

Blockchain-Based Internet of Vehicles: Distributed Network Architecture and Performance Analysis

Tigang Jiang, Hua Fang, and Honggang Wang^{ID}

Abstract—The rapid growth of Internet of Vehicles (IoV) has brought huge challenges for large data storage, intelligent management, and information security for the entire system. The traditional centralized management approach for IoV faces the difficulty in dealing with real-time response. The blockchain, as an effective technology for decentralized distributed storage and security management, has already showed great advantages in its application of Bitcoin. In this paper, we investigate how the blockchain technology could be extended to the application of vehicle networking, especially with the consideration of the distributed and secure storage of big data. We define several types of nodes such as vehicle and roadside for vehicle networks and form several sub-blockchain networks. In this paper, we present a model of the outward transmission of vehicle blockchain data, and then give detail theoretical analysis and numerical results. This paper has shown the potential to guide the application of blockchain for future vehicle networking.

Index Terms—Blockchain, Internet of Things (IoT), Internet of Vehicles (IoV).

I. INTRODUCTION

WITH the development of Internet of Vehicles (IoV) technology, a large number of IoV nodes need to access this huge network, and the amount of traffic to be handled is extremely large. At the same time, with the increasing of traffic load on centralized systems, the traditional centralized management and data storage will face significant challenges. Even without the consideration of the economic cost and complex engineering processes, the central server could be the bottleneck of the entire system. Once the server fails, it may break the whole system. It is difficult for different providers to guarantee interoperability and compatibility among nodes belonging to different providers.

When the IoV is combined with artificial intelligence, it can bring infinite possibilities to the world. When billions of smart devices need to interact with each other, the traditional centralized model will encounter huge challenges in terms of computations. Therefore, decentralization, distributed

management, and distributed storage could be the future technology trend of the next generation of Internet of Things (IoT). However, when decentralized technology is adopted, data and communication must have high security requirements.

Blockchain technology seems to be a powerful tool for solving trusted interactions in a decentralized approach. It is a digital cryptocurrency system represented by Bitcoin core support technology, which was invented in 2008 and published by the cryptography mailing group [1]. Its core strength is decentralization, and it can achieve point-to-point transactions, coordination, and collaboration based on decentralized credits in distributed systems where nodes do not need to trust each other. It adopts multiple means such as data encryption, time stamping, distributed consensus, and economic incentives. The blockchain is to solve the problems of high costs, inefficiency, and insecure data storage that are common in centralized organizations. With the rapid development and popularity of Bitcoin in recent years, blockchain technology research has been motivated to grow quickly, which is viewed as the fifth disruptive innovation of the computing paradigm after the Internet. The blockchain technology is the fourth milestone after the central bank's banknote credit [2].

Blockchains have been successfully applied to user cases below.

- 1) *Smart Contracts*: The applications in [3] is a blockchain example for implementing smart contracts. The application relies on blockchain for distributed computing and sharing software.
- 2) *Blockchain-Based Public Key Infrastructure (PKI)*: Fromknecht *et al.* [8] introduced a coin called Certcoin. It is a distributed PKI, which benefits from the consistency assurance provided by Bitcoin and Namecoin and ensures identity retention.
- 3) *Decentralized Storage*: The example of [4] is a peer-to-peer cloud storage network, and the network uses a so-called MetaDisk [5], which is a blockchain for decentralized metadata storage.
- 4) *Anti-Counterfeiting Solutions*: Blockverify provides blockchain-based anti-counterfeiting solutions that introduce transparency into the supply chain [6]. It can be used in the pharmaceutical, luxury goods, and electronics industries.
- 5) *Blockchain-Based Domain Name Server*: The distribution of secure and dispersed namespaces have been realized due to the blockchain infrastructure, which allows to define a domain system that resists censorship, such as [7].

Manuscript received June 4, 2018; revised September 7, 2018; accepted September 14, 2018. Date of publication October 5, 2018; date of current version June 19, 2019. This work was supported in part by the National Natural Science Foundation of China under Grant 61271170. (Corresponding author: Honggang Wang.)

T. Jiang is with the School of Information and Communication Engineering, University of Electronic Science and Technology of China, Chengdu 611731, China (e-mail: jtg@uestc.edu.cn).

H. Fang and H. Wang are with the College of Engineering, University of Massachusetts Dartmouth, Dartmouth, MA 02747 USA (e-mail: hfang2@umassd.edu; hwang1@umassd.edu).

Digital Object Identifier 10.1109/JIOT.2018.2874398

- 6) *Decentralized IoT*: Filament is a start-up company that offers a decentralized IoT software stack [6] that uses the Bitcoin blockchain to make devices unique in the public ledger.

Blockchain technology is the embryonic form of next-generation cloud computing, and it is expected to completely reshape human social activities, and achieve the transformation of Internet. Generalized blockchain technology could have many benefits, for example, using encrypted chain block structure to verify and store data, using distributed node consensus algorithm to generate and update data, and using automated script code (smart contract) to program and manipulate data. It presents a new decentralized infrastructure and distributed computing paradigm.

Therefore, the integration of blockchain technology and the IoT can greatly improve the security, intelligence, big data storage, and efficient management of the IoT, which is a promising research topic. Especially for IoV, because the communication link between vehicle to vehicle or vehicle to roadside unit (RSU) is unstable or may not be secure, how to design the blockchain-based vehicle network and model the access part of the vehicle network is an urgent problem to be solved.

In this paper, the integration of IoV and blockchain is presented in detail. Based on the characteristics of IoV, we proposed a blockchain architecture and network model. We also analyzed its data transmission performance.

The rest of this paper is structured as follows. Section II reviews the related literature. Section III discusses the design principles required for blockchains in IoV. Section IV presents the data classification, network architecture, and data flow for the proposed blockchain-based IoV. Section V presents our evaluation of the proposed model using multiple performance metrics. Finally, Section VI reaches our conclusions.

II. LITERATURE REVIEW

A. Blockchain for IoT

There are some research works focusing on the blockchain-based IoT architecture. Sharma *et al.* [9] proposed a distributed secure SDN architecture (DistBlockNet) using blockchain technology, which follows the principles required for security, scalable, and efficient network architecture, combining SDN with blockchain technologies to be verifiable. The approach establishes a distributed peer-to-peer network in which non-compliant members can interact with each other without a trusted intermediary. Under this architecture, security can automatically adapt to threat conditions without human management. In addition, the performance of the architecture was compared and analyzed. Daza *et al.* [10] presented a method for discovering the IoT by using hierarchical and general multilayer blockchains. This method uses the existing service provider's own protocol as much as possible and utilizes the information obtained from each blockchain, then to detect the surroundings and discover the network.

Novo [11] proposed a architecture for arbitrating roles and permissions for the IoT. The architect is full distributed, and the IoT access control system based on blockchain technology is supported by conceptual implementation. In this method,

through the blockchain network, distributing management center nodes that can connect restricted networks in different ways provides the solution with a high degree of flexibility. In [12], a blockchain-based distributed cloud architecture was proposed, which includes a software defined network that enables controller nodes at the edge of the network to meet the required design principles. The objective of the solution is to provide low-cost, secure, on-demand access for IoT. Yeow *et al.* [13] proposed a comprehensive review of the IoT decentralized consensus system, which includes a number of consensus areas, such as the data structure, the extended consensus ledger, and the transaction model. This paper also analyzes the advantages and disadvantages of the decentralized consensus system, and introduces several open research problems about the decentralized consensus of the IoT with edge as the center.

In [14], the paper proposes a multilayer secure IoT model based on blockchain. This model divides the IoT into a multilevel decentralized network and uses blockchain technology at all levels of the network. It also provides a wide area network solution for the IoT. Conoscenti *et al.* [15] studied whether blockchain and peering methods can be used to promote decentralized and design-specific IoT. The analysis of 18 blockchain cases reveals that the integrity of the blockchain depends largely on workload, demonstrating the limitation of the adaptability.

Varshney and Gupta [16] used blockchain technology to design a framework for data security and management on the Internet, showing how intelligent devices communicate with blockchain backbones. In order to address IoT identity and security issues, the designed framework must be scalable.

In the blockchain IoT environment, when data or device authentication information is placed on a blockchain, personal information may be leaked through a job certification process or address search. Lee and Kim [17] applied zero-knowledge proofs in the smart meter system and studied how to enhance the anonymity of the blockchain for privacy protection. Jeon *et al.* [18] proposed an IoT server platform by introducing blockchains and storing sensor data in the blockchain.

Xie *et al.* [19] proposed to use a chained data structure to store blockchain transaction hash values and form a double-stranded storage with the blockchain to track blockchain-based agricultural products and ensure that agricultural product data is not maliciously tampered with or destroyed.

Vehicle operating status can be obtained through roadside systems, such as the RFID system on roads. It can provide a variety of functions, including lane level locations, roads traffic control information, vehicle distance estimation, real-time driving behavior analysis, etc., to improve transportation safety and efficiency. Cheng *et al.* [20] proposed several applications, including auxiliary navigation systems, electric traffic control, unmanned patrol systems, vehicle distance estimation, parking assistance systems, routes tracking and access control, and unmanned ground vehicles.

In [21], a hierarchical identity-based encryption mechanism with an emerging blockchain infrastructure is investigated. The authors proposed a blockchain-based data usage audit architecture to ensure availability and accountability in a manner that

protects privacy. This method relies on the auditable contracts deployed in the blockchain infrastructure. It can preserve the privacy of data owners, and can ensure the confidentiality of data which is shared with multiple service providers. It also can provide the audit department with anti-tamper evidence against data usage in-compliance.

B. Blockchain for IoV

In order to help vehicular networking achieve higher throughput, the device-to-device (D2D) technology can be used to allow the effective communication between vehicles, or between vehicles and roadside systems, to reduce communication delay and improve the safety. The classification criteria of D2D communication security issues has been investigated in [22]. The authors consider the integration of the physical layer, MAC layer, network layer, and application layer. Chakravorty and Chunming [23] presented blockchain-based solutions to social networking. They offer a user-centric blockchain supported social media network that enables users to control, trace, and claim ownership of every piece of content they share. Harnessing peer-to-peer capabilities of the blockchain technology allows a truly decentralized, secure, anonymous, and traceable content distribution network.

In [24], a decentralized trust management system based on blockchain technology for in-vehicle networks is proposed. Vehicles can use Bayesian inference models to verify messages from neighboring vehicles. In the method, the vehicle will generate a rating for each vehicle, and RSUs calculate the offset value of the trust of the relevant vehicle and group the data into blocks to improve traffic safety and efficiency in an unreliable vehicle communication environment.

Liu *et al.* [25] proposed a new type of electric vehicle (EV) charging scheme for decentralized blockchain smart grid system. The goal is to minimize the power fluctuation level in the grid network and the overall charging cost of EV users. Considering the EV battery capacity, charging rate, charging behavior of EV users, and power grid fluctuations, an adaptive blockchain-based EV participation program has been proposed.

In [26], a blockchain-based privacy protection payment mechanism is proposed for vehicle to grid networks to protect sensitive user information while enabling data sharing. The mechanism includes the registration and data maintenance processes based on blockchain technology and supports anonymity and audit. Huang *et al.* [27] studied the management safety between EVs and charging piles. A blockchain ecosystem decentralized safety model based on lightning networks and smart contracts was proposed to improve the transaction security of EVs and charging piles.

Kshetri [28] evaluated the role of the blockchain in enhancing the security of the IoT. They conclude that the fragmentation of the blockchain is likely to lead to low sensitivity of malicious participants.

Kotobi and Bilen [29] proposed a blockchain authentication protocol, which enables spectrum sharing in mobile cognitive radio (CR) networks. The spectrum sharing mechanism is used as a media access protocol to access wireless bandwidth in a

competing CR, and they also propose a virtual currency called Specoins, which is used to pay for the access spectrum.

These existing work explore the potential of applying blockchain technology for IoT although many challenges still exist. The current research on the blockchain for IoV lacks the performance analysis of the access network part, and also does not clearly define the blockchain structure of the IoV. In this paper, we are to address these challenges.

III. REQUIREMENTS FOR BLOCKCHAIN-BASED IOV

A. Blockchain Requirements for IoV

“Blockchain” has attracted much attention of researchers because they believe that the technology will bring tremendous opportunities and changes to industries. However, the study on the integration of IoV and blockchain technology are at the early stage for the industry. We summarize the demand for blockchain technology for IoV in the following.

- 1) *Big Data Storage*: Future IoV data will not only include road traffic data, but also may include various sensory data from the vehicle, sensory data outside the vehicle, driving habit data, and human-computer interaction data. It will also include e-commerce transaction data, such as car insurance transactions, refueling transactions, EV charging transactions, and even car-to-car experience sharing, travel photographs, and other transactions. With the consideration of the huge number of vehicles on the road, the data amount will be huge and both the centralized and distributed storage should be fully utilized.
- 2) *Complete Decentralization and True Redundancy*: Using blockchain technology, it is possible to build a distributed cloud data center that save data on several designated nodes in a specific area and can be intelligently distributed to distributed nodes.
- 3) *Facilitating the Use of Resources*: Blockchain technology can be used to simplify on-demand use of resources by simply running an on-demand resource algorithm through smart contracts to complete the requested service. It will play an important role for vehicles' transactions.
- 4) *Selective Privacy*: With blockchain technology, each user manages their own keys, and each data block node only stores encrypted pieces of user data. Therefore, full privacy can be achieved without any third-party access and control data. However, due to regulatory needs, the key to some of the data should be transparent to the regulatory body, such as the government's vehicle management office.
- 5) *Service Quality Improvement*: By using blockchain technology, we can provide traceability of resource usage so that customers and service providers can correctly verify service level agreements.
- 6) *Lower Costs*: Due to the combination of distributed and centralized storage technologies, blockchain storage cost will be greatly reduced, and the transaction costs will be greatly reduced due to the use of smart contracts in transactions.

B. IoV Design

In order to design a high-performance, secure, centralized, and distributed scalable IoV to meet the ultimate goal of new service requirements, the following design principles could be considered.

- 1) *Invulnerability*: Even if some nodes fail, the computing will continue on other nodes.
- 2) *Easy to Deploy*: Existing network infrastructure can still be used as much as possible with the flexibility of adding new nodes.
- 3) *Adaptability*: The network architecture should be able to adapt to changing environments and expand its use to meet growing customer needs.
- 4) *Scalability*: It requires the networks to add/remove devices and manage the explosion of massive data.
- 5) *Security*: Protecting the communications and data security of the vehicular network is an important goal of the IoV design.
- 6) *High Availability and Fault Tolerance*: The IoV should be easy to use and reliable.

IV. BLOCKCHAIN-BASED IOV: DESIGN AND ANALYSIS

A. Blockchain Data Classification

The data that need to be distributed through the blockchain, cannot be denied. According to different application purposes, they will be classified into a variety of different blockchains. Different blockchains should not communicate with each other. We classify the data into the following categories.

- 1) *D1*: Car driving data monitored by roadside systems, such as driving habits, speeding, etc.
- 2) *D2*: Sensory data of the vehicle's internal machinery, electronics, air pressure, temperature, etc.
- 3) *D3*: User private voice, video and other data, such as in-car recordings, videos, etc.
- 4) *D4*: Vehicle insurance related data.
- 5) *D5*: General e-commerce and transaction data for users, such as car refueling, charging, car washing, etc.

The data can also be defined as the following types.

- 1) *Vehicle Management Blockchain Data*: *D1* (mandatory) and *D3* (optional).
- 2) *Automobile Factory Blockchain Data*: *D2*, which provides information for technical improvement of automobile manufacturers (need to sign contract).
- 3) *Audio and Video Surveillance Blockchain Data*: *D3*, mainly for the network security.
- 4) *Insurance Purchase Blockchain Data*: *D1*, *D2*, and *D4*, through smart contracts and automates insurance transactions with personalized prices based on the users driving habits and circumstances.
- 5) *Ordinary Transaction Blockchain Data*: *D5*.

B. Blockchain Node

As described above, we classify the vehicle network data into five categories from *D1* to *D5*, and also design five blockchains with different functions (as in Fig. 1). The data communications of different types of blockchains are independent.

The vehicle itself can record all the information, and the integrity of the data collection is similar to that of the black box on the plane and it has complete control over all its own data. On the one hand, the roadside system node can collect the motion information (such as the speed of movement) of the car. On the other hand, it can collect the in-vehicle sensing information (such as fuel consumption, temperature, pressure, various mechanical, and electronic system parameters) from the car, and is responsible for spreading to the network by neighboring vehicles and roadside system nodes, such as RSUs, toll station nodes, gas station nodes, or highway block monitoring, and other types of blockchain nodes.

In the vehicle networks, there are five different blockchain nodes, as in Fig. 1.

- 1) *N1*: Advanced management, including vehicles, all road monitoring nodes, and vehicle management nodes.
- 2) *N2*: Vehicle monitoring, including vehicles themselves, all toll station nodes, and car manufacturer blockchain nodes.
- 3) *N3*: Audio video surveillance, including vehicles themselves, all taxis, and network approx. platform nodes.
- 4) *N4*: Insurance, including vehicles themselves and all insurance company nodes.
- 5) *N5*: General trading categories, including vehicles themselves, all toll stations, gas stations, wash stations, and charging station nodes.

C. IoV Architecture

The network architecture we propose can be seen in Fig. 2: a moving vehicle transmits self-generated data blocks to the network through dynamic neighbor nodes (neighboring vehicles, roadside nodes, toll station nodes, gas station nodes, wash station nodes, and charging station nodes), or through a 4G telecommunications network when there is no available roadside system.

For the five different blockchain data described above, block generation and diffusion correspond to the following (as in Fig. 2).

- 1) *BC1*: They are generated by roadside nodes and can spread to their neighbors.
- 2) *BC2*: They are generated by vehicles and can be sent to a roadside system, where the roadside nodes further forward.
- 3) *BC3*: They are generated by roadside nodes and can be spread to the neighboring roadside nodes.
- 4) *BC4*: After the roadside system collects information, they can be transmitted to toll station nodes, which can be spread to other toll station nodes.
- 5) *BC5*: They are generated and maintained by vehicles, gas stations, wash stations, and charging stations.

D. IoV Blockchain Transmission

Due to the high-speed of vehicles, sudden changes in speed, and error-prone wireless transmission links, it is challenging to apply blockchain technologies in the applications. Therefore, it is critical to adopt effective methods to ensure successful transmission. Unlike the traditional applications of blockchain,

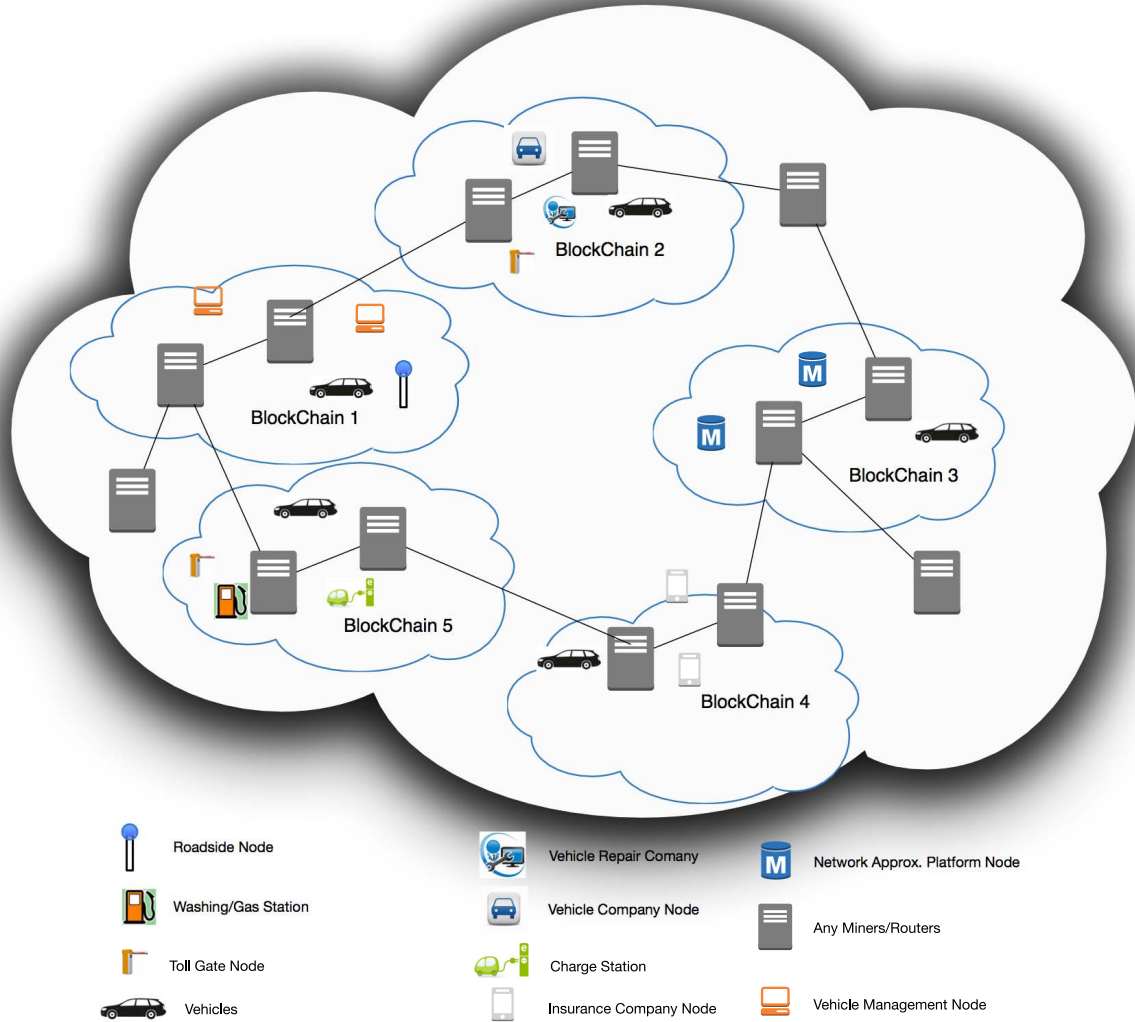


Fig. 1. Defined five blockchains in IoV.

the IoV blockchain technology must consider the mobility of the vehicle, the repeatability of the physical placement of the roadside system nodes and the limited communication range, and the poor communication link quality.

Assume that the vehicle generates a new set of data at regular intervals and is ready to be transmitted to the network. Since there are more roadside nodes that are to be used as nodes of some blockchains, the vehicle will choose to use the roadside system for data transmission. Poor quality transmission results in transmission failure. After a random backoff for a while, the transmission continues at the roadside system. If multiple retransmissions fail and the retransmission number reach a threshold, the cellular network such as 4G could be selected for transmission. We assume that the vehicle fails to transmit data to the roadside system due to the fact that channel available time is less than the data transmission time.

In the traditional blockchain, the current block contains the hash value of the previous block, and the block is simultaneously distributed by the P2P multineighbor node, and combined with the timestamp in the block. In the vehicle network, there are fewer neighbor nodes, and the roadside

nodes as neighbor nodes change dynamically due to the movement of the vehicle. In order to ensure the security of the data, we design a blockchain with “lag timestamp range.” Its details is described in the following.

- 1) Every data block sent by the IoV contains the hash value of the previous block.
- 2) The verification of the block is not only based on a fixed time stamp, but is jointly verified by several blocks whose time stamp is within a certain range. In this way, the problem of data corruption caused by a single RSU node being attacked can be avoided as much as possible. The blockchain structure can be designed as in Fig. 3.

V. PERFORMANCE ANALYSIS MODEL AND EVALUATION

A. Theoretical Model

Table I shows the notations we used in this paper. Assuming the vehicle speed is v , and a roadside node can communicate with a diameter of L , then from the perspective of the roadside node, the arrival of the vehicle follows a Poisson process with an average of λ , while the available channel time T_c follows

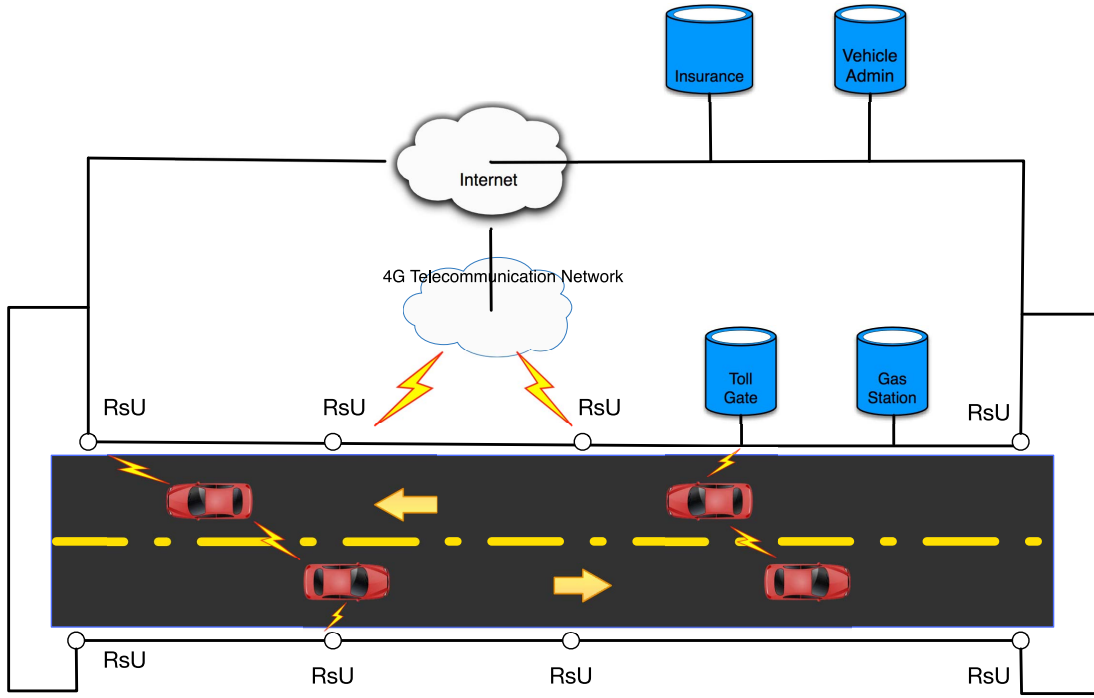


Fig. 2. Blockchain-based IoV network structure.

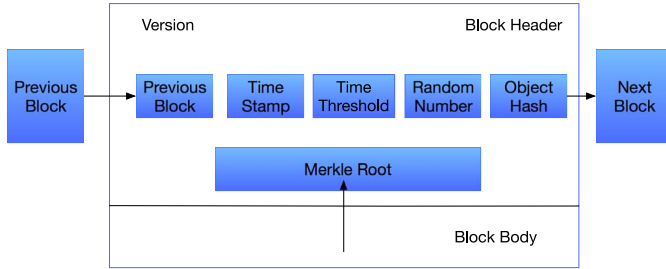


Fig. 3. Blockchain structure.

the uniform distribution with the mean of L/v . The required transmission time of the data is related to the increment of data collected by the current vehicle. Assuming that the data increment of the vehicle increases linearly and the data increment per unit time is Δ_D , and $\Delta_D = \Delta_{D_s} + \Delta_{D_a}$, where Δ_{D_s} is the mean data increment rate of a vehicle and Δ_{D_a} is the mean data arrival rate from other adjacent vehicles. The data from adjacent vehicles should be verified first. The paper in [24] no longer distinguishes between D_s and D_a , but only considers Δ_D in general terms. The minimum data threshold for starting data transmission is D_{th} . If the size of the convergent data is larger than D_{th} and there is no backoff waiting time, then the data transmission can initiate. The remaining time of the link is defined as

$$t_L = \frac{S}{v} \quad (1)$$

where S is the communication distance of the vehicles within the roadside node communication range and v is the vehicle speed. The position at which the vehicle starts transmission within the roadside node communication range, is random.

We assume that it follows a uniform distribution, and its probability distribution function (PDF) is

$$f(s) = \begin{cases} \frac{1}{L}, & 0 < s \leq L \\ 0, & \text{else} \end{cases} \quad (2)$$

where L is the double of communication radius of the roadside node. L follows the normal distribution with mean of u_L and variance of δ_L , and its PDF is

$$f_L(l) = N(u_L, \delta_L^2). \quad (3)$$

The vehicle speed follows the normal distribution with mean of u_v and variance of δ_v , and its PDF is

$$f_V(v) = N(u_v, \delta_v^2). \quad (4)$$

The condition of successful communication is that the communication time t_r is less than the link remaining time t_L

$$P_{\text{success}} = P\{t_r \leq t_L\}. \quad (5)$$

Once the data transmission fails ($P\{t_r > t_L\}$), then after a random delay, the sending process will be reinitiated. We set the random delay time to be between T and $2T$, where

$$T = \frac{u_L}{u_v}. \quad (6)$$

u_L and u_v are independent, for the retransmission of the i th time, $t_{wi} = T + \Delta_{T_i}$, where Δ_{T_i} is a random number within the range of $(0, T)$. The PDF of retransmission time is

$$f(t_{wi}) = f(T + \Delta_{T_i}) \quad (7)$$

where

$$f(\Delta_{T_i}) = \begin{cases} \frac{1}{T}, & 0 < \Delta_{T_i} \leq T \\ 0, & \text{else.} \end{cases} \quad (8)$$

TABLE I
TABLE OF NOTATIONS

L	communication diameter of roadside node
v	vehicle speed
λ	mean arrival rate of vehicle
T_c	available channel time
Δ_D	data traffic arrival rate of vehicle
D_{th}	the minimum data threshold for starting data transmission
t_L	remaining time of link
S	remaining communication distance
$f(s)$	pdf of S
$f_L(l)$	pdf of L
u_L	mean of L
δ_L	variance of L
u_v	mean of v
δ_v	variance of v
t_r	required communication time of a success transmission
$P_{success}$	probability of transmission success
T	the average time for the vehicle to pass through the roadside nodes
t_{w_i}	waiting time of the i th retransmission
ΔT_i	a random number within the range of $(0, T)$ of the i th retransmission
$f(t_{w_i})$	PDF of t_{w_i}
$f(\Delta T_i)$	PDF of ΔT_i
t_{s_i}	accumulation time of the i th retransmission
Δ_i	accumulation data from the first to the i th retransmission
t_{r_i}	the required channel time for the i th transmission
p_i	the probability that the data was sent successfully at the i th time
p_n^-	the probability of the n th transmission failure
$p_{cellular}$	the probability of blockchain packets through cellular network
$f(t_{r_i})$	PDF of t_{r_i}
$f(t_{s_i})$	PDF of t_{s_i}
$f(t_{s_i}, t_L)$	joint PDF of t_{s_i} and t_{r_i}
T_d	the average latency of all packets
N_w	average number of retransmissions
H	throughput

When the first i transmission condition is reached, the data accumulation time is t_{s_i} and the accumulated data amount in t_{s_i} is D_i . Then we can get

$$\begin{aligned}
 t_{s_1} &= D_1 / \Delta_D \\
 D_1 &= D_{th} \\
 t_{s_2} &= t_{s_1} + t_{w_1} \\
 D_2 &= D_1 + t_{w_1} \Delta_D \\
 t_{s_3} &= t_{s_2} + t_{w_2} = t_{s_1} + t_{w_1} + t_{w_2} \\
 D_3 &= D_2 + t_{w_2} \Delta_D = D_1 + (t_{w_1} + t_{w_2}) \Delta_D \\
 &\dots \\
 t_{s_n} &= t_{s_1} + t_{w_1} + t_{w_2} + \dots + t_{w_{n-1}} \\
 D_n &= D_1 + (t_{w_1} + t_{w_2} + \dots + t_{w_{n-1}}) \Delta_D.
 \end{aligned} \tag{9}$$

For the i th transmission, the required channel time is the size of the current data amount divided by the link bandwidth B . Therefore, the required channel time is

$$t_{r_i} = t_{s_i} \Delta_D / B. \tag{10}$$

The probability that the data was sent successfully in the first time is

$$p_1 = P(t_{r_1} \leq t_L). \tag{11}$$

If the first transmission fails, under this condition, the probability of the second successful transmission is

$$p_2 = P(t_{r_1} > t_L) P(t_{r_2} \leq t_L). \tag{12}$$

If the second transmission also fails, under this condition, the probability of the third successful transmission is

$$p_3 = P(t_{r_1} > t_L) P(t_{r_2} > t_L) P(t_{r_3} \leq t_L). \tag{13}$$

If the $(n-1)$ th transmission fails, the probability of the n th successful transmission under this condition is

$$p_n = P(t_{r_n} \leq t_L) \prod_{i=1}^{n-1} P(t_{r_i} > t_L). \tag{14}$$

If the $(n-1)$ th transmission fails, the probability of the n th transmission failure under this condition is

$$p_n^- = \prod_{i=1}^n P(t_{r_i} > t_L). \tag{15}$$

It is assumed that a sending process has at most $n-1$ retransmissions. After the n th failed transmissions, the data packet is not sent to the roadside nodes and will be directly transmitted to the Internet through the cellular network. In this paper, we assume that the transmission through the cellular network is successful. Therefore, the probability of transmitting blockchain packets through cellular network, can be expressed in the following:

$$p_{cellular} = p_n^-. \tag{16}$$

Also, there are

$$p_n^- + \sum_{i=1}^n p_i = 1. \tag{17}$$

Because $t_{w_1}, t_{w_2}, \dots, t_{w_i}$ are independent, so

$$f(t_{w_1}, t_{w_2}, \dots, t_{w_i}) = \prod_{j=1}^{i-1} f(t_{w_j}). \tag{18}$$

From (9), $f(t_{s_i})$ is solved, and from (10), we have

$$f(t_{r_i}) = f(t_{s_i}) \Delta_D / B. \tag{19}$$

Because the communication link time and the data accumulation time are independent, their joint PDF can be derived

$$f(t_{r_i}, t_L) = f(t_{r_i}) f(t_L) \tag{20}$$

so from (11) to (17), p_i can be solved.

B. Performance Parameters

1) *Average Delay Time*: If a packet pkt_1 was successfully sent at the first time, we would define this case as no delay. If the packet fails to be sent at the first time and is successfully sent at the second time, this pkt_1 waits for a retransmission time, plus pkt_2 the second packet formed by the new arrival data. These two packets form a new larger packet. If the new packet is sent successfully, then there is no time delay for pkt_2 , and the time delay for pkt_1 is $(T_1 + \Delta T_1)$, where the probability

density function for T_1 is (6), The probability density function for ΔT_1 is (8).

If a transfer process takes n times before the transfer is successful, that is, pkt_1 transmits successfully at the n times. It waits for $n-1$ retransmissions, while pkt_2 has waited for $n-2$ retransmissions, pkt_3 has waited for $n-3$ retransmissions. Therefore, for the event of n transfer success, the average latency of all packets is

$$T_d = \frac{\sum_{j=1}^{n-1} \left[\sum_{i=j}^{n-1} (T_i + \Delta T_i) \right]}{n-1}. \quad (21)$$

2) *Average Number of Retransmissions*: If a transmission process takes n times before the transmission is successful, that is, pkt_i will retransmit for $n-i$ times, then the sum of all the waiting times for this transmission process is

$$N_w = \sum_{j=1}^{n-1} p_j \left(\sum_{i=1}^{j-1} i \right). \quad (22)$$

3) *Throughput*: Throughput is defined as the average transmission rate, which is amount of data transmitted per unit time. Then the throughput can be calculated as

$$H_r = \frac{\sum_{j=1}^M p_j D_j}{T_d} \quad (23)$$

where M is the maximum number of retransmissions. The total throughput is

$$H = \frac{H_r}{1 - p_{\text{cellular}}}. \quad (24)$$

And the throughput by cellular is $p_{\text{cellular}} H$.

4) *Blockchain Transaction Delay*: Due to the flooding characteristics of the blockchain, according to the blockchain workload, the determination of the transaction needs to be approved by more than half of the nodes. Since this IoV blockchain network is composed of multiple heterogeneous networks, the transaction delay is significantly affected. The bottleneck is the communication between the roadside nodes and the vehicle nodes. The traditional Bitcoin blockchain transaction is established on a stable and reliable communication link, but the flooding information and confirmation could take a long time. The blockchain mechanism for IoV networks in this paper can pass smart contracts, tolerating longer delays.

If there is only one-time access to the vehicle networking node via a roadside node, the time delay does not increase significantly. We assume the nonvehicle node communication is stable, fast, and reliable, to achieve the workload proof of transaction confirmation (more than 50% nodes) with minimum delay. The number of vehicle nodes that need to participate should not be larger than 50% of the number of all block chain nodes. The United States has about 220 million cars. If 10% of the vehicles are connected to IoV, the non-vehicle nodes that need to run the blockchain program need about 22 million.

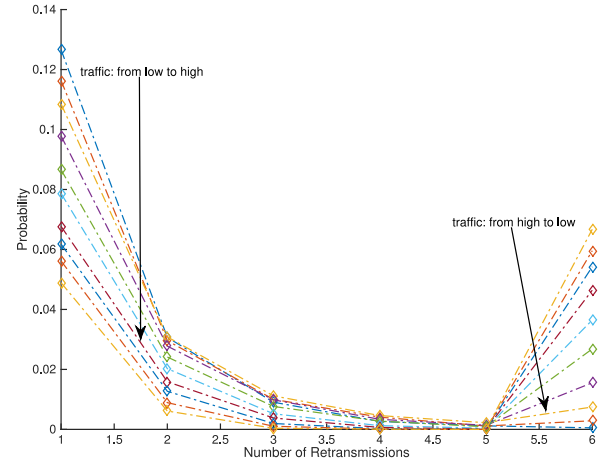


Fig. 4. Probability of retransmissions.

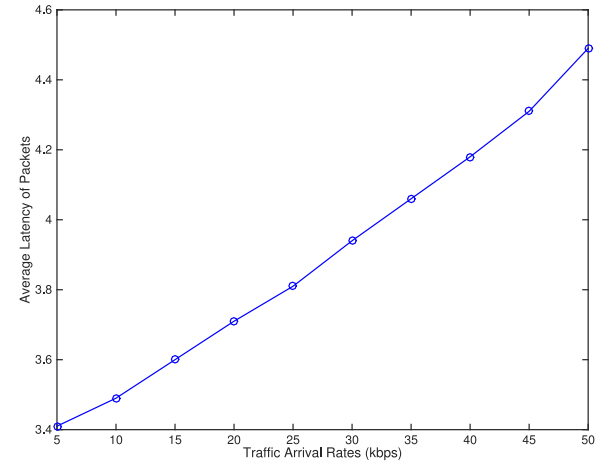


Fig. 5. Average latency of packets.

C. Simulation Results and Analysis

We utilize MATLAB tool to simulate the communication performance of the entire blockchain-based vehicle network. The simulation parameters are configured as follows.

- 1) *The Distribution of Distances Between Roadside Nodes*: $N(u_L, \delta_L^2) = N(400, 20^2)$ (m), $300 \text{ m} \leq L \leq 500 \text{ m}$.
- 2) *The Distribution of Vehicle Operating Speed*: $N(u_v, \delta_v^2) = N(80, 20^2)$ (km/h), $40 \text{ km/h} \leq v \leq 120 \text{ km/h}$.
- 3) *Packet Size Threshold for Bootable Data Transmission*: $D_{th} = 800 \text{ kb}$.
- 4) *Maximum Number of Retransmissions*: 6.
- 5) *Data Traffic Arriving in Unit Time*: $\Delta_D = 5, 10, 15, 20, \dots, 45, 50$ kb/s, channel bandwidth: $B = 200 \text{ kb/s}$.

The simulation results can be seen from Figs. 4–8. As shown in Fig. 4, if the traffic is heavier, the number of retransmissions tends to be larger, and the probability of retransmission is higher. Therefore, the probability of transmission by the cellular system is higher when the transmission cannot rely on the roadside system. Because the high traffic leads to longer packet and transmission time, the duration of link connections is not sufficient. In addition, the probability of retransmission

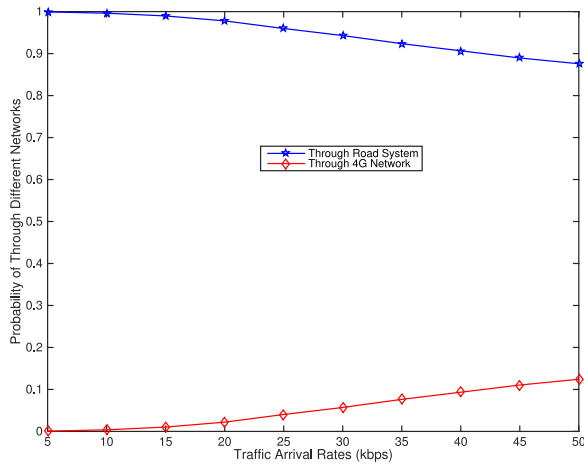


Fig. 6. Probability of packets sent by cellular/roadside system.

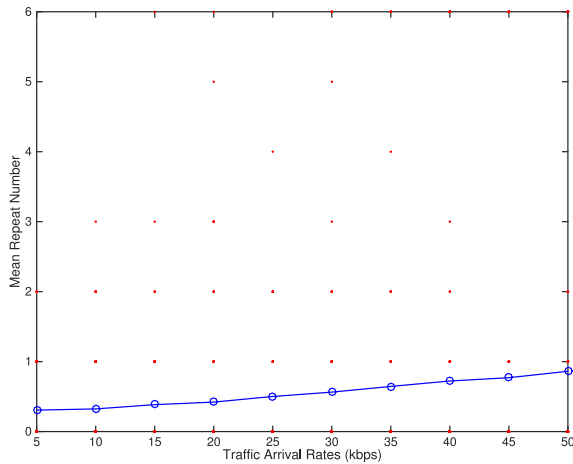


Fig. 7. Average number of retransmissions.

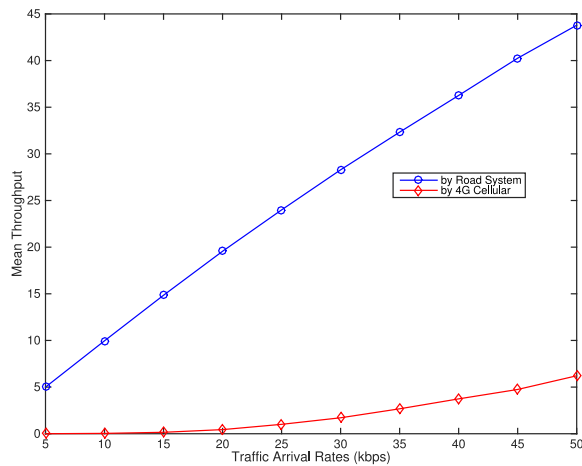


Fig. 8. Average throughput.

is higher when there are no remaining packets to be retransmitted after multiple retransmission attempts. When the number of retransmissions reaches the threshold 6, the communication switches to cellular links.

As shown in Figs. 5 and 8, the horizontal coordinate is traffic arrival rate, or Δ_D . It can be seen from Fig. 5 that the

average delay time of each packet increases when the traffic increases. In Fig. 6, it is observed that the higher the service arrival rate, the more data packets cannot be transmitted through the roadside system. Therefore, the probability of successful transmission of these data packets through the roadside system is greater. The smaller the blockchain packet size, the greater the probability of transmission over a cellular network, because these packets first attempt to pass through the roadside system, and multiple retransmissions fail. After the maximum number of retransmissions is reached, they still cannot pass through the roadside system.

As shown in Fig. 7, the average number of retransmissions of data packets sent in the blockchain increases. For example, when the arrival rate is 50 kb/s, the average number of retransmissions is about 0.86. Therefore, the total number of transmissions required for one transmission required is 1.86. Because the increased service arrival rate increase the amount of data packets, and thus requires longer link duration. Therefore, the probability ratio (compared to cellular systems as Fig. 8) of successful transmission by the roadside system is reduced, which increases the probability of retransmissions. Finally, it increases the overall transmission delay. With the increase amount of data, more traffic can be put into the network, and the average throughput by both cellular system and roadside system increase, as shown in Fig. 8.

VI. CONCLUSION

In this paper, we investigate how blockchain technology can be applied in IoV applications. We further analyze IoV based on blockchain technology in details and discuss the connections between blockchain and IoV as well as the technical difficulties of implementing blockchain for IoV applications. We classify the data blocks of IoV based on blockchain requirements and form multiple blockchain networks for IoV system. In addition, we also present how the nodes in IoV could participate in blockchains, and propose a blockchain network architecture. Based on the architecture, we conduct theoretical modeling and performance analysis of vehicle networking systems. This paper can potentially provide a new guideline to explore blockchain technologies for IoV. Due to space limitations, this paper focuses on the framework and network architecture of the IoV and blockchain including communication performance modeling and analysis methods. Our proposed model does not consider the traffic among vehicles [30], [31] and the channel reliability of the cellular networks. We will include these related studies in our future work.

REFERENCES

- [1] S. Nakamoto. (2009). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: <https://bitcoin.org/bitcoin.pdf>
- [2] M. Swan, *Blockchain: Blueprint for a New Economy*. Sebastopol, CA, USA: O'Reilly Media Inc., 2015.
- [3] V. Buterin, "A next-generation smart contract and decentralized application platform," Bitcoin Mag., White Paper, Jan. 2014. [Online]. Available: <https://github.com/ethereum/wiki/wiki/White-Paper>
- [4] S. Wilkinson, T. Boshevski, J. Brandoff, and V. Buterin, "Storj: A peer-to-peer cloud storage network," Rep. [Online]. Available: <http://citeseerx.ist.psu.edu/viewdoc/summary?doi=10.1.1.693.785>

- [5] S. Wilkinson, J. Lowry, and T. Boshevski, "MetaDisk a blockchain-based decentralized file storage application," Rep., 2014. [Online]. Available: <http://metadisk.org/metadisk.pdf>
- [6] C. Michael, Nachiappan, P. Pattanayak, S. Verma, and V. Kalyanaraman, "Blockchain technology: Beyond bitcoin," *Appl. Innov. Rev.*, vol. 1, no. 2, pp. 6–19, 2016. [Online]. Available: <http://scet.berkeley.edu/wp-content/uploads/AIR-2016-Blockchain.pdf>
- [7] H. Kalodner, M. Carlsten, P. Ellenbogen, J. Bonneau, and A. Narayanan, "An empirical study of namecoin and lessons for decentralized namespace design," in *Proc. Workshop Econ. Inf. Security (WEIS)*, 2015, pp. 1–27.
- [8] C. Fromknecht and D. Velicanu. (2014). *A Decentralized Public Key Infrastructure With Identity Retention*. [Online]. Available: <https://eprint.iacr.org/2014/803.pdf>
- [9] P. K. Sharma, S. Singh, Y.-S. Jeong, and J. H. Park, "DistBlockNet: A distributed blockchains-based secure SDN architecture for IoT networks," *IEEE Commun. Mag.*, vol. 55, no. 9, pp. 78–85, Sep. 2017.
- [10] V. Daza, R. Di Pietro, I. Klimek, and M. Signorini, "CONNECT: Contextual name discovery for blockchain-based services in the IoT," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Paris, France, 2017, pp. 1–6.
- [11] O. Novo, "Blockchain meets IoT: An architecture for scalable access management in IoT," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1184–1195, Apr. 2018.
- [12] P. K. Sharma, M.-Y. Chen, and J.-H. Park, "A software defined fog node based distributed blockchain cloud architecture for IoT," *IEEE Access*, vol. 6, pp. 115–124, 2018.
- [13] K. Yeow, A. Gani, R. W. Ahmad, J. J. P. C. Rodrigues, and K. Ko, "Decentralized consensus for edge-centric Internet of Things: A review, taxonomy, and research issues," *IEEE Access*, vol. 6, pp. 1513–1524, 2018.
- [14] C. Li and L.-J. Zhang, "A blockchain based new secure multi-layer network model for Internet of Things," in *Proc. IEEE Int. Congr. Internet Things (ICIoT)*, Honolulu, HI, USA, 2017, pp. 33–41.
- [15] M. Conoscenti, A. Vetrò, and J. C. De Martin, "Blockchain for the Internet of Things: A systematic literature review," in *Proc. IEEE/ACS 13th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Agadir, Morocco, 2016, pp. 1–6.
- [16] G. Varshney and H. Gupta, "A security framework for IoT devices against wireless threats," in *Proc. 2nd Int. Conf. Telecommun. Netw. (TEL-NET)*, Noida, India, 2017, pp. 1–6.
- [17] C. H. Lee and K. H. Kim, "Implementation of IoT system using block chain with authentication and data protection," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Chiang Mai, Thailand, 2018, pp. 936–940.
- [18] J. H. Jeon, K.-H. Kim, and J.-H. Kim, "Block chain based data security enhanced IoT server platform," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Chiang Mai, Thailand, 2018, pp. 941–944.
- [19] C. Xie, Y. Sun, and H. Luo, "Secured data storage scheme based on block chain for agricultural products tracking," in *Proc. 3rd Int. Conf. Big Data Comput. Commun. (BIGCOM)*, Chengdu, China, 2017, pp. 45–50.
- [20] W. Cheng, S. Wang, and X. Cheng, "Virtual track: Applications and challenges of the RFID system on roads," *IEEE Netw.*, vol. 28, no. 1, pp. 42–47, Jan./Feb. 2014.
- [21] N. Kaaniche and M. Laurent, "A blockchain-based data usage auditing architecture with enhanced privacy and availability," in *Proc. IEEE 16th Int. Symp. Netw. Comput. Appl. (NCA)*, Cambridge, MA, USA, 2017, pp. 1–5.
- [22] O. N. Hamoud, T. Kenaza, and Y. Challal, "Security in device-to-device communications: A survey," *IET Netw.*, vol. 7, no. 1, pp. 14–22, Jan. 2018.
- [23] A. Chakravorty and R. Chunming, "Ushare: User controlled social media based on blockchain," in *Proc. 11th ACM Int. Conf. Ubiquitous Inf. Manag. Commun. (ACM IMCOM)*, Jan. 2017, Art. no. 99.
- [24] Z. Yang, K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, "Blockchain-based decentralized trust management in vehicular networks," *IEEE Internet Things J.*, to be published.
- [25] C. Liu, K. K. Chai, X. Zhang, E. T. Lau, and Y. Chen, "Adaptive blockchain-based electric vehicle participation scheme in smart grid platform," *IEEE Access*, vol. 6, pp. 25657–25665, 2018.
- [26] F. Gao *et al.*, "A blockchain-based privacy-preserving payment mechanism for vehicle-to-grid networks," *IEEE Netw.*, vol. 32, no. 6, pp. 184–192, 2018.
- [27] X. Huang, C. Xu, P. Wang, and H. Liu, "LNSC: A security model for electric vehicle and charging pile management based on blockchain ecosystem," *IEEE Access*, vol. 6, pp. 13565–13574, 2018.
- [28] N. Kshetri, "Can blockchain strengthen the Internet of Things?" *IT Prof.*, vol. 19, no. 4, pp. 68–72, Aug. 2017.
- [29] K. Kotobi and S. G. Bilen, "Secure blockchains for dynamic spectrum access: A decentralized database in moving cognitive radio networks enhances security and user access," *IEEE Veh. Technol. Mag.*, vol. 13, no. 1, pp. 32–39, Mar. 2018.
- [30] Q. Yang and H. Wang, "Toward trustworthy vehicular social networks," *IEEE Commun. Mag.*, vol. 53, no. 8, pp. 42–47, Aug. 2015.
- [31] Q. Yang, B. Zhu, and S. Wu, "An architecture of cloud-assisted information dissemination in vehicular networks," *IEEE Access*, vol. 4, pp. 2764–2770, 2016.

Author's photographs and biographies not available at the time of publication.