CHAPTER TWO

Blockchain for a Trust Network Among Intelligent Vehicles

Shiho Kim
School of Integrated Technology, Yonsei University, Seoul, South Korea

Contents

Abstract

The intelligent vehicle communication network is prone to cyberthreats, which are difficult to solve using traditional centralized security approaches. Blockchain is an immutable peer-to-peer distributed database containing cryptographically secured information. Blockchain shows successful use cases in financial applications, smart contact, protecting digital copyright of media contents. It extends to all industries including the secure IoT devices, embedded systems, etc. The superior feature of blockchain is its decentralized, immutable, auditable database that secures transactions by protecting privacy. In this chapter, we contemplate the environment of the intelligent vehicle communication network and issues regarding methods of building a blockchain-based trust network among intelligent vehicles. We present the use cases of blockchain in intelligent vehicles in the phase of ongoing research or that under development from automotive industries and academic institutes. We also deliberate the challenging issue of blockchain for intelligent vehicles.

Advances in Computers, Volume 111
ISSN 0065-2458
https://doi.org/10.1016/bs.adcom.2018.03.010

1. INTRODUCTION

Vehicle technology has advanced rapidly toward the ultimate goals of autonomous driverless cars for efficient traffic flow, preventing human error-related accidents, and improving fuel economy, and emerging electric vehicle charging services. Wireless internet access combined with other communication elements is becoming basic features of intelligent vehicles. The modern intelligent connected car has become a computer system similar to a smartphone, controlled by a complex computer with a wireless communication network and internal in-vehicle network. The intelligent vehicles connected to almost everything are evolving rapidly as a cyber-physical system from the traditional rich mechanical system.

However, the introduction of a vehicular cloud network based on wireless internet connectivity means a remarkable increase in the reliance on the networked software. This leads to a cybersecurity issue, as well as safety-related function problems in the automotive industry. Based on these aforementioned facts, one of the most important concerns associated with intelligent vehicles is to use a trust network to secure them against malicious cyberattacks.

Conventional centralized security system is vulnerable because if a central system is compromised, owing to fraud, cyberattack, or a simple error, the entire network is affected. Conventional security and privacy methods used in personal computers or cloud networks tend to be ineffective in intelligent vehicles owing to their vulnerability in cyberattacks.

Blockchain technology works for the cryptocurrency, which has recently been used to build trust and reliability in peer-to-peer networks with similar topologies as networks of intelligent vehicles. Blockchain technology works for cryptocurrency, which has recently been used to build trust and reliability in peer-to-peer networks with similar topologies as networks of intelligent vehicles. Blockchain has shown successful use cases in financial applications, smart contact, and delivering media content with digital copyright protection. Applicable fields have now been extended to secure internet of things (IoT) devices, embedded systems, and to industries other than information-related fields [1]. A superior feature of blockchain is its decentralized, immutable, auditable database for secure transaction with privacy protection [2]. In this chapter, we contemplate the trusted environment of intelligent vehicle communication network and how the blockchain technology creates trust network among intelligent vehicles.

The blockchain technology is gaining momentum and creating new business opportunities in both the automotive and ICT (information and communication) industries to untangle the potential cybersecurity threat of intelligent connected vehicles; however, challenges lie ahead [3]. In order to apply blockchain to intelligent connected vehicles, participants of the vehicle cloud need to overcome a number of technical challenges due to the limited capability of in-vehicle power and storage, and many other factors.

Autonomous vehicles are no longer privately owned assets, but they may create many new business models. Blockchain technology has already disrupted the financial, media content service, and healthcare industries, and the automotive industry will follow [4,5]. Some automakers and research institutes have started to explore blockchain to create new ecosystems of new service and business models for autonomous and connected vehicles [6].

In this chapter, we introduce the key aspects of cybersecurity issues in intelligent vehicles and discuss how we build secure trust networks using blockchain technology.

Rest of the chapter is divided into two sections. In Section 3, we investigate use cases of blockchain in intelligent vehicle proposals and researches initiated from both automotive industries and academic institutes. To apply blockchain to intelligent connected vehicles, participants in the vehicle cloud need to overcome a number of technical challenges due to the limited capability of in-vehicle power and storage, and many other factors. In Section 4, we present challenging issues of blockchain for intelligent vehicles. The technology/technical terms used in this chapter are explained wherever they appear or at the "Key Terminology and Definitions" section. Apart from regular References additional references are included in the "References for Advance/Further Reading" for the benefit of advanced readers.

2. INTRODUCTION TO CYBERSECURITY ISSUES OF INTELLIGENT VEHICLES

Modern intelligent vehicles are controlled by complex computer with connectivity of both internal in-vehicle network and wireless communication network. While this computerized structure has offered a prominent technology for intelligent functionality such as advanced driver-assistant system or self-driving autonomous vehicles, but also it makes the vehicles insecure and potentially vulnerable to various kinds of malicious hackings and

cyberattacks. This section presents a brief introduction and use cases of intelligent vehicles and connected vehicles, and then we raise the open question of the cybersecurity issue of intelligent vehicles.

2.1 Brief Introduction to Intelligent Transportation System and Connected Vehicles

We generally define the connected car which is equipped with wireless internet connectivity and usually also with VANET (vehicular ad hoc NETwork). Advances in software and hardware technology lead to vehicles under full computerized intelligent control. Fig. 1 shows a typical architecture of an intelligent connected vehicle. Intelligent vehicles include numerous networked control units with sensors ensuring multiple vehicle functionalities. The necessary hardware devices realizing intelligent and connected vehicle function can be classified into built-in or brought-in connection systems.

Connected cars have become a smartphone-like computer system with internet connection, while it has more complex control through in-vehicle network for the control of motion dynamics, prolusion and drive train, and electronic accessories associated with a variety of functions providing comfort and convenience to occupants.

Sometimes, VANET is referred to as the wireless network known as intelligent transportation system (ITS), which is aiming to enable safe, efficient flow of traffic, environmentally conscious intelligent transportation services, as well as additional traveler information services. ITS is designed

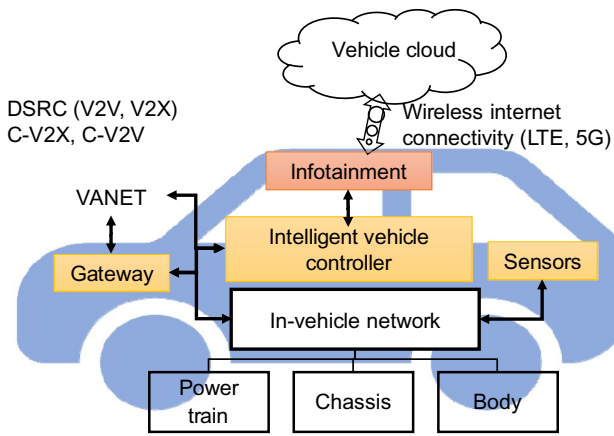

Fig. 1 Outline of intelligent connected car.

to support the car to share or to exchange information among vehicles and infrastructures through the communication protocols such as vehicle-to-vehicle (V2V), vehicle-to-(roadside) infrastructure (V2I), and vehicle-to-network (V2N) or vehicle-to-everything (V2X) communications. The standard protocol used for ITS includes traditional DSRC (dedicated short range communication) or emerging cellular V2X (C-V2X) communication. DSRC, which is based on a family of standards referred to as Wireless Access in Vehicular Environments, is a well-established technology undergone extensive product development and field trials by numerous stakeholders over nearly two decades. In contrast, C-V2X is an emerging technology developed within 5G LTE (long-term evolution) cellular communication by the standardization consortium of 3GPP (the 3rd Generation Partnership Project) [7].

Built-in telematics boxes most commonly used for internet connection via a WIFI and LTE modules integrated in the infotainment (i.e., information plus entertainment) system. The brought-in devices are plugged into the gateway of in-vehicle bus through the on-board diagnostics port, which is a network connector of the scanner and diagnostic tools of vehicles.

Autonomous vehicle is the state-of-the-art of systems where actuation and decision-making maneuvers operate concurrently with coping with incoming environmental information from sensors and communication networks during driving.

Intelligent vehicles will be connected to almost everything, and they will become a part of "IoT." The introduction of a wireless internet connectivity-based vehicle cloud will trigger a remarkable increase in the reliance on the networked software, consequently, leading to issues of cyberthreats for data security, leakage of privacy, as well as safety-related functions in vehicles.

2.2 Use Case/Application of Intelligent Vehicles

This section presents a broad overview of the current potential applications and those under development, as well as use cases of intelligent vehicles. Intelligent connected vehicles communicate with almost all systems and devices in cyberspace, and even those existing at off-line, including smartphones, other vehicles, surrounding roadside infrastructure, various servers, and even offices and homes. Vehicles that become a part of the IoT enable the development of numerous applications offering new services or business opportunities in the public transport, industrial, and entertainment sectors in addition to significant enhancements to safe, efficient, and comfort-driving functions. Fig. 2 shows

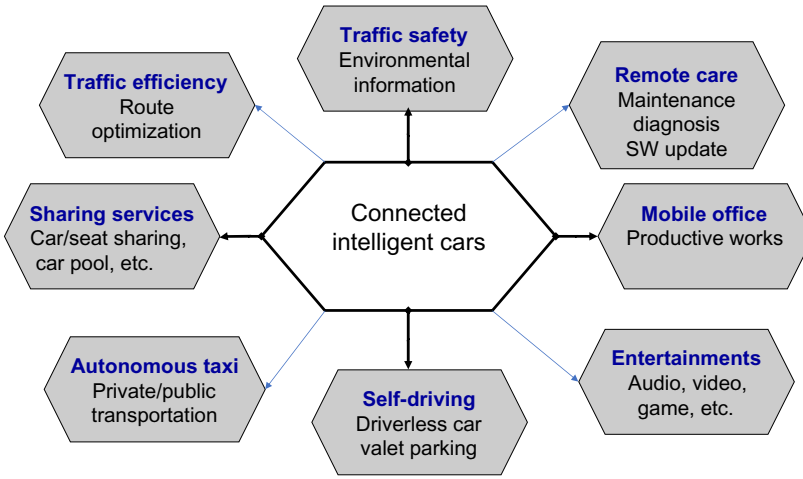

Fig. 2 Service and applications of next-generation intelligent connected cars.

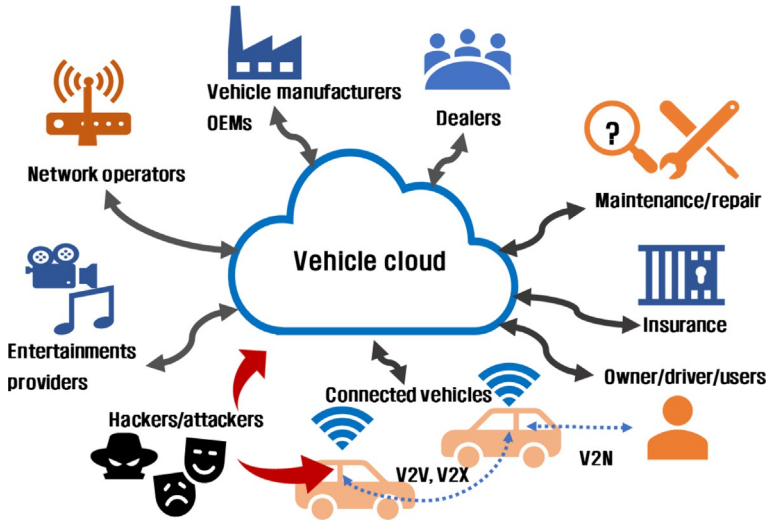

Fig. 3 Ecosystem of the intelligent vehicle industry based on the vehicle cloud.

service and applications of next-generation intelligent connected cars, and Fig. 3 illustrates an emerging ecosystem of the intelligent vehicle industry based on the Vehicle Cloud. Key features of current and potential applications and use cases of the connected vehicle include:

i. *Traffic Safety*: Statistics reveal that more than 90% of traffic accidents are caused by human error of drivers. Intelligent vehicle will clearly

improve traffic safety and effectively reduce the number of fatalities and injuries by implementing safety-assistant functions that exploit environmental information from in-vehicle sensors and installed communication devices.

ii. *Traffic Efficiency*: Optimization of the route by taking into account data of environmental and traffic condition offers substantial benefits in traffic efficiency by improving traffic flows and fuel efficiency, and reducing travel time.

iii. *Self-Driving/Driverless car*: Advanced intelligent connected cars will be born to support autonomous self-driving without human's involvement in maneuvering; these driverless cars offer people a new realm of experience and service in both private and public transportation. The self-driving cars may be a destructive creation, upsetting established industries and reshaping cities, and providing new options for what do while riding a car. Some examples of simple derived applications are automatic valet parking services, and remote charging services of electric vehicles.

iv. *Sharing Services*: Advancement in vehicle technology allows users to share of facility of transportation facilities more conveniently, and a progress in a new sharing service is ready to come. Established car sharing services still need a driver; however, autonomous cars will reshape the sharing services, to include not only sharing of a car, but also sharing a part of seats or cargo space of vehicles. The implication of a future of shared, autonomous vehicles is that ownership of private car is likely to be disrupted.

v. *Autonomous Taxi*: Traditional mobility operates in two ways: Public transportation at low maintenance cost but for low convenience and Private ownership at a high cost but high convenience. With the advent of on-demand autonomous mobility services, consumers have benefited from lower costs and high convenience. Self-driving cars lead to autonomous taxis, which is a new way of mobility combining the low management cost of public transportation and the convenience of personal mobility demand.

vi. *Entertainments*: Car entertainment systems are a collection of hardware and software in automobiles that provides audio, video or game, and entertainment. Traditional in-car information and entertainment originated with car audio and navigation systems, and this has advanced to include video players, games, and other means of advanced contents for entertainment connected to the internet.

vii. *Remote Care and Maintenance*: Advancements in the technology of wireless connectivity and in-vehicle networked embedded system with sensors enable remote diagnosis and maintenance of vehicles. Over-the-air update is a common way of distributing new software or updating revised version of software in mobile phones. Intelligent vehicles allow the automotive industry to embrace the Over-the-air update technologies, enabling secure remote software updates to be downloaded to the vehicle from a server.

viii. *Mobile Office*: Autonomous vehicle free drivers from having to pay attention to driving. Instead, they are able to rest or conduct productive tasks. Self-driving cars may ultimately morph into a fully connected mobile office so users can work on simple or professional tasks during their commute.

Methods of providing various services, such as the continuous evolution of services, management of protocol, and remote upgrading of vehicle firmware, to vehicle users are a challenge. The advent of wireless internet connectivity enables the realization of a vehicle cloud network that supports intelligent vehicle applications and services based on the cloud computing technique [8,9]. By integrating a bidirectional communication link in the cloud computing technique, convenient customized services and access control can be implemented for vehicle users, service providers, and various parties related to intelligent vehicles.

2.3 Cybersecurity Issue of Intelligent Vehicles

Wireless internet access combined with other communication elements is becoming basic features of intelligent vehicles. Intelligent vehicles are evolving rapidly as a cyber-physical system from the traditional rich mechanical system. Connected intelligent vehicles offer a range of sophisticated services that benefit the vehicle drivers, users, owners, authorities of transport management, automanufacturers, and other service providers. Whenever a device is connected to the internet it is exposed to a risk from various malicious cyberattacks. Advanced cars equipped with digital technology have the most computerized features and are networked to communicate with each other, which opens up new roads for hacking. Like the other ICT industries that are often targets of data breaches, the intelligent vehicles must consider the many potential attack surfaces that hackers can use to break into a network. In addition to the internet connections, other communication elements of automobile are vulnerable to security threats

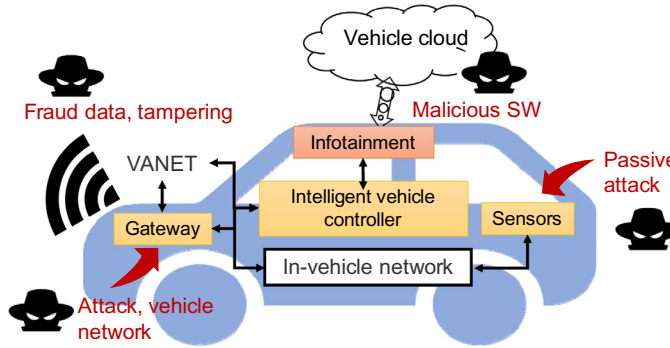

Fig. 4 Potential attack surface of intelligent connected car.

against vehicle safety and the protection of sensitive privacy information, which may lead to fatal consequences. The attack surfaces of intelligent connected car are broad and may extend far beyond the vulnerability of hacking the vehicle itself.

Potential security threats and attack surface of intelligent connected cars can be classified into following four categories as shown in Fig. 4: remote attack through VANET, cyberattack through the internet, passive attack by tampering with sensors data, and attempted unauthorized connection to the in-vehicle network architecture.

i. *Threat of V2X communication*: V2X communications can impose some serious threats against security and safety of vehicles and can lead to disturbed traffic flow. Intelligent vehicles are required to gather information such as the traffic environment, instantaneous traffic situations at invisible distances, and data for cooperative driving. V2X communications are vulnerable to attacks by transmitting fake information or tampering with messages. One of the challenges of blockchain technology for intelligent vehicles is the provision of a secure V2X communication network to trust messages from other vehicles or infrastructures, as well as without privacy leakages.
ii. *Passive attack:* A malicious attack that makes vehicle senses an incorrect information by counterfeiting traffic signals or road signs or by providing fake signals.
iii. *Attempting direct attacks on the in-vehicle network*: An attacker can attempt to make an unauthorized connection to the in-vehicle network, whereby we are able to control the core functions of the vehicle through the gateway of the in-vehicle network.

iv. *Internet connection and/or vehicular cloud:* Internet connection turns intelligent vehicles into a cyber-physical system and each vehicle behaves as a kind of nodes in the IoT [8]. Then, the vehicles are revealed to the potential malicious attackers through various channels by which to access the vehicle's delicate controller or in-vehicle network bus. This potentially exposes intelligent vehicles to a wide range of safety, security, and privacy threats such as malware attacks, location tracking, unauthorized connections, and remote hijacking of the vehicle. This cyberthreat is the biggest risk for autonomous self-driving vehicles. Malicious entities can compromise a vehicle, which not only endangers the security of the vehicle, but also the safety of the passengers.

Based on the aforementioned facts, one of the most important concerns associated with intelligent vehicles is to secure them against malicious cyberattacks. For integrated vehicle security, fundamental defense mechanisms other than conventional authentication, firewall, or limited access of connection against malicious attacks on the internet connection have not been announced. Conventional security and privacy methods used in personal computers or cloud networks tend to be ineffective in intelligent vehicles due to their differences in vulnerability in cyberattacks.

3. BLOCKCHAIN-BASED TRUST NETWORK AMONG INTELLIGENT VEHICLES

Intelligent vehicles (IVs) are experiencing a revolutionary growth in research and industry, but still suffer from numerous security vulnerabilities. To take advantage of the opportunities of intelligent vehicles as a new platform of information technology, we need to overcome a number of challenges in implementing a secure trust network between intelligent vehicles. In modern secure communication, all data communication is encrypted and authenticated using a public/private key infrastructure with certificate-based mutual authentication between connected nodes or cloud servers. Although mutual authentication ensures that both devices can verify the authenticity of each other, these traditional security methods are still vulnerable to secure data sharing between intelligent vehicles [10–12]. A fundamental requirement of ITSs is the guarantee of provenance, immutability, and an error-resilient network between intelligent vehicles.

The characteristics are described as follows:

- Provenance: Each participant knows where the asset came from and how its ownership has changed through transactions.

- Immutability: No participant can tamper with a transaction after it has been recorded in the database (Ledgers).
- Resilience: If a transaction is in error, the corruption is readily apparent, and everyone is made aware of it. A new transaction can be used to recover the error, and the transaction is then restored. In the event that some nodes are offline or under attack, the whole network operates as usual.

Blockchain has been recognized as an emerging technology with the potential to disrupt all traditional industries. The impact of blockchain technology has been experienced in the financial sector already with cryptocurrencies like Bitcoin, Ethereum, and other crypto coins. Currently, the blockchain technology has exploited to applications such as smart contacts, medical and healthcare, and business logistics, then, attempts are being made to incorporate blockchain into more sophisticated areas such as the security of IoT. In the following section, we will discuss "How the blockchain can enhance security and privacy capabilities in a trusted environment-based intelligent vehicle communication network".

3.1 A Brief Review: How the Blockchain-Based Trust Network Works

We are currently exploring the fundamental question of "How can the trust network among anonymous participants be formed by blockchain technology?" A blockchain is a decentralized ledger that contains data of all transactions performed across a peer-to-peer network. Then, how can the concept of a shared distributed ledger make a secure and immutable record of all transactions on the network? Fig. 5 shows an overview of the basic mechanism of Blockchain.

Blockchain uses a well-known asymmetric private/public key and hash cryptography mechanism to validate the authentication of transactions. The private key is used to sign the transactions made by each node. All transactions signed with a private key are broadcast to all network nodes. All mining nodes of the network collect new transactions and works on finding a resolution for a given consensus rule. When a node finds a consensus of the given mechanism, it broadcasts the block to all nodes. All other nodes receive the block and, only if all transactions therein are valid, all nodes express their acceptance of the block by creating the next block in the chain. The first node that encapsulates the block successfully, i.e., finds a consensus resolution, obtains a reward of cryptocurrency, which may be a worthwhile goal, to motivate each mining node to elaborate to find consensus of the

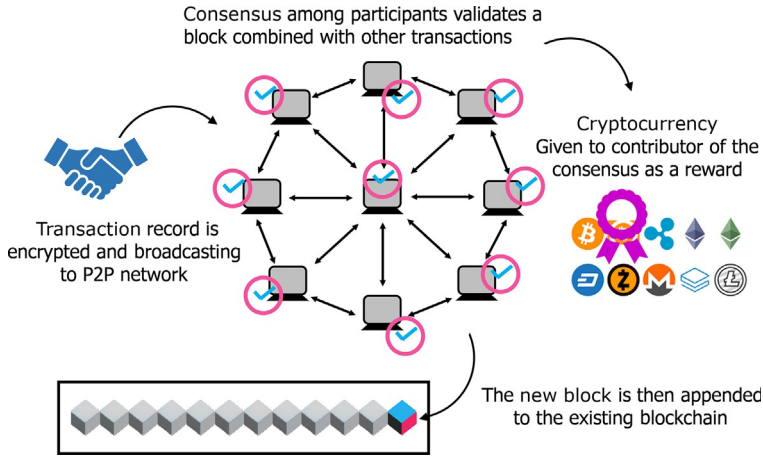

Fig. 5 Overview of the basic mechanism of blockchain.

next block. This consensus with reward and incentives system becomes the driving force for participants to maintain the blockchain without being breakdown.

The transaction data contained in these blocks become immutable, and this can be considered to be trusted and secured, because transactions are recorded by synchronized time stamps and grouped into cryptographically secured blocks that are organized in chains [13].

Depending on its openness, we classify the blockchain with public architecture like Bitcoin and Ethereum, which operate with anonymous untrusted participants with permission-less access, or with permissioned access, which deals only with approved members. In the public blockchain, each node can take participate in the consensus process, where, transactions are automatically approved and recorded by mass participation [14].

3.2 Blockchain-Based Trust Network Among Intelligent Vehicles

Blockchain is able to assure three major risks to build a trust network among intelligent vehicles without central control authority, protecting the privacy and security against cyberattacks, and guaranteeing resilience under unpredictable failure or attack on the vehicular cloud network.

Blockchain technology is based on peer-to-peer connections that allow intelligent vehicles to interact with each other without any intervention of third trusted authorities. A large number of vehicle nodes ensure the resilience of the blockchain network, and even when some nodes are unavailable

due to infected nodes with malicious software or those under a cyberattack, the correct blockchain will still be accessible to vehicles. Even if some nodes are offline or under attack, blockchain can make the vehicular network operates as usual. All transactions in blockchains are time-stamped, and encrypted with private keys so vehicle users can easily trace the history of transactions and track accounts at any historical moment. This feature also allows each participant to track and trace the provenance of data or assets, i.e., the valid information regarding the source of the asset and how its ownership has changed through transactions. This tracking capability prevents potential attack by sending fraudulent data or tampered messages in V2X communications, securing the network against fraudulent security. An attacker may attempt to deanonymize the ID of the vehicle or tracking privacy information of the user, and each transaction contains privacy-sensitive data that endangers the privacy of the user. The blockchain can ensure protection of the privacy of the user by using a hash function, and encryption using asymmetric cryptography.

3.3 Use Case/Application of Blockchain for Intelligent Vehicles

In this section, we will discuss some ongoing research and the implementation of blockchain applications for intelligent vehicles.

Several research organizations and industries are working on blockchain technology implementation for the intelligent vehicles. Yuan et al. [15] have proposed the blockchain technology for ITS for the establishment of a secured, trusted, and decentralized autonomous ecosystem and proposed a seven-layer conceptual model for the blockchain. Leiding et al. [16] have also proposed the blockchain technology for the VANET. They have combined the Ethereum blockchain-based smart contracts system with the VANET. They have proposed a combination of two applications for vehicles, namely, mandatory applications (traffic regulation, vehicle tax, vehicle insurance) and optional applications (applications that provide information and updates on traffic jams and weather forecasts) of vehicles. They attempted to connect the blockchain with VANET services. Blockchain can use multiple other functionalities such as communication between vehicles, provide security, and provide peer-to-peer communication without disclosing personal information. Dorri et al. [17] proposed the blockchain technology mechanism without disclosing any private information of vehicles users to provide and update the wireless remote software and other emerging vehicles services. Rowan et al. [18] described the blockchain technology for securing intelligent

vehicles communication through the visible light and acoustic side-channels. They have verified their proposed mechanism through a new session cryptographic key, leveraging both side-channels and blockchain public key infrastructure. However, thus far, the focus has been on services and their business models, and safe and secure trust environments for the intelligent vehicle communication has not been discussed.

In addition, Toyota has declared that they are working on blockchain technology for the connected vehicle project [6,19]. Toyota research institute (TRI) is collaborating with academic institutes and industry for this blockchain for intelligent vehicles projects. They believe that blockchain technology has emerging features for the storage and use of driving data of automated vehicles. TRI and its collaborators are concentrating on data sharing, ride sharing and transactions, and user-based insurance. ZF motion and mobility company [20] is working with the UBS Swiss bank on blockchain technology for electric cars. They have proposed the mobile e-wallet concept for secure vehicle-related payments such as toll payment, energy charge payment, and car sharing/ride sharing.

3.3.1 Toyota's Blockchain Projects

As mentioned, the automotive industry is the next target of blockchain technology. TRI has already started three blockchain projects on autonomous technology [6,19]. These projects are as follows:

- *Driving/testing data sharing:* Intelligent vehicles connected to the cloud are aware of their environment through onboard sensors, all of which generate valuable driving data. Blockchain technology can provide a decentralized platform of frameworks, which allows creators and perspective customers to share and monetize their driving information in a secure marketplace. Toyota aims to development of a blockchain framework to share driving data while preserving ownership of the data. The goal of this attempt is similar to the approach of the blockchain initiative of the open music initiative, which creates digital property rights in the music industry [21].
- *Car/rideshare transactions*: Blockchain enables storage of the vehicle usage data and information about users (owner, passengers, driver, etc.). Toyota is attempting to build a blockchain-based tool to empower vehicle owners to monetize their asset by sharing their car by selling rides or cargo space. This is a service based on a smart contract between two parties, and blockchain helps to manage the financial transaction between them without any third party intervention, thereby saving transaction surcharges.

The system will also provide connectivity to vehicle functions for remote access to locking/unlocking doors and on/off control of the engine.

- *Usage-based insurance:* By allowing collection of driving data and storage in a blockchain, vehicle owner's pay lower insurance costs by providing their driving data for evaluation of the driving style to influence safe driving. The insurance company can correctly evaluate the safety of the driving habits from the driving data stored in blockchain.

Blockchains and distributed ledgers may enable the pooling data from vehicle owners, fleet managers, and manufacturers to shorten the time to reach this goal, thereby advancing the safety, efficiency, and convenience benefits of autonomous driving technology. TRI insists that hundreds of billions of miles of human driving data may be needed to develop safe and reliable autonomous vehicles. Through an open-source approach to software tools, TRI is creating a user consortium and hopes to stimulate a rapid adoption of blockchain by other companies developing autonomous vehicles and providing mobility services. TRI is inviting current and future partners to collaborate on further development of blockchain and distributed ledger technology applications in vehicle data and services.

TRI is working on these projects with MIT Media Lab and several industry partners. These partners are BigchainDB (a German company), which is building the driving/testing database; Oaken Innovation (Canadian Company) developing peer-to-peer car sharing and mobility tokens based payments system; Commuterz, an Israeli Startup Company, developing a carpooling solution; Gem, (a US-based company) working with Toyota Insurance Solutions and anther Japanese company Insurance on a usage-based insurance system.

3.3.2 Blockchain-Based ITSs

The China Academy of Sciences proposed an ITS-oriented seven layers stacked open system model of blockchain similar to the well-known open system interconnection (OSI) reference model which defines a networking framework to implement protocols in seven layers as shown in Fig. 6 [15]. It provides a conceptual framework to understand complex relationships of layer to layer interactions that are occurring at each a vertical stack and internetworks. Although its usefulness for the reference model to see how the system can work over the network, OSI has been rarely actually implemented. The proposed seven-layer blockchain model provides a reference for characterizing and standardizing the typical architecture and major components of blockchain systems, and briefly describes its underlying key techniques.

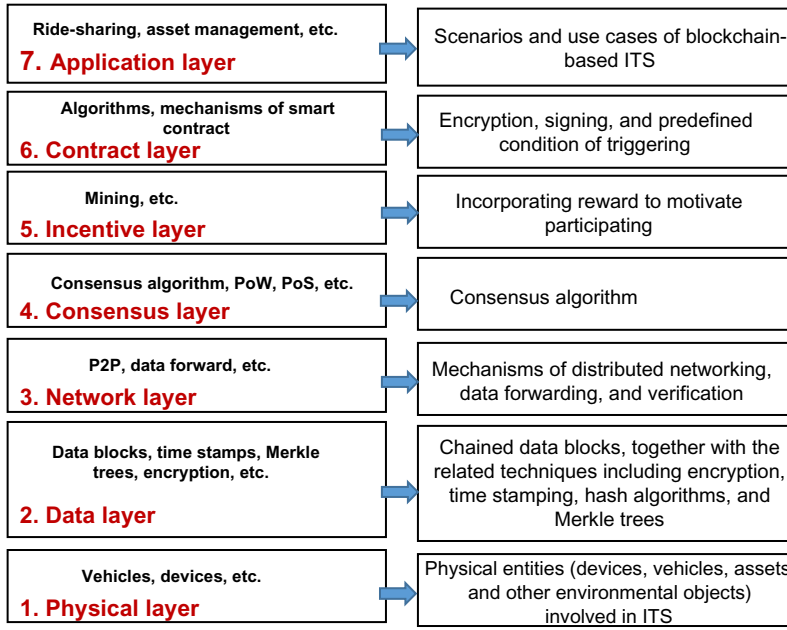

Fig. 6 ITS-oriented seven layers stacked open system model of blockchain [15].

3.3.3 CUBE—Autonomous Car Network Security Platform Based on Blockchain

CUBE aims to provide security platform for autonomous vehicles based on blockchain technology as a solution to autonomous vehicles' security. Autonomous vehicles rely heavily on over-the-air wireless technology, which increases the risk of malicious attacks on autonomous vehicles [22]. CUBE focuses on a tool to secure over-the-air software updates or contents exchange. CUBE has developed over-the-air technology that enables remote software diagnostics, and installation and bug patches of existing automotive software based on blockchains of the Ethereum platform. The CUBE token links every blockchain-based service such as over-the-air services, driving-related data sharing, and insurance services.

An example of a CUBE token application is the linking of driving-related information from vehicles to data consumers who need driving information. The vehicle owners generate the driving information while driving the car, receiving CUBE tokens in return. CUBE digitizes this information and links it into a blockchain. Data consumers who need this information provide the services in exchange for CUBE tokens. When an automobile generates information, all nodes send, utilize, and receive it. Automobiles exchange their data as nodes, and the data consumers who

need this information provide various services and receive tokens. Information consumers such as automobile and insurance companies can pay providers for traffic information using CUBE tokens. CUBE is an imminent technology for commercialization; it applies blockchain to intelligent vehicle security and has a payment and reward system using cryptocurrency. Using a CUBE token, one can receive services at CUBE affiliates such as gas stations, car dealers, repair shops, and insurance companies, and affiliate companies can provide services such as discounts, vehicle maintenance, vehicle purchase discounts, insurance benefits, and cash-back services. CUBE announced that its autonomous vehicle security platform technology based on blockchain will be released in 2019. The key of the autonomous vehicle security platform is that technology ensures trust using blockchain. CUBE uses blockchain technology to ensure the security of autonomous wireless networks. CUBEs algorithm adopts the blockchain technology proposed by Dorri et al. [17], which is a multisig mechanism, without disclosing any private information of vehicles users to provide and update the wireless remote software and other emerging vehicles services.

3.3.4 Use Case of Solving Intersection Deadlock Problem for Autonomous Vehicles

Deadlock is the state in which no operation can progress. Autonomous vehicles negotiate the right-of-way before traversing each intersection without traffic signals (on a first-come first-served basis), because the car reaching the intersection first has passing priority. If four autonomous vehicles arrive at a four-way intersection almost simultaneously, none can proceed until determination of the priority, which results in the deadlock at intersections without traffic signals. A cooperative traffic management system may allow high performance at intersections; however, it may cause considerable maintenance costs or inefficiency because most intersections without traffic signals are placed in low-traffic regions. Kim and Singh proposed a trust point-based blockchain technology for intelligent vehicles, as well as a solution to the deadlock scenario [23]. As shown in Fig. 7, four vehicles, namely, IV-1, IV-2, IV-3, and IV-4 approach the intersection. When the vehicles are about to reach the intersection, they broadcast their signals. A consensus is made regarding the vehicle the earliest timestamp associated with the block and which should move first. Then, the same procedure is followed for the other three (possibly more) vehicles. Fig. 7 shows an example of an intersection scenario for IVs, where the arrival times of IV-1, IV-2, IV-3, and IV-4 at the intersection are 10:06, 10:02, 10:04, and 10:03, respectively. IV-2 crosses the intersection first, after consensus is reached.

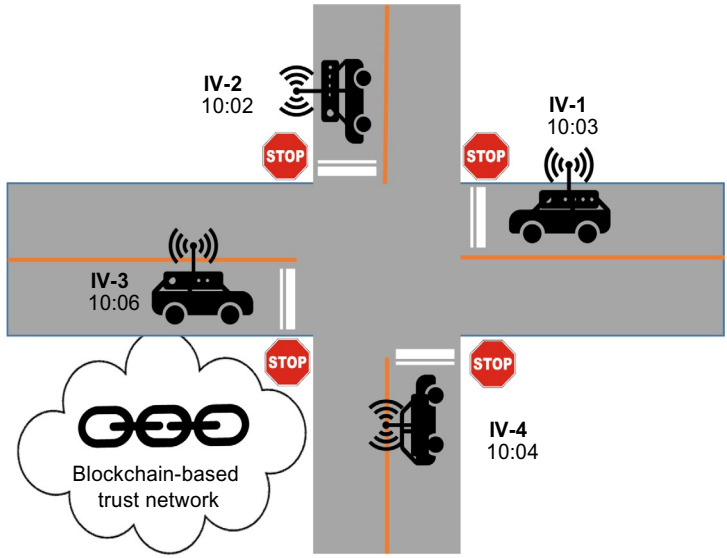

Fig. 7 Example of deadlock at traffic intersection without signals (on a first-come first-served basis) for autonomous vehicles.

4. CHALLENGES AND FUTURE RESEARCH DIRECTIONS OF BLOCKCHAIN IN INTELLIGENT VEHICLES

Blockchain technology is gaining momentum and creating new business opportunities both in the automotive and ICT industries to untangle the potential cybersecurity threat of intelligent connected vehicles; however, some challenges lie ahead.

While many applications are being experimented with in various fields, there remain some unsolved issues that prevent us from stating that blockchain technology has perfect integrity under any environmental condition of implementation.

The main challenge of blockchain consensus protocols such as Bitcoin, Ethereum, Ripple, and Tendermint is that every fully participating node in the network must process every transaction. Recall that every single node on the network processes every transaction and maintains a copy of the entire state. While a decentralization consensus mechanism offers some critical benefits, such as fault tolerance, and a strong guarantee of security, political neutrality, and authenticity, it comes at the cost of scalability.

4.1 Challenging Issue of Blockchain for Intelligent Vehicles

Blockchain technology is a breakthrough in cybersecurity, as it can ensure the highest level of data confidentiality, availability, and security. However, the complexity of the technology may cause difficulties with development and real-world use.

In order to bring the blockchain to intelligent connected vehicles, participants of the vehicle cloud need to overcome a number of technical challenges due to the limited capability of in-vehicle power and storage, and many other factors. Five main challenges are identified and explained as follows:

(a) *Scalability*: Scalability means the capability of the blockchain system to cope with and handle a growing amount of distributed ledger database. Scaling the blockchain is a known challenge and has been an active area of research for several years. Scalability is a primary concern of blockchain architecture for intelligent vehicles, because each vehicle has a limited amount of storage capacity and power budget to work for a mining node or distributed ledger. In the traditional blockchain mechanism, each node consumes a significant power for mining, and a data storage server is required to permanently store shared data of the distributed ledger, which is almost unable to implement in vehicle environment. One potential resolution is periodic backup of the in-vehicle data to external backup storage [17]. However, managing the ever-growing data size of the shared ledger may be burden in practical use cases.

Another solution for keeping the network lighter is the use of a decentralized storage service such as Swarm. Swarm is a peer-to-peer file sharing protocol for Ethereum that lets you store application code and data off the main blockchain (MB) in swarm nodes, which are connected to the Ethereum blockchain, and later exchange this data on the blockchain. The basic premise here is that instead of nodes storing everything on the blockchain, they only store data that is more frequently requested locally and leave other data on the "cloud" via Swarm.

As a result, all public blockchain consensus protocols that operate in such a decentralized manner make the tradeoff between low transaction throughput and high degree of centralization. In other words, as the size of the blockchain increases, the requirements for storage, bandwidth, and computing power required by fully participating in the network increases. At some point, it becomes sufficiently unwieldy that it is only feasible for a few nodes

to process a block—leading to the risk of centralization. To scale, the blockchain protocol must develop a mechanism to limit the number of participating nodes needed to validate each transaction, without losing the network's trust that each transaction is valid. It may sound simple, but is very difficult in a technological point of view.

Kim et al. proposed a branch-based blockchain composed of a local dynamic blockchain (LDB) and a MB enabled with intelligent vehicle trust point [24]. Fig. 8 shows the blockchain technology with Local Dynamic Block and Main Block for V2X communication proposed by Kim et al. LDB with circular queue architecture stores only local temporal data shared in local area. If data size exceeds the memory capacity of LDB, new incoming data are overwritten. If LDB receives any unusual event data (not a regular event), then it forwards it to MB for permanent storage. LDB can branch or merge depending on the amount of data traffic and the workload required to handle in real time. Fig. 9 shows branching and merging operation of a local dynamic blockchain. If a LDB branches, original LDB is divided into two child branches. Further, if two branches are merged, both parent branches must contain a block on the latest level.

(b) *Transaction speed and computing power:* To add a new transaction, consensus of among network participants must be recorded in the distributed ledger of the blockchain. However, the implemented blockchain consensus mechanism does not yet offer significant improvements to

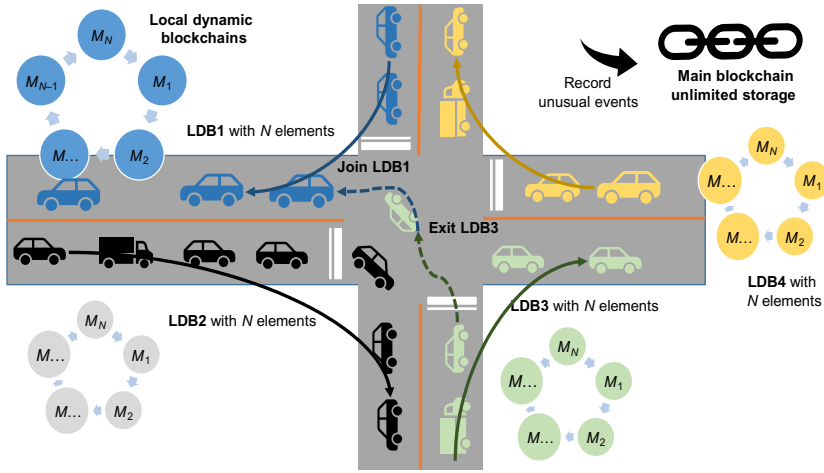

Fig. 8 Blockchain technology with local dynamic block and main block for V2X communication [24].

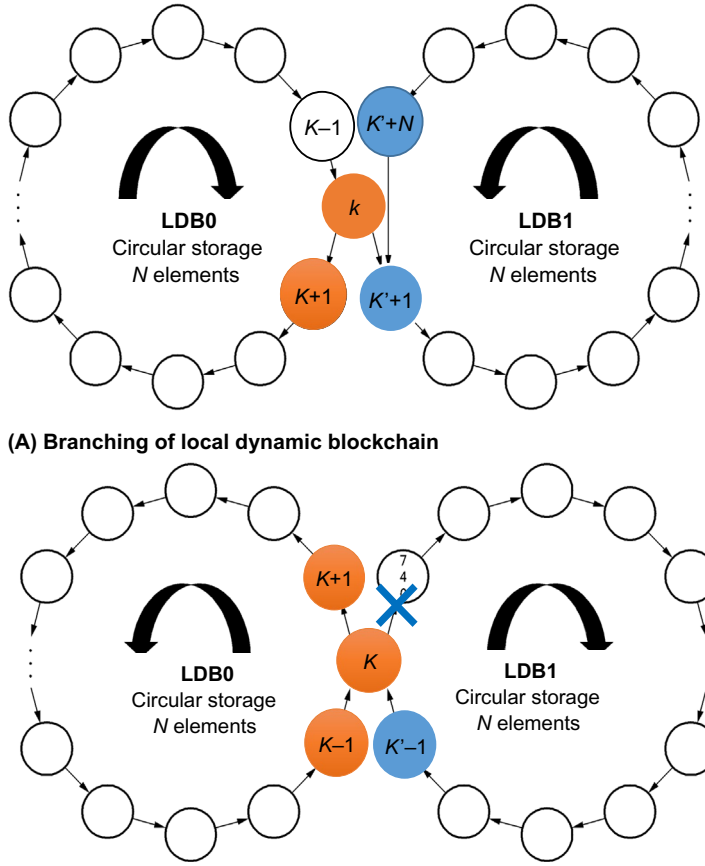

Fig. 9 Branching and merging operation of a local dynamic blockchain, where LDB0 splits at the *k*th element of the block to LDB1.

transaction speeds. In the case of commonly used algorithms, the period of consensus to encapsulate new block is 10 min for proof-of-work (for Bitcoin) and 17 s for proof-of-stake (for Ethereum). In contrast, the average confirmation time of Bitcoin is approximately 250 min; the longest time ever recorded, in February 2018, was more than 2500 min (approximately 42 h). These existing consensus algorithms of the blockchain are too slow for intelligent vehicles to record messages between vehicles in real time. Moreover, mining nodes consume considerable computing power. To resolve the barrier of speed and power budget, some new, innovative approaches have to be introduced to improve these essential blockchain characteristics.

An Ethereum node's maximum theoretical transaction processing capacity is over 1000 transactions per second. Unfortunately, this is not the actual throughput owing to Ethereum's "gas limit," which is currently approximately 6.7 million gas on average for each block [25]. Hence, the "gas limit" for each block determines how many transactions will fit in a block based on the gas limit specified by each transaction in the block. Similarly, Bitcoin, despite having a theoretical limit of 4000 transactions per second, currently has a hard cap of approximately seven transactions per second for small transactions and three per second for more complex transactions. Unfortunately, none of the solutions perfectly address the transaction speed and computing power problems.

Both of these solutions aim to solve the Bitcoin-specific issue where the Bitcoin blockchain has a built-in hard limit of 1 MB per block, which caps the number of transactions that can be added to a block. As a result, Bitcoin has been facing delays (sometimes hours and even days) in processing and confirming transactions for a while now. Similarly, as noted in the previous section, Ethereum also faces limitations in its ability to scale.

(c) *Confidentiality vs Transparency:* Despite great features of the blockchain technology, many regulators are being challenged by the type of data that should reside within the distributed ledge. Many people feel that encrypted information managed with public and private keys should support the confidential information being stored on the blockchain. In the decentralized model, all parties share information. No private contractual data should be stored on a distributed ledger, encrypted, or otherwise. Shared ledgers should contain the bare minimum information, interpretable only by those with a need and right to know, to permit notification, synchronization, and confirmation. For confidentiality, confidential and sensitive data should reside on a blockchain as it provides an extra layer of security with immutable records.

(d) *Privacy:* From a security perspective, researchers developed various techniques targeting privacy concerns focused on personal data. Data anonymization methods attempt to protect personally identifiable information. Recent research has demonstrated how anonymized datasets employing these techniques can be deanonymized [2], given even a small amount of data points or high dimensionality data.

Although we often use the terms "confidentiality" and "privacy" interchangeably in our daily lives, they are distinct terms from a legal standpoint. We generally use the term confidentiality in the context of protecting data (e.g., transaction details, account and wallet balances, and contents

of a contract) from unauthorized third parties. We use the term privacy to refer to protection from intrusion into the identity of blockchain participants and parties to transactions.

- Data Ownership: It focuses on ensuring that users own and control their personal data. As such, the system recognizes the users as the owners of the data and the services as guests with delegated permissions.
- Data Transparency and Auditability: Each user has complete transparency over the data collected and how they are accessed.

(e) *Locality of ground transportation/cyberspace is globally synchronized:* Seamless integration of local vehicular networks and globally distributed storage platform pose numerous challenges since all these building blocks are heterogeneous in terms of their dependencies on infrastructure and software elements. Ground transportation is localized, but blockchain is a global cyberspace. Local transactions do not need to be shared on the globally distributed ledger, which may reduce unnecessary data traffic. The problem of locality and globally synchronized ledger can be solved by focusing on data centric aspects of vehicular communication networks. The detection of the abnormality of cyberattacks for other regions by proof of driving is a potential solution.

Although blockchain technology can be applied to almost any business, intelligent vehicle industry may face difficulties integrating it. It is quite challenging to employ this technology in vehicle cloud systems, for instance, as it may be time-consuming to replicate vehicle network as blockchains and refine them. Blockchain applications can also require the complete replacement of existing systems; thus, business parties should consider this before implementing blockchain technology.

KEY TERMINOLOGY AND DEFINITIONS

Consensus in Blockchain It means decision-making among participant nodes: For a transaction to be valid, all participants must agree on the validity of a predefined algorithm or rule, such as proof-of-work, proof-of-stake, proof-of-concept, or else. The consensus involves conducting two key crucial functions of the blockchain technology. First, consensus protocols allow newly generated data block to be appended to a distributed Ledger, while ensuring that every block in the chain is truly valid and keeping participants incentivized to do mining. It prevents malicious hackers controlling or breaking down the blockchain system. Second, the consensus rule guarantees that a single blockchain keeps growing and is followed.

Cybersecurity Cyber security is defined as the protection of systems, networks, and data in cyberspace and is a critical issue for all businesses. Cybersecurity, computer security, or IT security is the protection of computer systems from the theft and damage to their hardware, software, or information, as well as from disruption or misdirection of the services

they provide. Cybersecurity includes controlling physical access to the hardware, as well as protecting against harm that may be caused as a result of network access, data, and code injection. In the vehicle networks, safety, security, and privacy are key issues of the protection of computerized networks from the theft and damage to their hardware, software, or information, as well as from disruption or misdirection of the services they provide.

Intelligent and Connected Vehicles Vehicles which are controlled by a complex computer with connectivity of both the in-vehicle network and wireless communication network. Autonomous vehicle is a state-of-the-art of system where actuation and decision-making maneuvers operate concurrently with coping with environmental information coming from sensors and communication networks during driving. The intelligent vehicles will be connected to almost everything, they have become a part of the internet of things.

Scalability Scalability is the capability of a system, network, or process to handle an increasing amount of work, or its potential to be enlarged to accommodate this growth. Scalability is a characteristic of a system, model, or function that describes its capability to cope and perform under an increased or expanding workload. A system that scales well is able to maintain or even increase its level of performance or efficiency when tested by larger operational demands.

Trust Network Among Intelligent Vehicles This is a networking environment that is secured against malicious cyberattacks on V2V, V2X communication, and vehicular cloud networks.

REFERENCES

[1] E.B. Hamida, K.L. Brousmiche, H. Levard, E. Thea, in: Blockchain for enterprise: overview, opportunities and challenges, International Conference on Wireless and Mobile Communications, 2017.
[2] G. Zyskind, O. Nathan, in: Decentralizing privacy: using blockchain to protect personal data, IEEE Security and Privacy Workshops, 2015, pp. 180–184.
[3] Z. Zheng, S. Xie, H.N. Dai, H. Wang, Blockchain challenges and opportunities: a survey, Int. J. Web Grid Serv. (2016).
[4] N. Kshetri, Blockchain's roles in strengthening cybersecurity and protecting privacy, Telecommun. Policy 41 (2017) 1027–1038.
[5] C. Mauro, C. Lal, S. Ruj, A Survey on Security and Privacy Issues of Bitcoin, arXiv:1706.00916, 2017.
[6] A.G. Simpson "Toyota, MIT Lab Eye Using Blockchain in Insurance Rating of Driverless and Shared Vehicles" https://www.insurancejournal.com/author/andrew-simpson, last visited March 2018.
[7] A. Papathanassiou, A. Khoryaev, Cellular V2X as the essential enabler of superior global connected transportation services, IEEE 5G Tech Focus 1 (2) (2017).
[8] Connected Vehicle Cloud—Under the Road, Ericsson, www.ericsson.com.
[9] S.K. Datta, R.P.F. Da Costa, J. Härri, C. Bonnet, in: Integrating connected vehicles in internet of things ecosystems: challenges and solutions, IEEE International Symposium on World of Wireless, Mobile and Multimedia Networks, 2016, pp. 1–6.
[10] M. Singh, S. Kim, Safety Requirement Specifications for Connected Vehicles, arXiv:1707.08715, 2017.
[11] J.H. Park, J.H. Park, Blockchain security in cloud computing: use cases, challenges, and solutions, Symmetry 9 (8) (2017) 164.

[12] P.K. Sharma, S.Y. Moon, J.H. Park, Block-VN: a distributed blockchain based vehicular network architecture in smart city, J. Inf. Process. Syst. 13 (1) (2017) 184–195.
[13] C. Cachin, M. Vukolic, Blockchain Consensus Protocols in the Wild, arXiv:1707.01873, 2017.
[14] C. Xu, K. Wang, M. Guo, Intelligent resource management in blockchain-based cloud datacenters, IEEE Cloud Comput. 4 (6) (2017) 50–59.
[15] Y. Yuan, F. Wang, in: Towards blockchain-based intelligent transportation systems, IEEE International Conference on Intelligent Transportation Systems (ITSC), 2016, pp. 2663–2668.
[16] B. Leiding, P. Memarmoshrefi, D. Hogrefe, in: Self-managed and blockchain-based vehicular ad-hoc networks, Proceedings of the ACM International Joint Conference on Pervasive and Ubiquitous Computing, 2016, pp. 137–140.
[17] A. Dorri, M. Steger, S.S. Kanhere, R. Jurdak, Blockchain: a distributed solution to automotive security and privacy, IEEE Commun. Mag. 55 (12) (2017) 119–125.
[18] S. Rowan, M. Clear, M. Gerla, M. Huggard, C. Mc Goldrick, Securing Vehicle to Vehicle Communications Using Blockchain Through Visible Light and Acoustic Side-Channels, arXiv:1704.02553, 2017.
[19] "Toyota's Vision of How Blockchain Will Change the Auto Industry", http://www.thebanksreport.com, last visited March 2018.
[20] Jen Clark, "ZF, UBS and IBM Bring Blockchain to In-Vehicle Payments", www.ibm.com/blogs/internet-of-things/zf-ubs-ibm-vehicle-payments/ last visited March (2018).
[21] R. Xu, L. Zhang, H. Zhao, Y. Peng, in: Design of network media's digital rights management scheme based on blockchain technology, IEEE International Symposium on Autonomous Decentralized Systems, 2017, pp. 128–133.
[22] CUBE, Autonomous Car Network Security Platform Based on Blockchain, White Paper, Cube, 2017.
[23] M. Singh, S. Kim, Intelligent Vehicle-Trust Point: Reward Based Intelligent Vehicle Communication Using Blockchain, arXiv:1707.07442, 2017.
[24] M. Singh, S. Kim, Blockchain Based Intelligent Vehicle Data Sharing Framework, arXiv:1708.09721, 2017.
[25] K. Croman, C. Decker, I. Eyal, A.E. Gencer, A. Juels, A. Kosba, A. Miller, P. Saxena, E. Shi, E.G. Sirer, D. Song, R. Wattenhofer, On scaling decentralized blockchains, in: International Conference on Financial Cryptography and Data Security (FC 2016), Lecture Notes in Computer Science, 9604, 2016, pp. 106–125.

FURTHER READING/REFERENCES FOR ADVANCE

[26] A. Lei, H. Cruickshank, Y. Cao, P. Asuquo, C.P.A. Ogah, Z. Sun, Blockchain-based dynamic key management for heterogeneous intelligent transportation systems, IEEE Internet Things J. 4 (6) (2017) 1832–1843.
[27] M. Gupta, Blockchain for Dummies, John Wiley & Sons, 2017.
[28] P. Fairley, Special report: blockchain world, IEEE Spectr. (2017) 24–56.
[29] M. Niforos, V. Ramachandran, T. Rehermann, BLOCKCHAIN-Opportunities for Private Enterprises in Emerging Markets, IFC (International Finance Corporation), 2017.
[30] J. Sun, J. Yan, K. Zhang, Blockchain-based sharing services: what blockchain technology can contribute to smart cities, Financ. Innov. 2 (2016) 26.
[31] Consensus—Immutable Agreement for the Internet of Value, kpmg.com/socialmedia, 2016.
[32] K. Toyoda, P. Mathiopoulos, I. Sasase, T. Ohtsuki, A novel blockchain-based product ownership management system (POMS) for anti-counterfeits in the post supply chain, IEEE Access 5 (2017) 17465–17477.

[33] T.D. Smith, in: The blockchain litmus test, IEEE International Conference on Big Data (Big Data), 2017, pp. 2299–2308.
[34] D. Yang, J. Gavigan, Z. Wilcox-O'Hearn, Survey of Confidentiality and Privacy Preserving Technologies for Blockchains, R3 Research Report, 2016.
[35] J.M. Easton, Blockchains: a distributed data ledger for the rail industry, in: Innovative Applications of Big Data in the Railway Industry, IGI Global, 2017, ISBN13: 9781522531760, pp 27–39.
[36] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, S. Uluagac, Block4Forensic: An Integrated Lightweight Blockchain Framework for Forensics Applications of Connected Vehicles, arXiv:1802.00561, 2018.

ABOUT THE AUTHOR

Shiho Kim is a professor in the school of integrated technology at Yonsei University, Seoul, Korea. His previous assignments include, being a System on chip design engineer, at LG Semicon Ltd. (currently SK Hynix), Korea, Seoul [1995–1996], Director of RAVERS (Research center for Advanced hybrid electric Vehicle Energy Recovery System), a government-supported IT research center. Associate Director of the Yonsei Institute of Convergence Technology (YICT) performing Korean National ICT consilience program, which is a Korea National program for cultivating talented engineers in the field of information and communication Technology, Korea [2011 – 2012], Director of Seamless Transportation Lab, at Yonsei University, Korea [since 2011 to present].

His main research interest includes the development of software and hardware technologies for intelligent vehicles, blockchain technology for intelligent transportation systems, and reinforcement learning for autonomous vehicles. He is a member of the editorial board and reviewer for various Journals and International conferences. So far he has organized two International Conference as Technical Chair/General Chair. He is a member of IEIE (Institute of Electronics and Information Engineers of Korea), KSAE (Korean Society of Automotive Engineers), vice president of KINGC (Korean Institute of Next Generation Computing), and a senior member of IEEE. He is the coauthor for over 100 papers and holding more than 50 patents in the field of information and communication technology.