number of Asia University: I112IB120.

Conflict of interest

The authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

Publisher's note

All claims expressed in this article are solely those of the authors and do not necessarily represent those of their affiliated organizations, or those of the publisher, the editors and the reviewers. Any product that may be evaluated in this article, or claim that may be made by its manufacturer, is not guaranteed or endorsed by the publisher.

References

Amin, M. R., Zuhairi, M. F., and Saadat, M. N. (2020). A survey of smart contracts: security and challenges. *Int. J. Netw. Secur* 29:3.

Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., Caro, A. D., et al. (2018). Hyperledger fabric: A distributed operating system for permissioned blockchains. Proceedings of the Thirteenth EuroSys Conference, Porto, Portugal, 23–26.

Antelmi, A., D'Ambrosio, G., Petta, A., Serra, L., and Spagnuolo, C. (2022). A volunteer computing architecture for computational workflows on decentralized web. *IEEE Access*. doi: 10.1109/ACCESS.2022.3207167

Benet, J. (2014). Ipfs-content addressed versioned, p2p file system. *arXiv*. doi: 10.48550/arXiv.1407.3561

Buterin, V. (2014). A next-generation smart contract and decentralized application platform. *white paper* 3, 2–1.

Casino, F., Politou, E., Alepis, E., and Patsakis, C. (2019). Immutability and decentralized storage: an analysis of emerging threats. *IEEE Access* 8, 4737–4744. doi: 10.1109/ACCESS.2019.2962017

Chen, C. L., Deng, Y. Y., Tsaur, W. J., Li, C. T., Lee, C. C., and Wu, C. M. (2021a). A traceable online insurance claims system based on blockchain and smart contract technology. *Sustain. For.* 13:9386. doi: 10.3390/su13169386

Chen, C. L., Lim, Z. Y., Liao, H. C., Deng, Y. Y., and Chen, P. (2021b). A traceable and verifiable tobacco products logistics system with gps and rfid technologies. *Appl. Sci.* 11:4939. doi: 10.3390/app11114939

Eckart, C. (1968). Principles and Applications of Underwater Sound (1968, Originally issued as summary technical report of division 6), vol. *7*. Washington, DC: National Defense Research Committee Reprinted by the Department of the Navy.

European Commission (2022). "Annual statistical report on road safety in the E.U., 2021" in European road safety observatory (Brussels: European Commission, Directorate General for Transport).

Feng, H., Chen, D., and Lv, Z. (2022). Blockchain in digital twins-based vehicle management in VANETs. *IEEE Trans. Intell. Transp. Syst.* 23, 19613–19623. doi: 10.1109/TITS.2022.3202439

Fisher, P. D. (1980). Law enforcement: shortcomings of radar speed measurement: It's based on sound principles, but present systems have practical limitations and may be misused. *IEEE Spectr.* 17, 28–31. doi: 10.1109/MSPEC.1980.6368323

Huang, D. C., Liu, L. C., Deng, Y. Y., and Chen, C. L. (2022a). A privacy-aware E.M.R. Sharing system combined with Blockchain and proxy re-encryption mechanisms. *Res. Square*. doi: 10.21203/rs.3.rs-2027461/v1

Huang, D. C., Liu, L. C., Deng, Y. Y., and Chen, C. L. (2022b). A digital media subscription management system combined with Blockchain and proxy re-encryption mechanisms. *Symmetry* 14:2167. doi: 10.3390/sym14102167

Hyperledger Fabric Docs. (n.d.) Read the docs. Available at: https://hyperledger-fabric.readthedocs.io/en/latest/policies/policies.html

Japan National Police Agency. (n.d.) Traffic accident occurrence status. Available at: https://www.npa.go.jp/publications/statistics/koutsuu/index_jiko.html

Johnson, D., Menezes, A., and Vanstone, S. (2001). The elliptic curve digital signature algorithm (ECDSA). *Int. J. Inf. Secur.* 1, 36–63. doi: 10.1007/s102070100002

Li, Y., Abdel-Aty, M., Yuan, J., Cheng, Z., and Lu, J. (2020). Analyzing traffic violation behavior at urban intersections: a spatio-temporal kernel density estimation approach using automated enforcement system data. *Accid. Anal. Prev.* 141:105509. doi: 10.1016/j.aap.2020.105509

Lin, H., Deng, J. D., Albers, D., and Siebert, F. W. (2020). Helmet use detection of tracked motorcycles using cnn-based multi-task learning. *IEEE Access* 8, 162073–162084. doi: 10.1109/ACCESS.2020.3021357

Nakamoto, S. (2019). Bitcoin: a peer-to-peer electronic cash system. Available at: https://bitcoin.org/bitcoin.pdf (Accessed February 11, 2012).

National Center for Statistics and Analysis (2022). Early estimate of motor vehicle traffic fatalities in 2021 (crash•stats brief statistical summary. Report no. DOT HS 813 283). Washington, DC: National Highway Traffic Safety Administration.

Peden, M., Scurfield, R., Sleet, D., Mathers, C., Jarawan, E., Hyder, A. A., et al. (2004). World report on road traffic injury prevention. Geneva: World Health Organization.

Rademeyer, M. C., Barnard, A., and Booysen, M. J. (2020). Optoelectronic and environmental factors affecting the accuracy of crowd-sourced vehicle-mounted license plate recognition. *IEEE Open J. Intel. Transport. Syst.* 1, 15–28. doi: 10.1109/OJITS.2020.2991402

Shahjalal, M., Islam, M. M., Alam, M. M., and Jang, Y. M. (2022). Implementation of a secure LoRaWAN system for industrial internet of things integrated with IPFS and Blockchain. *IEEE Syst. J.* 16, 5455–5464. doi: 10.1109/JSYST.2022.3174157

The Linux Foundation. (n.d.) Decentralized innovation. Built on trust. Available at: https://www.linuxfoundation.org/

World Health Organization. (n.d.) Road traffic injuries. Available at: https://www.who.int/news-room/fact-sheets/detail/road-traffic-injuries