Hindawi
Security and Communication Networks
Volume 2021, Article ID 5597679, 13 pages
https://doi.org/10.1155/2021/5597679

Research Article

Convergence of Blockchain and IoT for Secure Transportation Systems in Smart Cities

Khizar Abbas,[1] **Lo'Ai A. Tawalbeh**,[2] **Ahsan Rafiq**,[3] **Ammar Muthanna**,[4,5] **Ibrahim A. Elgendy**,[6,7] **and Ahmed A. Abd El-Latif**[8]

[1] *Department of Computer Engineering, Jeju National University, Jeju 63243, Republic of Korea*
[2] *Director of the Cyber Engineering Technology/Cyber Security Research Center, Department of Computing and Cybersecurity, Texas A&M University-San Antonio, San Antonio, TX, USA*
[3] *Chongqing University of Posts and Telecommunications, Chongqing 400065, China*
[4] *Telecommunication Networks and Data Transmission, St. Petersburg State University of Telecommunications, St. Petersburg 193232, Russia*
[5] *Peoples' Friendship University of Russia (RUDN University) Miklukho-Maklaya St, Moscow 117198, Russia*
[6] *School of Computer Science and Technology, Harbin Institute of Technology, Harbin 150001, China*
[7] *Computer Science Department, Faculty of Computers and Information, Menoufia University, Shebin El-Koom 32511, Egypt*
[8] *Mathematics and Computer Science Department, Faculty of Science, Menoufia University, Shebin El-Koom 32511, Egypt*

Correspondence should be addressed to Ahmed A. Abd El-Latif; a.rahiem@gmail.com

Received 30 January 2021; Revised 11 March 2021; Accepted 15 April 2021; Published 27 April 2021

Academic Editor: Debiao He

Smart cities provide citizens with smart and advanced services to improve their quality of life. However, it has been observed that the collection, storage, processing, and analysis of heterogeneous data that are usually borne by citizens will bear certain difficulties. The development of the Internet of Things, cloud computing, social media, and other Industry 4.0 influencers pushed technology into a smart society's framework, bringing potential vulnerabilities to sensor data, services, and smart city applications. These vulnerabilities lead to data security problems. We propose a decentralized data management system for smart and secure transportation that uses blockchain and the Internet of Things in a sustainable smart city environment to solve the data vulnerability problem. A smart transportation mobility system demands creating an interconnected transit system to ensure flexibility and efficiency. This article introduces prior knowledge and then provides a Hyperledger Fabric-based data architecture that supports a secure, trusted, smart transportation system. The simulation results show the balance between the blockchain mining time and the number of blocks created. We also use the average transaction delay evaluation model to evaluate the model and to test the proposed system's performance. The system will address residents' and authorities' security challenges of the transportation system in smart, sustainable cities and lead to better governance.

1. Introduction

In recent decades, rapid urbanization has been affected by urban relocation due to better employment chances and access to a better education system. Cities provide access to better services, transportation, and communication [1]. Building a smart city is no longer a vision but a reality. Smart cities endeavor to enhance citizens' lifestyle and living quality by solving common urban problems using the Internet of Things and modern technologies. Smart cities depend on data streams accumulated from numerous sensors to determine the spatiotemporal activities of the city [2]. Many organizations, government agencies, and research institutions are working hard to create a connected and well-equipped smart city. The smart city utilizes the development of the Internet of Things (IoT) [3–5], cloud computing [6, 7], and Industry 4.0, leading to potential vulnerabilities in smart city data, services, and applications. Therefore, these weaknesses make people worry about whether their data are transmitted and stored safely, confidential, and restricted for unauthorized access. Trust in smart cities is the foundation of transparency, governance, and people's participation in business, trade, and economic growth [8, 9]. Transportation is essential for improving living standards and giving people access to basic services, work, and roam around the city. Transport is an essential factor in improving the livelihoods of the citizens of a city [10]. A smart transportation system is vital to today's cities as it helps tourists and locals enjoy their urban experiences further comfortably and enjoyably. Smart cities provide effective smart transportation system solutions by encouraging innovation, facilitating a collaborative ecosystem, and achieving sustainability goals.

The authors in [11] pointed out that due to the high level of corruption in transportation-related projects, prices have increased by 30–35%. A report by the Federal Ministry of Economic Cooperation and Development, Germany, shows that corruption in the transportation sector is common and has reached the highest authorities [12]. The General Data Protection Regulation (GDPR) of the European Union (EU) has raised public awareness of personal data and data protection, which should increase end-users confidence in the use of personal data by private and public institutions. This allows the users to exchange personal data to improve big data analysis [13]. It is not easy to track mitigation measures in the transportation sector [14].

These challenges are part of the rapidly changing urban transportation system environment, seen through the smart city planner's lens. The strategies for solving urban transportation system problems are unique to each city and involve several factors. The primary purpose is to design an effective, fair, safe, and secure public transport system integrated with the blockchain and the IoT [5].

Blockchain is a digital ledger technology (DLT), which creates a chain of blocks [15]. Each block contains timestamped information or transactions. These blocks are immutable; nobody can temper them; hence, this property makes blockchain a secure and trustworthy platform [16]. Most of the consensus algorithms used in today's blockchain-based systems cannot be used on devices with minimal computing resources [17]. Proof of Work (PoW) is the first consensus algorithm introduced into the blockchain network and is used by many existing systems [18]. The distribution of the decision-making responsibility process among all individual nodes is called mining. Mining requires a lot of computing power [19]. The conventional security and privacy methods are ineffective when it comes to the smart transportation system. The main challenges that can be solved using the blockchain instead of a traditional database system are summarized as follows:

(i) Decentralization: distributed systems are very fault-tolerant. Nodes in the blockchain network do not destroy the entire system in case of failure of one node. There are other nodes on the network that can manage the blockchain. Information stored on the blockchain node is copied to all nodes on the network. This means that if one node is compromised, a hacker must change all nodes' information to process the data, whereas if the database server fails on an existing database system, the entire system is affected.

(ii) Overhead cost reduction: by maintaining a blockchain ledger through a network of distributed nodes, the company can keep hosting, security, and maintenance costs low. It eliminates a lot of IT staff costs and a lot of operational and infrastructure overhead.

(iii) Immutability: blockchain stores information that cannot be changed. This means that once the block has been confirmed, it can no longer be changed. Because many nodes store information in a secure digital ledger, they can also resist manipulation and tampering.

(iv) Transparency: transparency is an essential function of the blockchain that makes it reliable compared to traditional databases. This makes any blockchain audit flexible. There is no way to hide information about transactions that build trust and increase system value.

(v) Security: blockchain provides a secure environment because it uses advanced cryptographic technology and a decentralized network. Editing data in a block takes a lot of computer resources. This is not ideal because a potential hacker cannot change every node's data on the network. This is to prevent attacks as they are more expensive than the mining rewards. This feature helps protect the blockchain from hackers.

While blockchain technology has clear advantages and opportunities to increase efficiency and reduce costs, there are still some challenges and limitations to blockchain's widespread use in different domains. Additionally, blockchain platforms should partially or completely replace existing systems that require time and resources. In recent studies, DLT has been applied to communication systems that can almost immediately impact big data. Additionally, smart mobility requires decentralized accounts to track data generation. So, there is a need for a new or specific blockchain application to fix this problem. The proposed system adapts to vehicle innovation and supports autonomous, connected, electric, shared dockless vehicles.

Smart city transportation system has various applications, such as payment through a single interface and a shared transportation system services. The smart transportation system application also provides sustainable travel behaviors for travelers and consumers and traffic management systems, including signal and road occupation management. Another application of a smart urban transportation system is micromobility management. One of its main applications is a passenger information system that tracks passengers to manage public transport better.

We have proposed using private blockchain to address data security and transparency issues in smart cities' transportation systems. The novelty of this work is to design a decentralized platform for combining IoT and blockchain technology with smart transportation systems. This system will help enhance the legacy transportation systems by overcoming data security issues, transparency, and trust. Besides, other tests are applied, and the results are compared with the existing literature to demonstrate the effectiveness of the proposed work. The fundamental contributions of the study included the following:

(i) We present a smart transportation system by converging blockchain and IoT for smart cities

(ii) We employ a private blockchain to mitigate the trust issues and vulnerabilities in data security

(iii) We further analyze the performance of our recommended system by evaluating the private blockchain network

The rest of the article is organized as follows: related work is described in Section 2. The proposed architecture is highlighted in Section 3. Section 4 describes the implementation mechanism of the proposed blockchain and IoT-based smart transportation system. Section 5 describes the experimental results and compares them with existing work. The work is completed and any relevant issues that may arise while implementing the proposed plan are highlighted in Section 6.

2. Related Work

The attention towards developing the smart transportation system has been increasing day by day. A smart and intelligent transportation system (ITS) should be autonomous, decentralized, secure, efficient, intelligent to understand the safety level at roads and improve the user's experience [20–22]. Currently, ITSs are facing several challenges related to data integrity, centralization, and trustful communication. Besides, the data generated by the vehicles can be manipulated, intercepted, and corrupted due to the attackers [23–25]. Blockchain emerged as an innovative technology that can be able to store data securely and transparently [26, 27]. It has distributed ledger technology that provides a reliable way to perform transactions without a third-party involvement. Moreover, blockchain features such as immutability, verifiability, transparency, integrity, and security are required elements for developing a smart transportation system [28]. These revolutionary features of blockchain technology are not restricted to financial applications only, but researchers use them in many domains. As aforementioned, we have adopted blockchain technology due to its innovative features and implemented it in our proposed transportation system for smart cities environment. This system provides the users a secure and trusted platform that can store the data in an organized and transparent manner. However, we have summarized several transportation systems from the literature to understand the proposed system better.

In work by Zhang and Wang [29], a consortium blockchain-based traffic signal control system has been proposed that can save the various material and financial resources efficiently. This system can reduce human involvement in traffic signal management and overcomes centralization issues. This work is a step towards an ITS for vehicular ad hoc networks (VANETs). It can manage and control the traffic signals aptly. In the case of road congestion, the vehicles forward the messages about road conditions to the traffic department. The traffic department can optimize the traffic signal duration and update it accordingly. They can also control the vehicle status via a smart contract. This article also proposed credibility, which can prevent vehicles from broadcasting deceitful or irreverent messages. It provides a secure way of communication in the VANETs environment. Moreover, for ensuring the privacy and confidentiality of any data, an encryption algorithm named El-Gamal has been utilized. The demonstration results of the proposed system show that it can control and manage traffic signals.

The current traffic signal control systems do not have the ability to handle increasing traffic volume in urban areas. Thereby, a centralized and intelligent signal control system is needed for meeting high traffic demand. Due to the complex structure of VANETs networks, lack of security is another major issue in traditional centralized systems. However, many malicious attacks such as ghost cars and Sybil attacks are a massive threat to the security of legacy intelligent signal control systems. For these issues in traditional signal control systems, the author has proposed a distributed intelligent traffic light control system with blockchain technology [30]. It can control the existing traffic light systems and enhance security with the help of distributed ledger technology of blockchain. It can also introduce the edge intelligence for running the smart contracts, which can reduce the distributed ledger's data transmission rate to an extent. The comparison results of the proposed mechanism with existing traffic lights control systems show the system's superiority.

Wang and Zang [31] have proposed a consortium blockchain-based platform for secure data sharing and customized services. It has a ciphertext policy-based data reencryption algorithm for guaranteeing security while retrieving, forwarding, and sharing the data. This algorithm provides a secure and trustworthy environment for communication in a vehicular network. Different service organizations like traffic police, insurance companies, and maintenance companies attain the corresponding ciphertext and decrypt it. After that, smart contracts have been applied to provide customized services to the onboard units (OBUs). The presented system's performance results demonstrate that it can share the data with confidentiality and security.

Ahmed et al. [32] presented a smart parking system for smart cities that aims to provide one stop for parking services information to the customers. It brings many parking providers to one unified platform in a smart city environment. There are some trust, security, and performance concerns for making this kind of system because a tremendous amount of data is shared between multiple parties. So, security is a significant threat to the smart parking system. For handling security, privacy, and trust challenges, they have proposed a blockchain platform for developing an integrated smart parking system [33]. The authors have proposed blockchain-based outlier detection ITS system to prevent the vehicles from malicious activities while information sharing in the work by Maskey et al. [34]. Machine learning models are used with a blockchain-based ITS system to detect anomalies from the data. It is very beneficial for various ITS applications like accident detection, criminal activity detection, user profiling, and reporting, controlling, and monitoring traffic.

Another similar kind of work, blockchain-based ITS, is proposed to solve the data security and privacy issues and boost the vehicles to share their data with ITS systems [35]. Blockchain technology provides users with a secure and trustworthy way to perform transactions in the ITS system. This system can also perform services with traditional ITS and infrastructure. The proposed ITS system is scaleable and ductile enough to introduce new services anytime due to its smart contacts. The proof of concept implementation of the proposed work is based on the Ethereum blockchain platform.

Hirctan et al. have presented a blockchain-enabled reputation system for ITS in which only validated users can get traffic information from the ITS system [36]. The users can securely share or used the system-generated data and validated data while traveling between two points. The stored data are reliable based on its provider's reputation and cannot be altered or modified. The proposed system has been implemented in a simulated environment of three cities: Beijing, San Francisco, and Rome. They have implemented a routing algorithm with a blockchain network for guiding the validated cars on free routes in case any malicious information was stored in the blockchain network. The routing algorithm detects malicious information and provides accurate route information to the vehicles. Blockchain technology is usually not suitable for power-constrained IoT devices; to undertake this issue, Huang et al. [37] have proposed a credit-based PoW mechanism for IoT devices that can ensure system security and transaction efficiency at the same time. They designed data rights management methods to regulate sensor data access to protect the confidentiality of sensitive data. They have used the Raspberry Pi system application to conduct case studies from smart factories. The evaluation and analysis results show that the credit-based PoW mechanism and data access control are safe and effective in the IoT environment.

Another similar work related to blockchain in mobile crowdsensing was conducted by Huang et al. [38]. Mobile crowdsensing is integrated with industrial systems without configuring any additional devices. To overcome the shortcomings of the existing mobile crowdsensing system, they propose a blockchain-based mobile crowdsensing system. Specifically, they use miners to identify sensory data and design dynamic incentive mechanisms to place rewards that mitigate the imbalances of multiple search operations while developing personal data observation methods to identify and reduce variances in the data. They create a blockchain-based mobile crowdsensing system on Ethereum and conduct extensive experiments in the industrial IoT. Both experimental results and security analysis have shown that this system can protect industrial systems and improve the system's reliability.

The authors have proposed a multilayered blockchain-based system for smart transportation system data markets (BSMD), which handles the challenges related to security, privacy, scalability, and management in Lopez et al. 's work [39]. Each user of the system can share their encrypted data to the blockchain network with some defined rules for accessing the data. If the other party agreed with these terms and conditions, they could access the blockchain network's data. This set of defined rules or terms and conditions are known as a smart contract. So, there is a smart contract between both parties for performing the transaction in the blockchain network. Moreover, data integrity, security, transparency, immutability, and auditability are the significant features of the proposed blockchain-based BSMD system. To test the BSMD system's performance, the authors have deployed 370 peer nodes over the heterogeneous network. The proposed system ensures cybersecurity across spoofing and message attacks [40].

ITSs are getting much attention these days, but road accidents, traffic congestion, and delays have also increased significantly. So, the relevant information on these events is vital. ITS systems store multidimensional data, but recording all the data makes it very difficult to retrieve specific data when needed and remove the rest of the features [41]. For this issue, they have performed data analysis on accident datasets using AI techniques, such as nonnegative matrix factorization (NMF), principle component analysis (PCA), and linear discriminator analysis (LDA) for dimensionality reduction. After that, a blockchain-based system has been presented that can store the data about these critical events in an immutable manner [42]. So, these data are essential for other legal organizations like insurance companies. There is a smart contract between them for getting accurate information from the blockchain system. So, the proposed mechanism can provide specific dimensionality and reduced data to other legal companies. The comparative analysis of the smart transportation system with existing approaches is presented in Table 1.

3. Design and Architecture of the Proposed System

The smart city concept incorporates many innovative methods aimed at providing better solutions to residents' problems. Besides, smart cities rely on various sensor systems, cell phones, smart transportation systems, the IoT, and support home devices and enhance digital systems' integration with traditional systems [44]. The amount of data produced by these IoT devices has proliferated over the past few decades. Presently, machines are producing unprecedented data. Sensors, closed-circuit television (CCTV) cameras, and digital imaging devices produce data in a large amount and send it to storage systems that can be accessed over the Internet [45]. Mobility is a crucial point that directly affects sustainability within the smart city. It is essential to analyze the information for providing a smart transportation system for a smart city's residents within the transportation

Table 1: Comparative analysis of the proposed smart transportation system with existing approaches.

Ref. #	Platform	Smart contract	Access policy	Consensus determination	Efficiency	Functionality
[29]	Ethereum	Yes	Consortium	Selected nodes	High	Traffic signal control
[30]	Ethereum	Yes	Permissionless	All nodes	Low	Edge intelligent traffic light control system
[31]	Ethereum	Yes	Consortium	Selected nodes	Low	Secure data sharing in VANETs
[43]	No	No	No	No	Low	AI-enabled ITS system
[33]	Hyperledger Fabric	Yes	Permissionless	Complete nodes	High	Smart parking
[34]	Ethereum	Yes	Permissioned	Complete nodes	Low	Outlier detection using ML
[35]	Ethereum	Yes	Permissionless	Selected nodes	Low	ITS system
[36]	Ethereum	Yes	Permissioned	Selected nodes	High	Reputation system for smart ITS
Proposed system	Hyperledger-fabrics	Yes	Permissioned	Arbitrary nodes	High	Mitigate trust issues, secure data sharing, ensure IoT data security

system. As a starting point, we must consider that smart transportation system users' private data are confidential and must not be shared with the irrelevant party. Implementing an intelligent transport system with blockchain is the solution to this problem [46].

3.1. Convergence Scenario of Blockchain and IoT. We have designed an IoT- and blockchain-based architecture for data security and transparency in smart transportation systems. The intelligent transport network consists of various IoT devices, which are responsible for collecting and transmitting data. The data are retrieved through the gateway. The blockchain uses representational state transfer (REST) application programming interface (API) commands to interact with these devices and user displays. Users can interact with blockchain services using their smartphones, standard personal computers, or tablets.

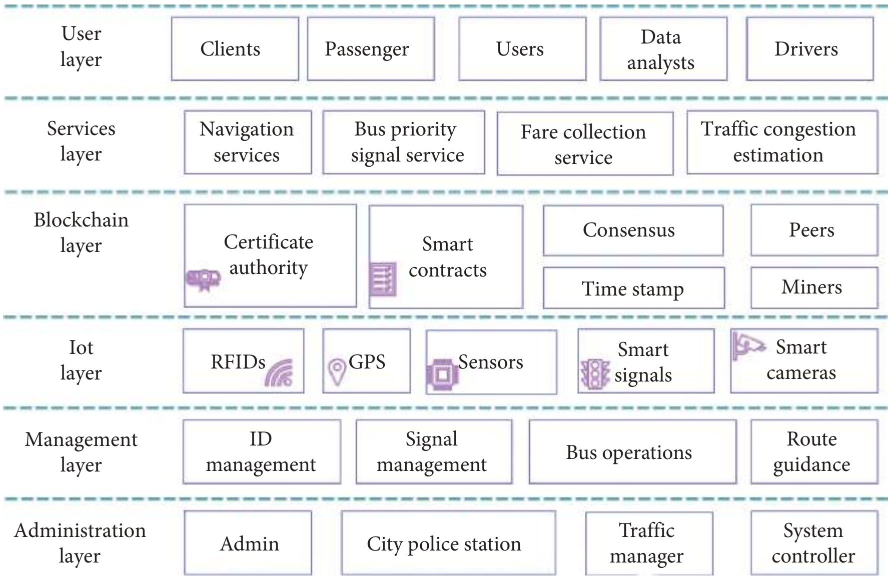
3.2. Architecture of the Proposed System. The proposed system covers different departments and different functions required to manage the smart transportation system properly. Figure 1 depicts the six-level architecture of the proposed system. The basic level is the administrative level that manages the entire system. It consists of management applications such as unique identity management, signal management, bus operation, and route guidance. The next step is the IoT layer. This layer is responsible for data collection using radiofrequency identification (RFID), a global positioning system (GPS), sensors, smart signals, and smart cameras. The central layer is the blockchain layer, which contains certification authorities, smart contracts, and other blockchain elements. This layer plays a vital role in data security. Another level is the service level. This tier provides various services such as navigation, bus priority signals, toll collection, and traffic congestion estimation. The final step is the level of users who use this system as smart city citizens.

The proposed system integrates the IoT environment and blockchain to provide different services to the end-users or participants. Figure 2 describes the overall structure of the proposed system and describes the blockchain and IoT convergence for intelligent transport networks in smart cities. The basic structure of the proposed system gives an abstract level view of the different components. It provides the road map to connect different IoT devices with blockchain. It also highlights the services that can be added to the proposed system. This system facilitates users by using the blockchain to provide various services and ensure user data security. Participants in the system are various users such as customers, passengers, drivers, data analysts, traffic managers, and city police stations. These participants have a graphical user interface (GUI) for communicating with the blockchain. The blockchain communicates with the GUI through REST API commands. For this, we have proposed using a private blockchain. IBM has provided an open-source private blockchain platform called Hyperledger Fabric [47]. Hyperledger Fabric provides ledger services to users and administrators of applications.

In most cases, multiple organizations come together into one consortium to form a network. Their consent is determined by the consortium's set of policies when the network is actually created. In smart transportation systems, there are different stakeholders. Hyperledger Fabric provides a common platform for suborganization to work independently within the transportation system. We create channels for each organization to ensure privacy and transparency. This platform provides all the features of a private blockchain and allows users to track timestamped transactions. IoT devices interact with the blockchain and store data. These devices or actuators can also operate according to the instructions received from the smart contract. ITSs provide various services to users, so an efficient transaction management system is required. It provides various services such as navigation, bus priority signals, toll collection, traffic congestion estimation, and gas station location.

4. Implementation

Blockchain technology has appeared as the latest solution to various problems, for example, counterfeiting in the supply chain process, finance security, ITS data security, and



User layer	Clients	Passenger	Users	Data analysts	Drivers
Services layer	Navigation services	Bus priority signal service	Fare collection service	Traffic congestion estimation	
Blockchain layer	Certificate authority	Smart contracts	Consensus Time stamp	Peers Miners	
Iot layer	RFIDs	GPS	Sensors	Smart signals	Smart cameras
Management layer	ID management	Signal management	Bus operations	Route guidance	
Administration layer	Admin	City police station	Traffic manager	System controller	

Figure 1: Layer-based architecture of the proposed solution.

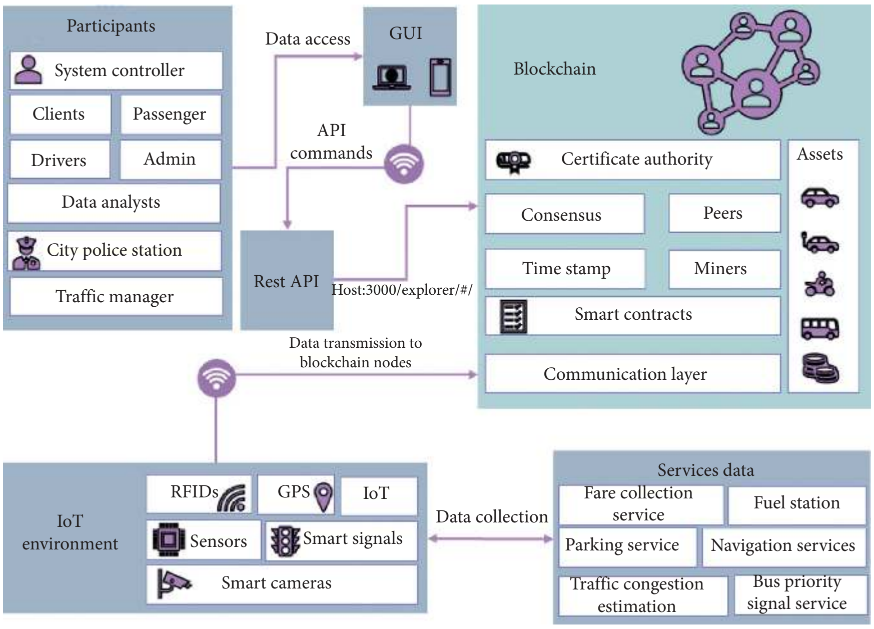


Figure 2: Structure of the proposed solution.

transparency while exchanging IoT data. Blockchain was initially introduced in Bitcoin [48]. It is a type of decentralized digital currency that can be exchanged between the users on the P2P (peer-to-peer) Bitcoin network over the Internet without third-party involvement such as banks. IoT is the key to enabling any primary Internet connection to control devices switching between the real world and the virtual world [49]. The IoT also helps connect devices and sensors, and connecting IoT to blockchain proves to be a time- and money-saving approach. This duo is proving helpful in building trust and transparency for the end-users [50].

We have configured the Hyperledger Fabric to maintain the transaction history or records performed by our private blockchain system participants through the GUI of the client application. Participants will be provided with a GUI that allows them to execute transactions on the blockchain network. These transactions execute the issuance of traffic tickets, ticket settlement, new participants' addition, deletion of participants, display of traffic information, and confirmation of accident information. System administrators can update, remove, and add system components depending upon the assigned rules defined in the smart contracts.

Hyperledger Fabric is configured to allow the participants to check the transaction details.

4.1. Secure Transaction Mechanism. Hyperledger Fabric-based private blockchain platform allows users to create channels, manage assets, and view transaction history. Figure 3 shows a flowchart of transaction execution in Hyperledger Fabric. Transactions within blockchain must be securely routed between different peers of the blockchain. Transactions between certification authority, endorser, orderer, nonendorser, and devices are explained using a flow diagram. Each device that initiates a transaction obtains a certificate of registration from Fabric's certification authority (CA). After registration, it can send a request to get an enrollment certificate. The Fabric CA issues a digital certificate to the device. The device then sends a request to create a channel for the subscriber. Approver and nonapproval peers also joined these channels after they were created. The client initiates the chain code on the peer. The approver peer checks the transaction and sends the response to the client. If this is a valid transaction, it will be forwarded to the subscriber. The orderer then delivers a block of order transactions and notifies the peer.

There are several transactions within the blockchain to perform various operations, such as updating the system's state of IoT devices. The IoT device's state can be updated using Algorithm 1. The user needs a deviceID to get the data of a specific device. The algorithm starts with initializing different variables required to perform the operation. Here, t-list represents the list of available devices. This algorithm will check that the transaction state for a specific sensor is new or not; if the new state is true, it will update the state of IoT device; otherwise, it will generate the message that the state is previous and has not been changed.

4.2. Multichannel Configuration. The Hyperledger Fabric guarantees confidentiality, privacy, and high abstraction. The Fabric allows creating private subsections for communication between two or more specific network members called channel networks.

Channels are used to conduct private and confidential transactions. Figure 4 shows a diagram of two channels. One of the major reasons to choose Hyperledger blockchain for a smart city is its functionality to interact within the consortium. It provides the support to connect multiple channels while considering privacy and transparency. The second channel is a subchannel of the first channel; the second channel members can communicate privately. A channel consists of organizations, peers, the ledger, chain code applications, and the certificate authority. Each transaction on the network is executed on a channel, reaches an agreement, and forwards the transaction to all participants. Network operations are performed on the channel. Each party must be authorized and authorized to operate on this channel. This channel contains unique identifiers provided by the member service provider (MSP). The MSP authenticates associates, subchannels, and services [51].

4.3. Endpoint Security. A communication endpoint is a type of communication node whose interface is vulnerable to connectivity or network partners. Endpoint security includes protection of endpoints or end-user nodes. The endpoint acts as an access point to the blockchain network. Malicious parties can use these points for malicious activities. Therefore, in a secure smart city transportation system, endpoint assurance is critical. Devices will be registered by the admin using Fabric CA. Admin will ensure that keys are assigned only to the trusted devices assigned. Hyperledger Fabric CA is the CA for the registration of clients. It offers features like ID registration, issuance, registration, renewal, and cancellation of certificates.

Figure 5 illustrates the certification mechanism for security separation. Clients or customers apply to the CA to issue an electronic certificate. A CA contains a root server, a proxy server, and a certificate database [52]. It checks that the client is not on the revocation list. Then, a signed certificate is issued to the client. It also issues public and private keys. Fabric CA is the ID issuing authority; users can trust certification authority because even CA cannot tamper with their data once recorded in the blockchain. The CA is important for the endpoint security of the whole system.

5. Results

This results section provides substantive simulation outcomes to evaluate the proposed smart transportation system's performance based on the blockchain and IoT platform's convergence. To present a thorough approach, we conducted several experimental tests using various performance metrics. We analyzed the performance based on resource usage analysis, transaction response time for multiple user requests, and latency rate while querying transactions. For evaluation purposes, we have used Postman, a tool that analyzes RESTful APIs, and Hyperledger Caliper.

While querying transactions, the latency rate includes the time the transaction request was sent and the time required to get approval from the web client.

5.1. Simulation Environment. Our test-bed is deployed in two separate development environments: blockchain network and web application. The online version of the Hyperledger Composer is deprecated; hence, we have installed the offline version Hyperledger Composer playground for simulation purposes. The installation process includes the prerequisites, preparation of the development environment, starting fabric composer, and user interface of the composer playground.

For developing an interactive web application, we have used the bootstrap framework, JavaScript, and JQUERY. On the other hand, for developing a private blockchain network, we have used Hyperledger Fabric that is an open-source solution provided by the Linux Foundation for building blockchain-based applications. The Ubuntu 18.04 LTS is an operating system for the development of a private blockchain network. Docker-engine and Docker-composer are

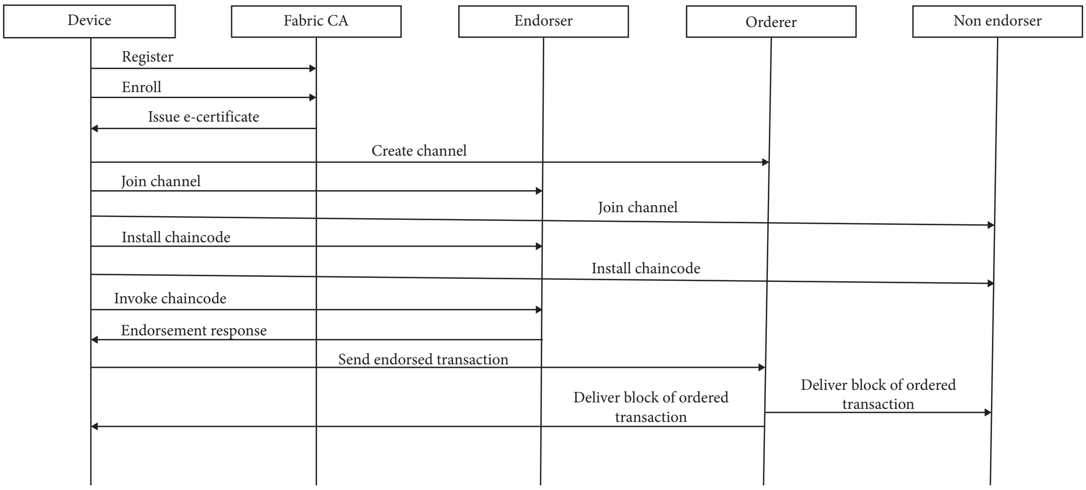


Figure 3: Flow diagram of the transaction between peers of blockchain.

```
Ensure: Initialize var deviceRegistry
Ensure: Initialize var deviceID
Ensure: Initialize var t-list
Ensure: Initialize var station = getstation ()
if tx.newstate = True then
        deviceID.state = tx.newstate
        if tx.enables ! = null then
          deviceID.enabled = tx.enabled }\newline
          dev-station = station }\newline
          t-list = deviceID }\newline
        elseif tx.newstate = False
          event.msg ("State of IoT dvice having ID "+ deviceID +" has not changed")
     end if
  end if
return asset.update (deviceID)
return event.msg ("State of IoT dvice having ID "+ deviceID +" has been changed.") = 0
```

Algorithm 1:Pseudocode for IoT device state transaction.

used for providing the running environment and integrated development environment (IDE), respectively. They both are used to configure the containers and docker images in the VMs. The Hyperledger Fabric used the Node JavaScript platform to develop a software development kit (SDK). Besides, REST APIs are used for the communication of client web applications with the private blockchain network.

For developing and managing the smart contract, we have used the composer command-line interface (CLI). Hyperledger Composer is a set of collaborative tools for building private blockchain networks that make it easy and quick for developers to create smart contracts and blockchain applications to solve business problems [47]. Further, couch DB is a database repository that can store the current states of the distributed ledger.

Figure 6 presents the transaction history or records performed by our private blockchain system's participants through the GUI of the client application. The participants are provided with GUI where they can perform the transactions in the blockchain network; these transactions should issue traffic tickets, transfer ticket or ticket payment, add new participants, delete participants, check traffic information, and check accident information. The system's admin can update, delete, and add any system participants if they violate the private blockchain network's rules. This transaction history portal has attributes such as date-time of the transaction, transaction type, and participants involved in performing this transaction. The users can only see the transaction detail by clicking on the view transaction detail button, but no participant can alter or delete the transaction in this blockchain network.

5.2. Resource Utilization Analysis. We have used an open-source Hyperledger Caliper to analyze and test the resource utilization of our private blockchain system [53]. Table 2 presents the average and maximum CPU, RAM resource utilization results generated by the Hyperledger Caliper.

In the peer node case, the maximum CPU and memory were recorded to 13.3% and 115 MB, respectively. The

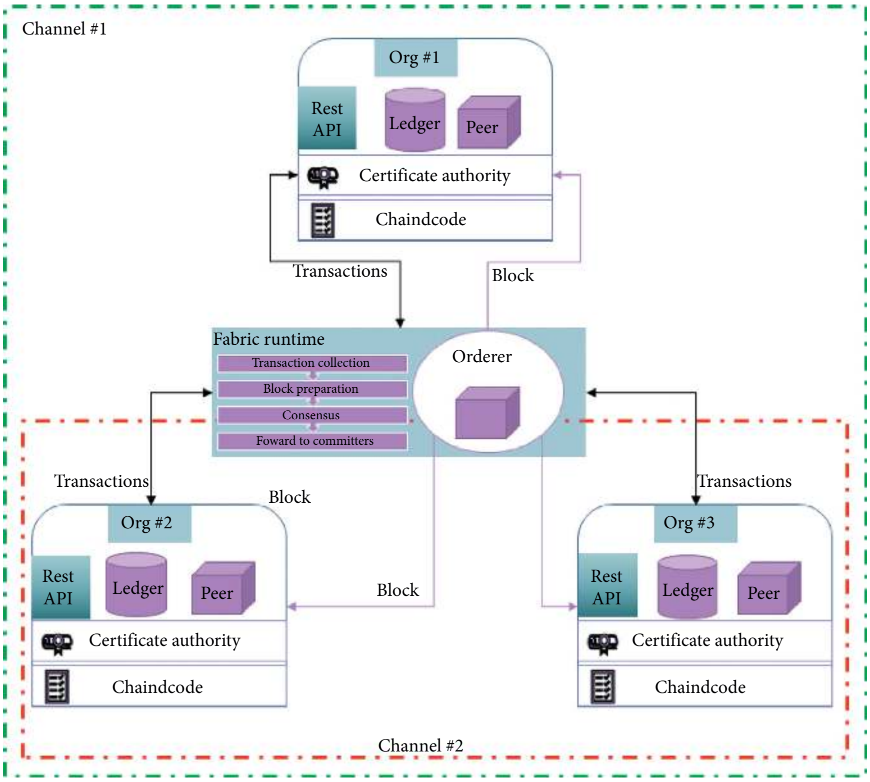


Figure 4: Multichannel network within a private blockchain.

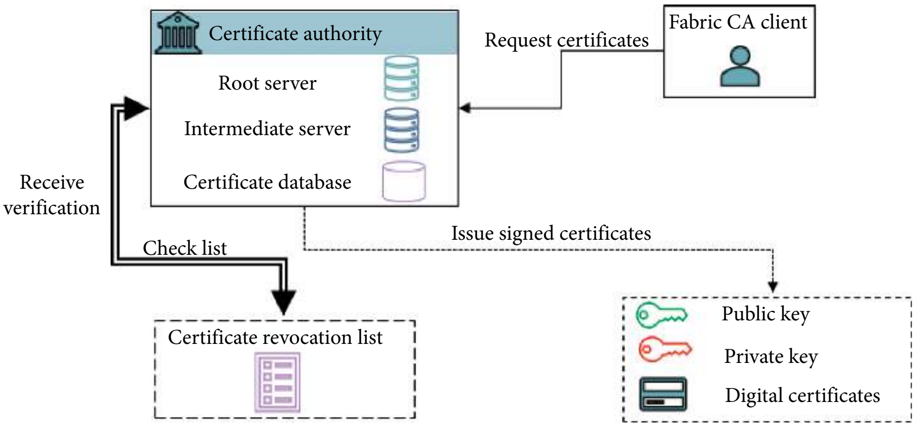
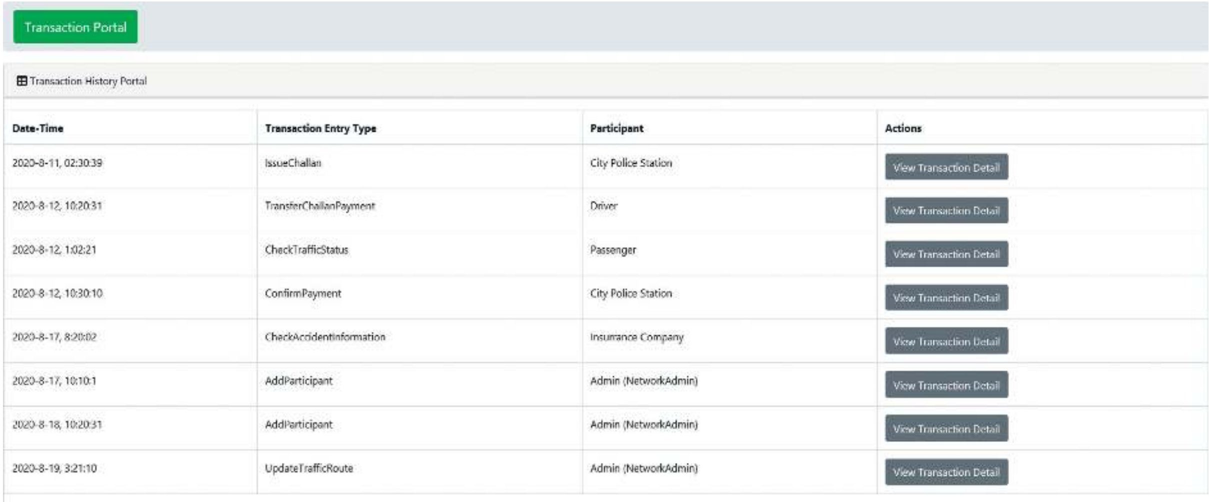


Figure 5: Certificate authority for endpoint security.

average memory of 78 MB and an average CPU of 7.8% was recorded. In a system proposed by Jamil et al. [54], the average memory of peer node was recorded at 98.5 MB and a maximum of 106.6 MB. Moreover, in the case of the orderer node, the average memory and CPU usage have been recorded to 30 MB and 2\%, respectively. In work by Jamil et al. [54], the average memory and CPU usage were recorded at 88.7 MB and 6.75%, respectively. In the CA node case, the memory and CPU utilization were 6 MB and 0.25%, respectively. The resource utilization experimental results show that our private blockchain system has used low resources, better user experience, and reliability.

To test our blockchain network's response time, three user groups with 200 users, 400 users, and 600 users have been used with a simulation period of 140 ms. As shown in Figure 7, the blockchain network's response time continuously increases with the growing number of user's requests. More users querying at the same time to the blockchain network cause an increase in the response time. We have evaluated our system's performance with 200 users in the first phase, 400 users in the second phase, and 600 users at the last phase. The response time is almost the same for the first two user groups, but when we increased the users to 600, the response rate slightly increased to 30 ms. Overall, the



Date-Time	Transaction Entry Type	Participant	Actions
2020-8-11, 02:30:39	IssueChallan	City Police Station	View Transaction Detail
2020-8-12, 10:20:31	TransferChallanPayment	Driver	View Transaction Detail
2020-8-12, 1:02:21	CheckTrafficStatus	Passenger	View Transaction Detail
2020-8-12, 10:30:10	ConfirmPayment	City Police Station	View Transaction Detail
2020-8-17, 8:20:02	CheckAccidentInformation	Insurance Company	View Transaction Detail
2020-8-17, 10:10:1	AddParticipant	Admin (NetworkAdmin)	View Transaction Detail
2020-8-18, 10:20:31	AddParticipant	Admin (NetworkAdmin)	View Transaction Detail
2020-8-19, 3:21:10	UpdateTrafficRoute	Admin (NetworkAdmin)	View Transaction Detail

Figure 6: Transaction history portal.

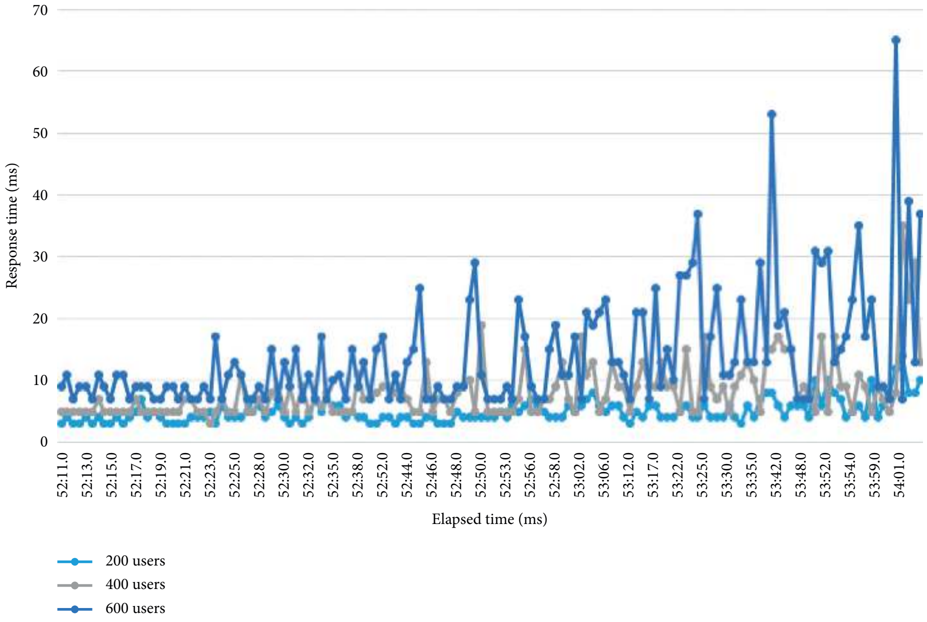


Figure 7: Transaction response time for multiple user requests.

proposed blockchain network's performance remains stable and satisfactory even we have increased the number of users to 600.

Figure 8 illustrates the maximum, average, and minimum latency of the blockchain network while running the query transactions. We have used Equation 1 to calculate latency, where T_{con} represents the confirmation time, N_t is network threshold is represented by N_{trh}, and submission time is represented by T_{sub}. Transaction latency L_{tra} can be obtained by multiplying the network threshold with confirmation time and subtracting the submission time.

$$L_{\text{tra}} = T_{\text{con}} N_{\text{trh}} - T_{\text{sub}}. \tag{1}$$

Similar to Figure 7, three different user groups with 200, 400, and 600 users are used for testing the latency of the

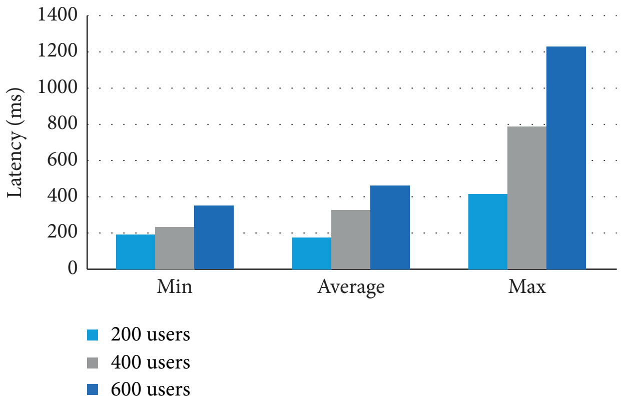


Figure 8: Latency rate while querying transactions.

Table 2: Blockchain network resource usage analysis.

Name	Memory (Max) (MB)	Memory (Avg) (MB)	CPU (Max) (%)	CPU (Avg) (%)	Traffic-in (MB)	Traffic-out (MB)
Peer0	78.2	67	9	4.3	5.2	4.9
Peer1	73.1	66	8.3	3.45	6	5.2
Peer2	115	78	13.3	7.8	7.2	10.9
CA0	8	6	1.56	0.25	510	0.12
CA1	9	6.34	1.58	0.35	570	0.2
Orderer1	40.4	30	10.2	2	6.3	11.2
Orderer2	48.5	36.2	13.34	4.5	5.12	9.43

proposed system. The average latency for the first user group, with 200 users, is 220 ms. The average latency for the second user group is 330 ms, and for the third user group with 600 users, average latency is 460 ms.

6. Conclusions

Smart cities provide citizens with smart and sophisticated services that can improve their quality of life. However, it should be noted that the collection, storage, processing, and analysis of heterogeneous data typically collected from residents face vulnerability issues. In Industry 4.0, advances in the IoT, cloud computing, social media, and other influencers place technology within a smart society's framework, creating potential loopholes for smart city data, services, and applications. This vulnerability creates a data security issue. To solve this problem, we propose a decentralized data management system that allows users to use the blockchain and the IoT to manage their data in a smart and sustainable environment. Integrating blockchain technology and the IoT into their transportation systems will undoubtedly have many benefits. These benefits cover a wide range of data sharing and tracking to smart city residents' transparency and privacy. This article describes a new procedure for designing and implementing a decentralized platform for combining IoT and blockchain technology with smart transportation systems. It aims at file creation. It is a safe, transparent, and reliable transportation system for officials, police departments, traffic managers, and drivers in smart cities using this service. Designed for enterprise use, Hyperledger Fabric was used to conduct case studies of blockchain-based smart city transportation systems as a proof of concept. Various performance indicators can be used in the test to show a certain level and achieve significant transaction productivity and low resource utilization. A comparative analysis of systems designed in the current method underscores the importance of this task. As a result, the designed system performed better than other systems in other respects. This system will address residents' and authorities' security challenges in smart and sustainable cities and lead to better governance and better policies. The future study guide for this article is based on covering more complex business networks with more vehicle sensors.

Data Availability

Any data will be available upon request to the corresponding author.

Conflicts of Interest

The authors declare that they have no conflicts of interest regarding the present study.

Acknowledgments

This work was supported by the RUDN University Strategic Academic Leadership Program and by the Chancellor Research Initiative (CRI) grant awarded to Texas A&M University-San Antonio, TX, USA.

References

[1] C. Ingrao, A. Messineo, R. Beltramo, T. Yigitcanlar, and G. Ioppolo, "How can life cycle thinking support sustainability of buildings? Investigating life cycle assessment applications for energy efficiency and environmental performance," *Journal of Cleaner Production*, vol. 201, pp. 556–569, 2018.

[2] ¸S. Kolozali, M. Bermudez-Edo, N. FarajiDavar et al., "Observing the pulse of a city: a smart city framework for real-time discovery federation and aggregation of data streams," *IEEE Internet of Things Journal*, vol. 6, pp. 2651–2668, 2018.

[3] A. Tewari and B. B. Gupta, "Security, privacy and trust of different layers in Internet-of-Things (IoTs) framework," *Future Generation Computer Systems*, vol. 108, pp. 909–920, 2020.

[4] B. Gupta and M. Quamara, "An overview of Internet of Things (IoT): architectural aspects challenges and protocols," *Concurrency and Computation: Practice and Experience*, vol. 32, Article ID e4946, 2020.

[5] A. A. Abd El-Latif, B. Abd-El-Atty, I. Mehmood, K. Muhammad, S. E. Venegas-Andraca, and J. Peng, "Quantum-inspired blockchain-based cybersecurity: securing smart edge utilities in IoT-based smart cities," *Information Processing & Management*, vol. 58, no. 4, p. 102549, 2021.

[6] A. Sunyaev, "Cloud computing," *Internet Computing*, pp. 195–236, 2020.

[7] I. Elgendy, W. Zhang, C. Liu, and C. H. Hsu, "An efficient and secured framework for mobile cloud computing," *IEEE Transactions on Cloud Computing*, vol. 9, 2018.

[8] P. W. Khan and Y.-C. Byun, "Smart contract centric inference engine for intelligent electric vehicle transportation system," *Sensors*, vol. 20, no. 15, p. 4252, 2020.

[9] H. Wang, Z. Li, Y. Li, B. B. Gupta, and C. Choi, "Visual saliency guided complex image retrieval," *Pattern Recognition Letters*, vol. 130, pp. 64–72, 2020.

[10] L. Butler, T. Yigitcanlar, and A. Paz, "How can smart mobility innovations alleviate transportation disadvantage? Assembling a conceptual framework through a systematic review," *Applied Sciences*, vol. 10, no. 18, p. 6306, 2020.

[11] M. Fazekas and B. Tóth, "The extent and cost of corruption in transport infrastructure. New evidence from Europe," *Transportation Research Part A: Policy and Practice*, vol. 113, pp. 35–54, 2018.

[12] N. Sieber, *Fighting Corruption into the Road Transport Sector: Lessons for Developing Countries*, Federal Ministry for Economic Cooperation and Development, Berlin, Germany, 2012.

[13] E. Economic and S. Committee, "The ethics of big data: balancing economic benefits and ethical questions of big data in the EU policy context," 2017.

[14] F. Jürg, S. Sudhir, B. Stefan et al., "Reference document on transparency in the transport sector," 2018.

[15] G. Saldamli and A. Razavi, "Swarm robotics meets blockchain to deploy surveillance missions," in *Proceedings of the 2020 32nd International Conference on Microelectronics (ICM)*, pp. 1–6, Aqaba, Jordan, August 2020.

[16] E. M. Abou-Nassar, A. M. Iliyasu, P. M. El-Kafrawy, O.-Y. Song, A. K. Bashir, and A. A. A. El-Latif, "DITrust chain: towards blockchain-based trust models for sustainable healthcare IoT systems," *IEEE Access*, vol. 8, pp. 111223–111238, 2020.

[17] G. Xu, Y. Liu, and P. W. Khan, "Improvement of the DPoS consensus mechanism in Blockchain based on vague sets," *IEEE Transactions on Industrial Informatics*, vol. 16, pp. 4252–4259, 2019.

[18] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pp. 3–16, Vienna, Austria, October 2016.

[19] P. W. Khan and Y.-C. Byun, "Secure transactions management using blockchain as a service software for the internet of Things," *Software Engineering in IoT, Big Data, Cloud and Mobile Computing*, pp. 117–128, 2021.

[20] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C. P. A. Ogah, and Z. Sun, "Blockchain-based dynamic key management for heterogeneous intelligent transportation systems," *IEEE Internet of Things Journal*, vol. 4, no. 6, pp. 1832–1843, 2017.

[21] M. A. Alsmirat, F. Al-Alem, M. Al-Ayyoub, Y. Jararweh, and B. Gupta, "Impact of digital fingerprint image quality on the fingerprint recognition accuracy fingerprint image quality on the fingerprint recognition accuracy," *Multimedia Tools and Applications*, vol. 78, no. 3, pp. 3649–3688, 2019.

[22] C. Yu, J. Li, X. Li, X. Ren, and B. B. Gupta, "Four-image encryption scheme based on quaternion Fresnel transform, chaos and computer generated hologram," *Multimedia Tools and Applications*, vol. 77, no. 4, pp. 4585–4608, 2018.

[23] A. A. Ganin, A. C. Mersky, A. S. Jin, M. Kitsak, J. M. Keisler, and I. Linkov, "Resilience in intelligent transportation systems (ITS)," *Transportation Research Part C: Emerging Technologies*, vol. 100, pp. 318–329, 2019.

[24] W. Z. Zhang, I. A. Elgendy, M. Hammad et al., "Secure and optimized load balancing for multi-tier IoT and edge-cloud computing systems," *IEEE Internet of Things Journal*, 2020.

[25] I. A. Elgendy, W.-Z. Zhang, Y. Zeng, H. He, Y.-C. Tian, and Y. Yang, "Efficient and secure multi-user multi-task computation offloading for mobile-edge computing in mobile IoT networksficient and secure multi-user multi-task computation offloading for mobile-edge computing in mobile IoT networks," *IEEE Transactions on Network and Service Management*, vol. 17, no. 4, pp. 2410–2422, 2020.

[26] S. Nakamoto, "Bitcoin: a peer-to-peer electronic cash system," Technical report, 2019.

[27] C. Esposito, M. Ficco, and B. B. Gupta, "Blockchain-based authentication and authorization for smart city applications," *Information Processing & Management*, vol. 58, no. 2, p. 102468, 2021.

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

[29] X. Zhang and D. Wang, "Adaptive traffic signal control mechanism for intelligent transportation based on a consortium blockchainfic signal control mechanism for intelligent transportation based on a consortium blockchain," *IEEE Access*, vol. 7, pp. 97281–97295, 2019.

[30] P. Zeng, X. Wang, H. Li, F. Jiang, and R. Doss, "A scheme of intelligent traffic light system based on distributed security architecture of blockchain technologyfic light system based on distributed security architecture of blockchain technology," *IEEE Access*, vol. 8, pp. 33644–33657, 2020.

[31] D. Wang and X. Zhang, "Secure data sharing and customized services for intelligent transportation based on a consortium blockchain," *IEEE Access*, vol. 8, pp. 56045–56059, 2020.

[32] S. Ahmed, M. S. Rahman, M. S. Rahaman, and others, "A blockchain-based architecture for integrated smart parking systems," in *Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pp. 177–182, Kyoto, Japan, March 2019.

[33] M. M. Badr, W. A. Amiri, M. M. Fouda, M. M. E. A. Mahmoud, A. J. Aljohani, and W. Alasmary, "Smart parking system with privacy preservation and reputation management using blockchain," *IEEE Access*, vol. 8, pp. 150823–150843, 2020.

[34] S. R. Maskey, S. Badsha, S. Sengupta, and I. Khalil, "Bits: blockchain based intelligent transportation system with outlier detection for smart city," in *Proceedings of the IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops)*, pp. 1–6, Austin, TX, USA, March 2020.

[35] Y. Li, K. Ouyang, N. Li, R. Rahmani, H. Yang, and Y. Pei, "A blockchain-assisted intelligent transportation system promoting data services with privacy protection," *Sensors*, vol. 20, no. 9, p. 2483, 2020.

[36] L. A. Hîr¸tan, C. Dobre, and H. González-Vélez, "Blockchain-based reputation for intelligent transportation systems," *Sensors*, vol. 20, p. 791, 2020.

[37] J. Huang, L. Kong, G. Chen, M.-Y. Wu, X. Liu, and P. Zeng, "Towards secure industrial IoT: blockchain system with credit-based consensus mechanism," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3680–3689, 2019.

[38] J. Huang, L. Kong, H.-N. Dai et al., "Blockchain-based mobile crowd sensing in industrial systems," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 10, pp. 6553–6563, 2020.

[39] D. López and B. Farooq, "A multi-layered blockchain framework for smart mobility data-markets," *Transportation Research Part C: Emerging Technologies*, vol. 111, pp. 588–615, 2020.

[40] D. López and B. Farooq, "A blockchain framework for smart mobility," in *Proceedings of the IEEE International Smart Cities Conference (ISC2)*, pp. 1–7, Kansas, MO, USA, September 2018.

[41] B. Rojas, C. Bolaños, R. Salazar-Cabrera, G. Ramírez-González, Á. Pachón de la Cruz, and J. M. Madrid Molina, "Fleet management and control system for medium-sized cities based in intelligent transportation systems: from review to proposal in a city," *Electronics*, vol. 9, no. 9, p. 1383, 2020.

[42] A. Balasubramaniam, M. J. J. Gul, V. G. Menon, and A. Paul, "Blockchain for intelligent transport system," *IETE Technical Review*, pp. 1–12, 2020.

[43] F. Zhu, Y. Lv, Y. Chen, X. Wang, G. Xiong, and F. Y. Wang, "Parallel transportation systems: toward IoT-enabled smart urban traffic control and management," *IEEE Transactions on Intelligent Transportation Systems*, vol. 21, 2019.

[44] S. Nesmachnow and L. Hernández-Callejo, "CITIES: Ibero-American Research Network for sustainable efficient and integrated," *Smart Cities*, vol. 3, no. 3, pp. 758–766, 2020.

[45] P. Khan, Y.-C. Byun, and N. Park, "A data verification system for CCTV surveillance cameras using blockchain technology in smart citiesfication system for CCTV surveillance cameras using blockchain technology in smart cities," *Electronics*, vol. 9, no. 3, p. 484, 2020.

[46] W. Villegas-Ch, X. Palacios-Pacheco, and S. Luján-Mora, "Application of a smart city model to a traditional university campus with a big data architecture: a sustainable smart campus," *Sustainability*, vol. 11, no. 10, p. 2857, 2019.

[47] IBM, *Hyperledger Composer*, IBM, Armonk, NY, USA, 2020, https://www.hyperledger.org/use/composer.

[48] S. Nakamoto and A. Bitcoin, "A peer-to-peer electronic cash system," *Bitcoin*, https://www.klausnordby.com/bitcoin/Bitcoin_Whitepaper_Document_HD.pdf.

[49] L. a. Tawalbeh, F. Muheidat, M. Tawalbeh, and M. Quwaider, "IoT privacy and security: challenges and solutions," *Applied Sciences*, vol. 10, no. 12, p. 4102, 2020.

[50] L. Hang and D.-H. Kim, "Reliable task management based on a smart contract for runtime verification of sensing and actuating tasks in IoT environmentsfication of sensing and actuating tasks in IoT environments," *Sensors*, vol. 20, no. 4, p. 1207, 2020.

[51] P. W. Khan and Y. Byun, "A blockchain-based secure image encryption scheme for the industrial internet of Things," *Entropy*, vol. 22, no. 2, p. 175, 2020.

[52] L. Hang and D.-H. Kim, "Design and implementation of an integrated iot blockchain platform for sensing data integrity," *Sensors*, vol. 19, no. 10, p. 2228, 2019.

[53] IBM, *Hyperledger Caliper*, IBM, Armonk, NY, USA, 2020, https://www.hyperledger.org/projects/caliper.

[54] F. Jamil, S. Ahmad, N. Iqbal, and D.-H. Kim, "Towards a remote monitoring of patient vital signs based on IoT-based blockchain integrity management platforms in smart hospitals," *Sensors*, vol. 20, no. 8, p. 2195, 2020.