Towards Robust & Secure Blockchain-based Communications in ITS

Atsuki Yoshimura, Yan Chen, Jin Nakazato, *Members, IEEE*,
Tarik Taleb, *Senior Member, IEEE*, Manabu Tsukada, Hiroshi Esaki, *Member, IEEE*,

***Abstract*—In Intelligent Transportation Systems (ITS), the limited perception range of individual connected autonomous vehicles (CAVs) necessitates the collaborative utilization of information detected by nearby vehicles and roadside units (RSUs) to achieve accurate environmental perception and awareness, which relies on reliable data transmission among involved entities. Blockchain technology has been widely recognized for its effectiveness in ensuring secure and trustworthy data exchanges, with its importance rapidly increasing across various industries. However, traditional blockchain approaches have not fully addressed the dynamic mobility of CAVs or the efficient coordination among multiple RSUs within ITS scenarios. To address these challenges, this paper proposes an Integrated Membership Management Unit (IMMU) system utilizing blockchain technology to facilitate secure vehicle-to-infrastructure (V2I) communication among multiple CAVs and RSUs. This approach enables RSUs to cooperate effectively and uses reinforcement learning to achieve optimal load balancing. The performance and effectiveness of our proposed approach have been thoroughly evaluated through an end-to-end simulation.**

***Index Terms*—V2X, ITS, blockchain, trust, security, reinforcement learning, and robust communication.**

I. Introduction

SINCE its global commercialization, the fifth-generation (5G) mobile communication system has continuously driven innovations towards next-generation services, such as augmented reality/virtual reality (AR/VR) and autonomous driving (AD) [1], leveraging its capabilities in ultra-high-speed and high-capacity communication (eMBB), ultra-reliable and low-latency communication (URLLC), and massive machine-type communication (mMTC) [2]. Furthermore, the research and development for sixth-generation (6G) mobile communication systems are actively progressing globally under leading organizations such as International Telecommunication Union–Radiocommunication Sector (ITU-R) and 3rd Generation Partnership Project (3GPP). For example, China Mobile initiated the commercial deployment of 5G-Advanced in 2024 [3]. To secure industrial leadership in 5G and 6G technologies, the European Union established the Smart Networks and Services Joint Undertaking funding initiative, which seeks to strengthen Europe's technological sovereignty in 6G development, while expediting the deployment of 5G infrastructure across the continent [4]. In May 2024, 3GPP Technical Specification Group Service and System Aspects Working Group 1 organized a workshop inviting leading global research organizations to share insights on regional priorities, use cases, and key technological enablers for 6G standardization [5]. AD was reaffirmed as a priority use case by major stakeholders [6].

Traffic accidents remain a significant public safety challenges, causing approximately 40,000 annual fatalities in the United States as reported by the National Highway Traffic Safety Administration [7]. Beyond the devastating loss of life, the economic burden is substantial. Hallegatte et al. [8] estimated that reducing traffic accidents by one million annually could generate savings of approximately $26 billion, highlighting the immense financial and societal benefits of improving road safety. Intelligent Transportation Systems (ITS) can enhance public transportation safety through real-time monitoring and predictive responses, with vehicle-to-everything (V2X) communication as a core enabler, ensuring seamless interaction between connected autonomous vehicles (CAVs), infrastructure, and pedestrians to improve situational awareness and prevent accidents [9], [10]. With V2X technology, CAVs can share real-time information regarding traffic conditions and the road environment with surrounding vehicles, infrastructure, and pedestrians, which can significantly improve safety and reduce traffic congestion [11], [12].

V2X communication enables the exchange of critical and sensitive information between CAVs, roadside units (RSUs), and pedestrians, making the authenticity, integrity, and confidentiality of the data paramount [13]. However, the dynamic and distributed nature of V2X networks increases their vulnerability to cyberattacks such as message tampering, spoofing, and denial-of-service attacks. Blockchain technology offers a compelling solution owing to its decentralized architecture, immutability, and cryptographic security, providing a robust framework for trust and data protection. Integrating the blockchain into V2X enhances security, ensures tamper-proof

This work was partly supported by the JST ASPIRE project under Grant JPMJAP2325; in part by International Exchange Program of National Institute of Information and Communications (NICT); in part by the European Union through the 6G-Path project under Grant 101139172 and the 6GSandbox project under Grant 101096328.(*Corresponding author: Yan Chen, Jin Nakazato, Hiroshi Esaki*)

Atsuki Yoshimura, Manabu Tsukada, and Hiroshi Esaki are with the Graduate School of Information Science and Technology, The University of Tokyo, 1–1–1, Yayoi, Bunkyo-ku, Tokyo, 152–8657 Japan (e-mail: yoshimura0230@gmail.com, mtsukada@g.ecc.u-tokyo.ac.jp, hiroshi@wide.ad.jp).

Jin Nakazato is with the Department of Electrical Engineering, Faculty of Engineering, Tokyo University of Science, Tokyo, Japan. (e-mail: jin.nakazato@ieee.org).

Yan Chen and Tarik Taleb are with the Faculty of Electrical Engineering and Information Technology, Ruhr University Bochum, 44801 Bochum, Germany (e-mail: yanchen@ieee.org, tarik.taleb@ruhr-uni-bochum.de).

Fig. 1. Illustration of Blockchain application in V2X networks.

data storage, and facilitates reliable identity management. Its transparency supports cooperative perception, decision making, and accurate evidence preservation, further strengthening V2X functionality. Fig. 1 provides an overview of blockchain applications in V2X, demonstrating their potential to address current limitations and foster the development of ITS. Despite their potential, most existing blockchain applications have concentrated on cryptocurrencies and financial services. Recently, blockchain has attracted substantial attention in the V2X domain, where it serves as an enabler for a wide range of innovative applications. For instance, blockchain-based payment systems like ParkRes [14] enable drivers to securely locate and reserve parking spaces. Moreover, blockchain facilitates micropayments in data marketplaces, supporting transactions as small as a cent [15]. Smart contracts further facilitate advanced mechanisms, including dynamic pricing for Electric Vehicle charging [16]. Within V2X, these blockchain-powered services improve payments, incentivization, reputation management, authentication, and forensic capabilities.

One notable study is V-Guard [17], which applied blockchain to V2X communication to improve reliability and evidence preservation. Nevertheless, V-Guard lacks support for real-world mobility scenarios and has not examined realistic environments involving multiple blockchains, along with the challenges posed by their simultaneous deployment.

To address these challenges, this study proposes a robust Integrated Membership Management Unit (IMMU) architecture that leverages blockchain and achieves coordination of multiple RSUs in mobility environments. The proposed IMMU architecture designates RSUs as proposers and vehicles as validators, enabling vehicles to participate in consensus formation, either within the nearest blockchain or across different RSUs. Additionally, the proposed IMMU architecture incorporates reinforcement learning features to optimize the assignment of participant nodes during consensus processes. These enhancements are incorporated into V-Guard, referred to here as Enhanced V-Guard. Our previous study has connected V-Guard to Artery [18] for simplified verification in a single RSU vehicle-to-infrastructure (V2I) scenario [19]. The only contribution of our previous study was the integration of simulations; multiple roadside units and IMMUs were not considered. The main contributions are summarized as follows.

- We propose a robust IMMU architecture utilizing blockchain in highly dynamic V2X environments. The IMMU accommodates multiple RSUs, defines roles for RSUs as proposers and vehicles as validators, and enables consensus formation for each RSU's blockchain. Additionally, the IMMU enables tracking of the blockchain, even when the vehicle transitions between different RSUs during movement, thereby ensuring a high probability of successful consensus formation. This capability effectively addresses the mobility challenges.
- We address handover challenges during blockchain consensus formation by leveraging reinforcement learning to optimize participant node assignment, which improves load balancing and connection accuracy for vehicles in dynamic and randomly moving environments.
- We validate the proposed IMMU framework by implementing a comprehensive simulation environment integrated with Artery platforms, enabling end-to-end evaluation of V2X blockchain systems. Extensive experiments involving multiple RSUs and test vehicles in realistic scenarios are conducted, and results demonstrate the effectiveness of the proposed approaches in optimizing consensus formation within dynamic V2X environments.

The remainder of this paper is organized as follows. Section II introduces related work and outlines the challenges of integrating blockchain with V2X communication. Section III explains the proposed solutions. Section V details the integration of existing simulators with the Artery traffic simulator and evaluates the system performance. Finally, Section VI concludes this paper.

II. Related Works

This section reviews some related studies on the application of blockchain to V2X, highlighting the challenges and limitations of existing approaches.

A. The Need of Blockchain for V2X

In ITS environments, Sybil attacks [20], constitute a critical security threatwherein malicious actors infiltrate the system through multiple fabricated identities (IDs) to propagate false information and compromise the decision-making processes of neighboring vehicles [21]. Implementing a robust reputation mechanism is essential for preventing the dissemination of false data among vehicles in V2X systems. Reputation pertains to the perception of an entity's actions by others and functions as a critical mechanism for evaluating the trustworthiness of a given identity and distinguishing it from potentially malicious actors. The traceability and immutability inherent in blockchain are significant advantages for reputation management, prompting the proposal of various blockchain systems [22]. In a blockchain-based reputation-tracking system, when one vehicle rates another, rating information is recorded on the blockchain. By tracking this rating information, we can verify whether the vehicle is a reliable source of information. Systems that handle sensitive data, such as vehicle location data, require strong authentication protocols that can be achieved using blockchain-based identity and

reputation frameworks. A notable example is the Blockchain-based Privacy-Preserving Authentication Scheme, which has been proposed for Vehicular Ad hoc Network (VANET), which not only ensures the accuracy and reliability of messages exchanged within a VANET, but also protects the privacy of involved vehicles [23].

Furthermore, in the event of an accident, it is crucial to accurately preserve information regarding the vehicle and its surrounding environment for subsequent investigative purposes. The immutability and timestamp features of blockchains can substantially enhance the reliability and accuracy of digital forensics in the context of vehicles investigation [24]. A blockchain-based intelligent digital forensic system has been proposed and implemented on a local Ethereum platform to safeguard the security and privacy of CAVs equipped with autonomous driving technology and network connectivity capabilities [25]. When data are stored on a blockchain, all participating nodes must maintain the information in their databases, rendering it currently infeasible to store the massive amounts of data generated by V2X systems on a blockchain. In such cases, only the hashes of large data files, such as videos from onboard cameras, can be stored [26].

Building on these motivations, this study explored the application of blockchain technology to V2X systems and proposed the implementation of an IMMU architecture capable of adapting to vehicle mobility.

B. The Challenges of Blockchain in V2X: Member Change and Load Balancing Issues

Applying blockchain to V2X systems presents several challenges, including the member change problem and the load balancing problem. First, the member-change problem involves dealing with a permissioned blockchain. A permissioned blockchain is a type of blockchain in which only nodes with known identities approved by an administrator can participate in consensus. Practical Byzantine Fault Tolerance (PBFT) [27] is a popular mechanism for consensus in permissive blockchains. It operates as a majority voting model, enabling consensus to be reached even in the presence of malicious participants who submit false information as long as their number remains below a predefined threshold. Nevertheless, PBFT suffers from a fundamental scalability constraint wherein network reconfiguration events trigger mandatory system interruptions. Since the protocol requires global awareness of participant count among all nodes, any membership modification necessitates temporary system suspension and broadcast dissemination of updated network parameters to ensure consensus integrity. This process can result in frequent system interruptions and performance degradation, particularly in V2X environments where vehicles are constantly moving and blockchain nodes change frequently. Linear BFT attains $O(n)$ communication by compressing $3f+1$ replica votes into a constant-size quorum certificate via threshold signatures, eliminating PBFT's all-to-all exchanges [28]. However, this linearity does not inherently solve the member-change issue: the protocol assumes a fixed replica set within each configuration/epoch, so adding or removing nodes still requires a reconfiguration agreed through consensus, which is ill-suited to highly dynamic V2X membership. Mempools based on Directed Acyclic Graph (DAG), such as Narwhal, separate transaction dissemination from ordering: batches are disseminated in a DAG, and the BFT layer orders only their digests [29]. It does not address dynamic membership: the validator set is fixed within a configuration/epoch, so adding or removing nodes requires a reconfiguration agreed through consensus. A solution to this member update problem was proposed using V-Guard [17], comprising a single proposer node and multiple validator nodes. The Membership Management Unit (MMU) within the proposer node is responsible for managing membership, aggregating validation success messages, and embedding membership information into the transactions. By centralizing membership management within the proposer node, the proposed MMU eliminates the need for the synchronization of membership information across nodes with each update, thereby enabling the system to handle dynamic node changes flexibly without interruption. However, there are unaddressed challenges in V-Guard, particularly regarding the V2V scenario and the conditions of other vehicles within the communication range. Specifically, V-Guard is limited to V2V, whereas V2I has not been considered. Furthermore, the issues of mobile communication and the logic of whether communication is possible have not yet been considered. This study addresses these challenges by proposing an architecture capable of handling member changes and a method that allows flexible node changes without stopping the system.

In addition to member changes, load balancing is critical in V2X systems due to the limited computing resources of vehicles and RSUs. When the computation is concentrated on specific nodes, the overall efficiency may degrade, leading to slow processing and potential bottlenecks. This issue is exacerbated in dynamic V2X environments, where uneven load distribution affects the system performance, scalability, and responsiveness. An effective load-balancing mechanism that dynamically redistributes tasks across nodes is essential for optimizing resource utilization and maintaining system stability. Therefore, approaches have been proposed by leveraging the stable matching theory to maximize the efficiency of task offloading within the edge network while ensuring privacy protection [30] and game theory to form computing clusters within the network, allowing vehicles with low computational power to offload computational tasks to the cluster [31]. Most of the existing research on V2X load balancing focuses on permissionless blockchains, with limited attention given to permissioned blockchains. To address this gap, this paper proposes a method specifically designed to solve the load-balancing problem in permissioned blockchain environments.

A comparision of existing Blockchain technologies in V2X is detailed in Table I. We can conclude that V-Guard provides advantages in lower message complexity and higher consensus throughput. Moreover, it achieves higher reliability, as the system operates seamlessly without interruption when nodes join or leave. Therefore, we select V-Guard as the cornerstone of our proposed architecture and address its limitations when implementing it in V2X environments.

TABLE I
BLOCKCHAIN TECHNOLOGIES IN V2X

Items	**PBFT** [32]	**Linear BFT [28]**	**DAG-based mempool [29] + BFT**	**V-Guard** [17]
Message Complexity	O(n^2)	O(n)	O(n)	O(n)
Consensus Interruption	✓	✓	✓	-
Consensus Throughput	small	medium	large	large
Representative Example	ResilientDB	HotStuff	Narwhal	-

C. Blockchain meets V2X and AI

Blockchain offers various advantages such as transparency and immutability, which can complement artifical intelligence (AI) to enhance its capabilities [33]. For instance, blockchain provides a decentralized framework with an immutable audit trail, enabling AI to leverage reliable data models and training processes [34]. AI can analyze frequency variations, load changes, and anomalies in industrial control, whereas blockchain can track and automate these processes [35], [36]. A decentralized measurement system based on blockchain was proposed to replace traditional energy meters [37]. Moreover, AI can address some limitations of blockchain [38], such as improving the energy efficiency of mining in permissionless blockchains [39]. Additionally, federated learning can tackle the requirement of scalability in the blockchain and further enhance its security.

Research on AI for network optimization has progressed substantially, with approaches using machine learning [40] and deep reinforcement learning [41]–[44] to accomplish diverse objectives such as load balancing, service migration, Quality of Experience (QoE) optimization, resource allocation, and data privacy. These approaches have been widely applied in various edge-enabled systems, including V2X networks, to enhance efficiency and performance by tackling fundamental challenges inherent in modern communication systems, including network dynamics, environmental heterogeneity, and partial observability constraints. However, most of these studies have focused on permissionless blockchains. In practical V2X systems, the presence of untrusted vehicles and RSUs often necessitates the use of permissionless blockchains. However, this approach has drawbacks, including a slow processing speed and significant energy consumption.

Therefore, high-speed and low-latency Permissioned Blockchains are more suitable for handling data that require real-time performance, such as CAVs. This study leverages AI methods to explore approaches for task offloading in V2X systems that integrate Permissioned Blockchains.

III. PROPOSED SYSTEM ARCHITECTURE

In this section, we introduce the proposed system architecture and describe its components.

A. Overview of the Proposed Architecture

The proposed system targets cooperative cognition, utilizing sensors and communication equipment installed at cooperative infrastructure sites to enable infrastructure-based vehicle recognition and information processing. Therefore, we focus on V2I communication scenario. In this context, we assume a permissioned blockchain built on RSUs and CAVs. A single RSU is designated as the proposer, with multiple CAVs capable of communicating with the RSU serving as validators to construct a blockchain. To ensure reliability and accommodate system capacity requirements, we employ V-Guard as the foundation for constructing blockchain in the investigated V2X system. However,, V-Guard allows the proposer (i.e., RSU) to unilaterally decide the participating nodes (validators) of the blockchain at each consensus [17]. This presents a challenge in V2X system: *if a validator moves out of the communication range of the proposer during consensus, it becomes unable to communicate further and cannot receive the results of the consensus in which it participated.*

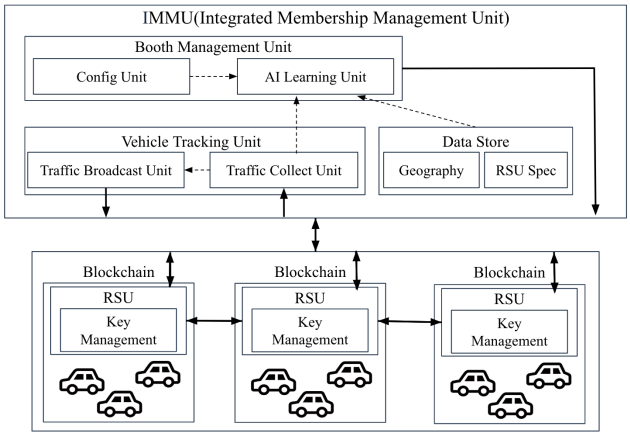


Fig. 2. The proposed IMMU architecture.

To address this challenge, we propose an IMMU architecture (Fig. 2) that enables RSUs (i.e., proposers) to collaboratively select their optimal validators (i.e., CAVs), solving the vehicle mobility problem. Specifically, RSUs are interconnected with the management center, where the IMMU is deployed, through high-bandwidth wired links such as optical fiber, facilitating efficient and low-latency data exchange. The IMMU communicates with every maintained RSU to collect information about the CAVs within their communication range. It shall be noted that each CAV can communicate directly with only one RSU in the system at any time instant, depending on its real-time position. The IMMU then centrally manages the selection of CAVs for each blockchain based on the collected information. The real-time status information of each CAV is broadcast in the form of Cooperative Awareness Messages (CAMs), as specified by European Telecommunications Standards Institute (ETSI) [45], to surrounding V2X entities within its communication range. This information is subsequently acquired by the IMMU and RSUs acting as proposers to support consensus decisions and operations.

Through the proposed IMMU architecture, two key benefits can be achieved to enhance the robustness of ITS in terms of data transmission. The first benefit is that it addresses the issue of changes in blockchain consensus formation due to vehicle movement. For example, consider a scenario in which proposer RSU#1 and CAV X are part of blockchain A and proposer RSU#2 is part of blockchain B. During the consensus process of blockchain A, if CAV X moves from the service area of proposer RSU#1 to that of proposer RSU#2, proposer RSU#1 will inquire the IMMU as soon as it detects the loss of communication with vehicle X. If it is confirmed that vehicle X is in the area of proposer RSU#2, communication with vehicle X can be maintained through the relay of proposer RSU#2. This ensures uninterrupted communication with the vehicle through consensus.

The second benefit is that it helps mitigate the issue of load concentration by allowing CAVs to be allocated to the blockchain established by a remote RSU, rather than the directly associated one, thereby preventing an RSU overload. For example, suppose there are 10 CAVs with proposer RSU#1 in blockchain A and 50 CAVs with proposer RSU#2 in blockchain B. As the number of participating nodes (vehicles) increased, the time required for consensus formation per blockchain block also increased. Therefore, it is necessary to balance the number of participating nodes in each blockchain to reduce load. Through the IMMU, 20 CAVs from blockchain B can be allocated as participating nodes for blockchain A and relayed by proposer RSU#2 to proposer RSU#1. This reallocation balances the number of vehicles in blockchains A and B, reducing the risk of prolonged consensus times in blockchain B and improving overall system efficiency.

Therefore, the proposed IMMU architecture allows for cooperation among multiple proposer RSUs to solve the aforementioned challenges.

B. Design of the proposed IMMU system

To ensure effective IMMU operation in multi-RSU, multi-CAV environments, the following requirements must be met to address the challenges of member change and load balancing:

- IMMU must establish connections with all RSUs and must maintain high-speed communication with them to ensure efficient information gathering and data exchange.
- IMMU shall continuously collect state information from CAVs associated with the respective RSUs and respond to requests for environment information from any RSU.
- IMMU shall be able to dynamically optimize blockchain member assignments based on CAV state information collected from RSUs.
- IMMU must be aware of the edge environment constructed by all RSUs and CAVs, as well as the processing specifications (e.g., computation resources, current resource usage) of each RSU.

Additionally, as a prerequisite to meeting the above requirements, vehicles must be able to connect to any RSU through wireless communication, and neighboring RSUs can communicate among themselves through established wired or wireless links. In wireless links, V2X communications have been widely explored, resulting in a variety of technologies and solutions tailored to support ITS, such as Dedicated Short-Range Communications (DSRC), Cellular V2X/Long Term Evolution V2X (C-V2X/LTE-V2X), Fifth Generation New Radio V2X (5G NR-V2X), and millimeter-wave V2X. In this paper, we employ IEEE 802.11p [46] to support V2I communication. As summarized in Table II, IEEE 802.11p operates in the 5.9 GHz ITS band and supports direct communication with low latency and decentralized management. These features make it particularly suitable for real-time vehicular environments where infrastructure-based connectivity is essential but cellular coverage may be limited or unnecessary. The choice of IEEE 802.11p aligns with our focus on RSU-centric consensus formation, as it enables RSUs to directly broadcast consensus results and membership information to nearby vehicles without relying on centralized cellular infrastructure. Moreover, since our proposed IMMU architecture emphasizes local collaboration among adjacent RSUs, the use of DSRC facilitates rapid and reliable data dissemination within the RSU's communication range.

As depicted in Fig. 2, the developed IMMU consists of three main components: a Data Store, Vehicle Tracking Unit, and Booth Management Unit. The Data Store contains two functions: Geography, which holds the geographical information of the RSU locations, and RSU Spec, which retains each RSU's specifications. The Vehicle Tracking Unit communicates with RSUs to collect and distribute information of road and CAVs. This unit comprises two functional units: the Traffic Collect Unit and the Traffic Broadcast Unit. The Traffic Collect Unit periodically collects information about the communication associations between CAVs and RSUs. Then, the Traffic Broadcast Unit responds to inquiries from remote RSUs about: *which RSU's communication range a certain vehicle is within*. Based on the information obtained by the Traffic Collect Unit, it returns the corresponding RSU number. This allows each RSU to identify the association between the RSUs and target vehicle, allowing it to maintain uninterrupted communication through the corresponding RSU. Furthermore, the Booth Management Unit is deployed with policies to determine the optimal vehicle assignment to the blockchain based on vehicle information obtained from the Vehicle Tracking Unit. In this study, this optimized assignment was achieved through the application of reinforcement learning models deployed within the AI Learning Unit. Specifically, the vehicle information from the Vehicle Tracking Unit, along with the RSU specifications and location from the Data Store, as well as other geographical information, is used to dynamically assign vehicles for consensus formation in the RSU's blockchain. The Config Unit saves information such as the internal weights of various reinforcement learning models. Because the optimal reinforcement learning model may dynamically change due to various environmental factors such as the amount of data stored in the blockchain, the Config Unit adjusts the AI Learning Unit model accordingly.

C. Establishment of Communication

By utilizing the IMMU's Vehicle Tracking Unit, connections between RSUs and CAVs that are not directly associated

TABLE II
COMPARISON OF EXISTING V2X COMMUNICATION TECHNOLOGIES

Technology	Description	Communication Type	Key Features / Considerations
IEEE 802.11p (DSRC) [46]	Wi-Fi-based standard operating in the 5.9 GHz ITS band (e.g., 5.850–5.925 GHz)	Direct V2V/V2I	Low latency, decentralized, ad hoc; limited range and capacity
C-V2X (LTE-V2X) [47], [48]	Cellular-based V2X using LTE (e.g., 5.9 GHz) via PC5 and Uu interfaces	Direct (PC5) + Infrastructure (Uu)	Wide coverage, QoS support, depends on cellular infrastructure
5G NR-V2X [49], [50]	5G-based V2X supporting URLLC and high mobility (e.g., 3.5 GHz, 28 GHz)	Direct + Infrastructure	Ultra-low latency, high throughput, evolving standards
millimeter-wave V2X [51], [52]	Uses millimeter-wave spectrum for high-speed V2X (e.g., 28 GHz, 60 GHz)	Primarily V2I (RSU ↔ Vehicle)	Very high data rate, low latency; limited coverage, blockage-sensitive

can be established with the assistance of RSUs that are accessed by the target CAVs. The connection can be separately triggered from CAV or RSU sides, and their procedures are briefly described below separately. The 'Nearest RSU' is defined as the RSU that the CAV is currently connected to via wireless communication for immediate data exchange. The 'Destination RSU', also referred to as the 'Remote RSU', is the RSU with which the CAV coordinates to exchange consensus information within the blockchain.

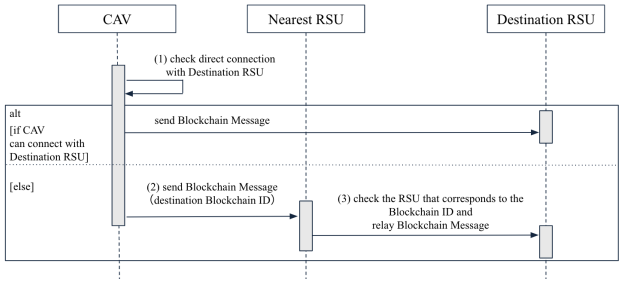


Fig. 3. Sequence Diagram of CAV-to-Remote RSU Communication.

Connecting from a CAV to a Remote RSU

The sequence diagram of the CAV-to-remote RSU communication is shown in Fig. 3. The working procedure includes the following steps:

1) The CAV checks if it can directly communicate with the RSU managing its blockchain.
2) If there is no direct communication link, the CAV sends a message to the directly accessible RSU for consensus formation, including the ID of the destination Blockchain.
3) The receiving RSU forwards the message to the destination RSU based on the blockchain ID and RSU correspondence.

Sending a Message from a RSU to a Remote CAV

The sequence diagram for RSU-to-remote CAV communication is shown in Fig. 4. The working procedure mainly includes:

1) The RSU first verifies whether it can establish direct communication with the target CAV.
2) If direct communication is not possible, the RSU interacts with the IMMU's Vehicle Broadcast Unit to obtain information about RSUs that can directly communicate with the CAV, and the forwards the message to the corresponding RSU.
3) The receiving RSU forwards the message if it can directly communicate with the target CAV (i.e., the CAV is within its service area and is directly associated with it). Otherwise, the source RSU re-queries the IMMU and forwards the message to the other RSU.

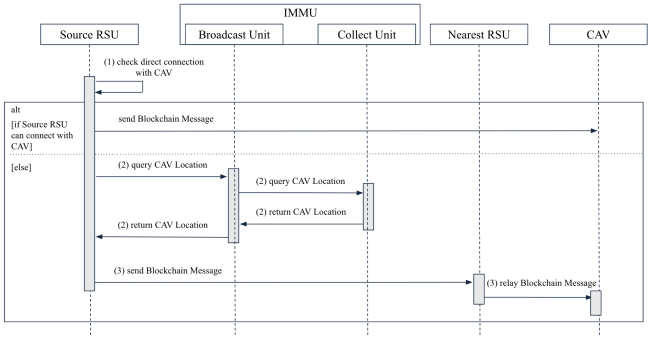


Fig. 4. Sequence Diagram for RSU-to-Remote CAV Communication.

After receiving the blockchain message, the destination RSU/CAV sends an acknowledgment message back to the corresponding source CAV/RSU to confirm the receipt of the message and establish communication between them. The message format for the RSUs is as follows.

```
type BetweenproposerMsg struct {
    Message   any
    Sender    int
    Recipient int
    Phase     int
}
```

In the message structure, the original message required for blockchain construction is stored in the Message, Sender and Recipient, containing the IDs of the sending and receiving RSUs or vehicles. The phase indicates the current stage of consensus formation. This phase makes it possible to distinguish whether the communication is from an RSU to a vehicle or from a vehicle to an RSU, and the message is forwarded according to the procedure described above.

D. Establishment of Blockchain

The consensus formation process for establishing a blockchain can be divided into three major phases:

- Phase-1: block information distribution by the proposer (RSU on the road).
- Phase-2: block verification and voting by validators (vehicles on the road).

- Phase-3: aggregation and verification of validator votes, as well as block generation by the proposer.

At each time of consensus formation t , the total consensus time ($\mathcal{T}_t$) consists of both the communication time (τ_t^c), which accounts for message exchange, and the validation time (τ_t^v). Formally, we have:

$$\mathcal{T}_t = \tau_t^{\text{com}} + \tau_t^{\text{val}}. \tag{1}$$

For each CAV u, the communication time between it and the RSU ($\tau_{t,u}^{\text{com}}$) is influenced by the quality of the wireless channel and network congestion conditions. It can be expressed as:

$$\tau_{t,u}^{\text{com}} = \frac{V_{t,u}^m}{B_{t,u}} + \tau_{t,u}^{hs} + \tau_{t,u}^{\text{com},wait}, \tag{2}$$

where $V_{t,u}^m$ denotes the real-time message size, $B_{t,u}$ is the communication rate between the CAV u and its associated RSU, $\tau_{t,u}^{hs}$ is the handshaking latency as specified by the underlying communication protocol, and $\tau_{t,u}^{\text{com},wait}$ represents the additional communication waiting latency due to network congestion. In practical V2X systems, the communication latency $\frac{V_{t,u}^m}{B_{t,u}}$ can often be neglected during the consensus process because modern communication technologies generally offer extremely high data rates, and the message sizes are typically very small. Therefore, in this study, we only consider the handshaking latency and waiting latency, both of which are simulated by our simulation platform.

The consensus validation operations are conducted by both CAVs and RSUs, i.e., vehicles verify the block information distributed by RSUs and RSUs verify the final voting information aggregated from all involved CAVs. It should be noted that each CAV can verify the block information upon receiving it; however, the aggregated votes can only be verified by RSUs after collecting sufficient votes from CAVs. Therefore, we can separately express the validation time for a CAV ($\tau_{t,u}^{\text{val}}$) and an RSU ($\tau_{t,rsu}^{\text{val}}$) as

$$\tau_{t,u}^{\text{val}} = \frac{\rho_{t,u}^{\text{block}}}{\boldsymbol{P}_u}, \tag{3}$$

and

$$\tau_{t,rsu}^{\text{val}} = \frac{\sum \rho_{t,rsu}^{\text{votes}}}{\boldsymbol{P}_{rsu}}, \tag{4}$$

where $\rho_{t,u}^{\text{block}}$ is the computation requirement of the block information received by u. $\boldsymbol{P}_u$ is the computing speed of u. $\sum \rho_{t,rsu}^{\text{votes}}$ denotes the total computational requirement of votes received by RSU rsu. $\boldsymbol{P}_{rsu}$ is the computing speed of rsu. As the transmission of messages and validation on vehicles can be performed simultaneously but the final verification of votes can only be executed after collecting sufficient votes, we can rewrite Eq. (1) as

$$\mathcal{T}_t = \max_{u \in \mathcal{U}^+} \{\tau_{t,u}^{\text{com}} + \tau_{t,u}^{\text{val}}\} + \tau_{t,rsu}^{\text{val}}, \tag{5}$$

where $\mathcal{U}^+$ denotes the set of CAVs whose votes are finally selected by RSU.

A consensus process is considered successful only if the proposer receives a sufficient number of votes within an acceptable time threshold. Specifically, let the number of participants be n, and let f denote the maximum number of Byzantine (arbitrarily faulty) participants tolerated within a configuration/epoch. Under the assumption $n = 3f + 1$, the required quorum size is $2f + 1$. For example, when $n = 7$ ($f = 2$), consensus is achieved if at least five valid votes from distinct participants are collected within the deadline.

IV. AI-Driven Consensus in Blockchain

The use of AI in the Booth Management Unit can be designed to optimize various objectives according to the V2X system's operational goals. In this study, we leverage AI with two objectives: i) to balance the load across RSUs to prevent overload, thereby improving workload distribution and reducing consensus time, and ii) to minimize user reallocation to remote RSUs to decrease data transmission overhead and further lower latency. The former addresses the issue of varying numbers of CAVs accessing each RSU, resulting in inefficient resource utilization, with some RSUs being overloaded, while others are underutilized. The latter rationale is based on the fact that the transmission between RSUs introduces additional overhead and latency.

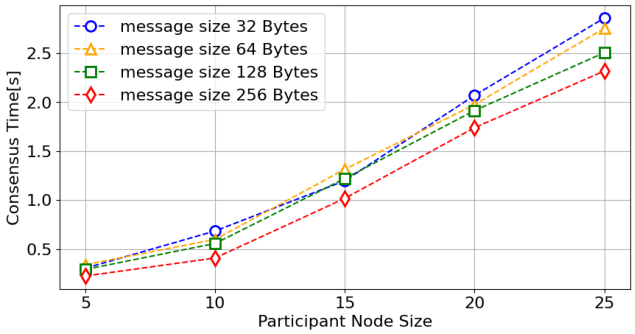


Fig. 5. Consensus Time vs. Participant Node Size.

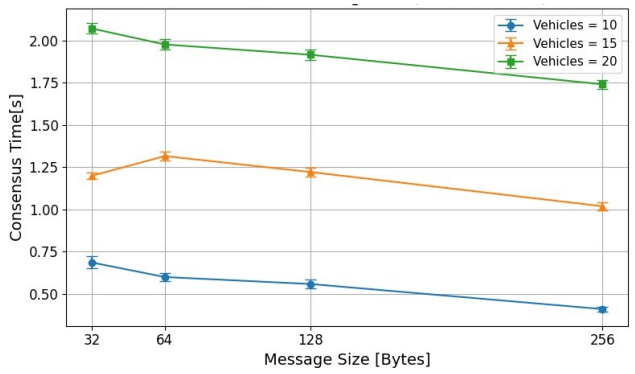


Fig. 6. Consensus Time vs. Message Size.

As a preliminary study for optimizing participant assignment, we used V-Guard standalone [17] to investigate the correlation between consensus time and the number of participat nodes (i.e., validator). As shown in Fig. 5, it is evident that an increase in the number of participant nodes in the blockchain leads to longer consensus times. Meanwhile, the impact of message size is investigated and displayed in Fig. 6, where the error bars indicate the confidence intervals and demonstrate

that the variance across trials remains relatively small. This supports the stability of the consensus process. Besides, we can find that node scalability plays a more significant role in determining consensus performance than message payload size in our proposed system. Hence, we can ignore the impact of the message size in this work.

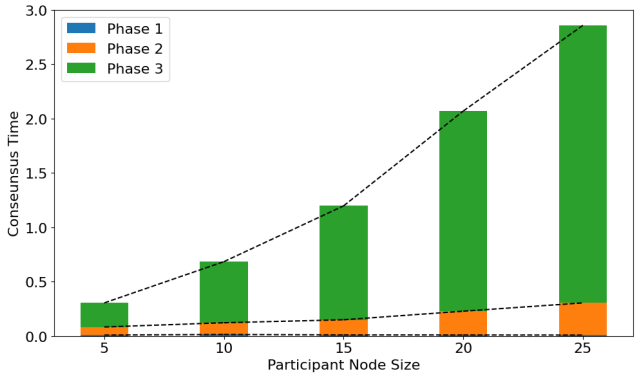


Fig. 7. Time Consumed by Consensus Phases vs Participant Node Size.

The time required for each consensus formation phase and the total consensus time were measured for different participant node sizes with a 32-byte message size. The results are presented in Fig. 7. This figure shows that as the number of vehicles increases, the consensus time, particularly the time for Phase-3, also increases. This is because Phase-3 integrates partial signatures from validators into a single signature, which requires time proportional to the number of partial signatures. Therefore, the consensus time is significantly influenced by the number of participating vehicles.

If each RSU simply uses all directly connected CAVs as blockchain members, significant variations in consensus formation times may occur across RSUs, particularly when some RSUs become overloaded. In practical V2X systems, it is conceivable to synchronize the time across all nearby blockchains maintained by a single IMMU and periodically create blocks. Therefore, it is preferable to minimize discrepancies in the consensus formation times across blockchains to ensure more consistent system performance. Additionally, although the amount of data currently included in the blockchain is relatively small, it is anticipated to grow significantly with the widespread adoption of autonomous driving technologies. If CAVs are assigned to the blockchain of remote RSUs, a substantial amount of data may be unnecessarily forwarded across the network, potentially leading to severe congestion. Therefore, it is crucial to mitigate network overhead and congestion by minimizing the data transmission between RSUs.

To achieve these, we need to optimize CAV-to-RSU assignment. Each time, we assume that there are n CAVs within the coverage of the IMMU. The consensus formation time of each blockchain depends only on the CAVs assigned to it. At any given time, the real-time states of the CAVs were determined and monitored by the IMMU. The assignment of CAVs to RSUs depends on the observed state of the CAVs. Therefore, the performance of blockchain consensus formation at a given time depends solely on the real-time state and CAV assignment action generated by the employed policy. In conclusion, this process can be formulated as a Markov Decision Process (MDP). Based on this, we can leverage reinforcement learning to develop a policy for optimal CAV assignment.

Based on the designed IMMU architecture and objectives, we defined the state, action, and reward functions required for reinforcement learning as follows:

State: the location of CAVs within the coverage of IMMU, i.e.,

$$s_t = \{(v_{x,t}, v_{y,t}, f_{\text{dummy},t}) \mid v \in \mathcal{V}_t\}, \tag{6}$$

Here, we consider only the two-dimensional coordinate information on the horizontal plane. $(v_{x,t}, v_{y,t})$ represent the x and y coordinates of the CAV v in the defined x-y coordinate system at time t. $\mathcal{V}_t$ denotes the set of CAVs in the system. In the learning process, there are scenarios in which the state consists of the information for less than n vehicles. In such cases, dummy vehicles not used for training are added to state along with regular vehicles to ensure that the state dimension remains consistent. In this context, $f_{\text{dummy},t}$ serves as a flag to distinguish between the regular and dummy vehicles. Specifically, for regular vehicles, we set $f_{\text{dummy},t} = 0$, and for dummy vehicles, we set $f_{\text{dummy},t} = 1$. Additionally, the coordinates of the dummy vehicles, $v_{x,t}$ and $v_{y,t}$, were assigned an outlier value of $(10000, 10000)$.

Action: the assignment of CAVs to RSUs, i.e.,

$$a_t = \{v_h | v \in \mathcal{V}_t\}, v_h \in \mathcal{H}, \tag{7}$$

where v_h represents the RSU assigned to CAV v. $\mathcal{H}$ denotes the set of RSUs in the system.

Reward: we define the reward function as the weighted sum of a distance reward ($R_{d,t}$) and load balancing reward ($R_{\text{lb},t}$), i.e.,

$$R_t = w \cdot R_{d,t} + (1 - w) \cdot R_{\text{lb},t}, \tag{8}$$

where w denotes a weight parameter that adjusts the relative importance of $R_{d,t}$ and $R_{\text{lb},t}$. The Distance Reward encourages the policy to minimize transmission overhead between RSUs, while the Load Balance Reward considers the distribution of CAVs among RSUs to achieve load balancing.

$R_{d,t}$ can be formulated as

$$R_{d,t} = \frac{1}{|\mathcal{V}_t|} \sum_{i=1}^{|\mathcal{V}_t|} \left(\frac{d^i_{\text{selected}} - d^i_{\text{min}}}{d^i_{\text{max}} - d^i_{\text{min}}} \right), \tag{9}$$

where d^i_{selected} is the distance from CAV i to the selected RSU, d^i_{min} is the minimum distance from CAV i to any RSU, and d^i_{max} is the maximum distance from vehicle i to any RSU. $R_{d,t}$ decreases as the distance d^i_{selected} from the selected RSU increases. When a CAV is assigned to the nearest RSU, it contributes a reward of +1. Conversely, if it is assigned to the farthest RSU, it contributes a reward of -1. $||$ denotes the operation used to determine the number of elements in a set. Thus, $|\mathcal{V}_t|$ represents the number of regular vehicles, excluding the dummy vehicles.

The load balancing reward $R_{\text{lb},t}$ can be formulated as

$$R_{lb,t} = \begin{cases} -1, & \text{if } \sigma_l > T \\ 1 - 2 \cdot \frac{\sigma_l}{T}, & \text{otherwise,} \end{cases} \tag{10}$$

where σ_l represents the standard deviation of the number of assigned vehicles across the RSUs and T is the threshold (set to $T = 10$ in this model). If the standard deviation σ_l exceeds T, then the load-balancing reward $R_{\text{lb},t}$ is set to a fixed value of -1. However, as the standard deviation decreases, the load-balancing reward $R_{\text{lb},t}$ increases linearly, reaching $R_{\text{lb},t} = 1$ when the standard deviation is 0.

V. Performance Evaluation

This section introduces the experimental setup used to evaluate the performance of the proposed IMMU architecture and discusses the obtained results.

A. End-to-End Simulator Setup

When evaluating the application of blockchain to V2X, the following assumptions are made.

1) All CAVs participating in the blockchain are within the communication range of at least one RSU.
2) Every CAV participating in the blockchain is assigned to a single blockchain built by a specific RSU.
3) The decision time for CAV assignment for blockchain construction is sufficiently short.
4) Communication bandwidths available between RSUs, and between the IMMU and RSUs are sufficiently high. Assuming that RSUs are interconnected with the management center via high-bandwidth optical links, enabling low-latency data exchange among them that satisfies requirements.
5) RSUs can always obtain the state information of CAVs accessed to it.
6) All CAVs can connect to a RSU in the system as long as they are within the coverage area of the RSU.

To implement these assumptions, we establish a simulation environment that integrates Artery with a Python-based implementation of IMMU. Artery is a simulator primarily used for research on CAV communication systems, designed to model and evaluate scenarios in ITS and V2X communication. It integrates the OMNeT++ network simulator with the Simulation of Urban Mobility (SUMO) traffic simulator to jointly simulate real-time traffic conditions and communication protocols [18]. This integration allows for a detailed analysis of how CAVs exchange information and how this affects traffic volume and safety. V-Guard involves a single proposer and multiple validators, where the proposer collects incoming data in batches during the ordering phase to create blocks. This is followed by the consensus formation phase, in which the proposer aggregates the blocks ordered thus far and forms a consensus with the other validators. In this simulation, the scenario was constructed with RSUs as proposers and CAVs as validators for V2I scenarios.

The experimental setup considers three RSUs at equal distances from each other and uses SUMO to generate CAVs moving in both directions on two lanes. Communication feasibility and timing were measured using OMNeT++. Communication measurement times are logged, and the consensus formation time for each RSU's blockchain is measured in the V-Guard. The evaluation was considered successful if the consensus time was less than the feasible communication time. Decisions regarding which RSU a CAV connects to are made using the proposed reinforcement learning logic, and the details of this signaling are explained in the previous subsection. The logic of the evaluation platform is shown in Fig. 8. We conducted simulations using SUMO v1.20.0, OMNeT++ v5.6, and Python v3.11.4. The specifications of the hardware used are listed in Table III. Simulation parameters used in each experiment are introduced separately in the corresponding sections.

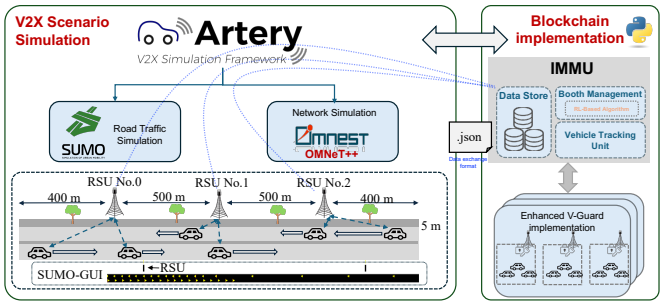


Fig. 8. The Framework of End-to-End Simulator.

TABLE III
Hardware Information

CPU	Intel Core i7-10875H (2.30 GHz base, 5.10 GHz boost, 8 cores, 16 threads)
Memory	62GB DDR4
Storage	953.9GB NVMe SSD
GPU	NVIDIA RTX 2070 SUPER (8GB, CUDA 12.6)
OS	Ubuntu 22.04.4 LTS (Kernel 6.8.0-51-generic, x86_64)

B. Data Preparation

1) Improvement of Consensus Success Ratio: During the consensus process, each CAV communicates through an RSU facilitated by the IMMU. Consensus formation is confirmed only when the consensus results are propagated to all the member CAVs. In practice, consensus formation is successful if more than 2/3 of the participants are able to communicate normally by the time the consensus formation is completed.

However, it will not be possible to know whether the consensus formation is successful if a CAV that is moving during the consensus formation leaves the communication range of the connected RSU, and the CAV in question (under such a condition) will not be able to share data and will have to go through the process of consensus building with a new vehicle again, which will cause overhead. Therefore, we define consensus formation as successful if the results of the consensus formation are correctly received by all vehicles.

We deployed a one-lane road on each side and set the total length of the road to 1800 m in the SUMO. At 400 m, 900 m, and 1400 m along the road, RSUs were placed 5 m from the side of the road as RSU#1, RSU#2, and RSU#3. CAVs

enter the selected road range from both sides every 5 s, and then drive at a constant speed [53]. The success probability of consensus formation is then examined for RSU#2 in the middle of the road, with and without communication bypassing the RSUs.

We conducted a road simulation using Artery to investigate the time variation in the number of CAVs with which RSU#2 can communicate. The results for the CAV speeds of 40, 60, and 80 km/h are shown in Fig. 9. The x-axis shows the simulation time and the y-axis shows the number of CAVs communicated with. We observed that, as the speed increased, the number of connected CAVs increased, but the number of CAVs communicated with decreased. In addition, the figure shows that the number of CAVs that can be connected is approximately 24 at a CAV speed of 40 km/h, 16 at 60 km/h, and 12 at 80 km/h.

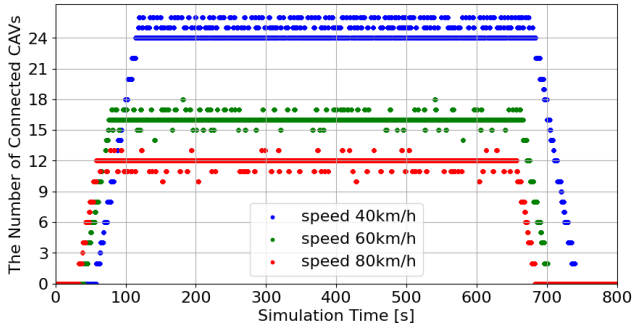


Fig. 9. Number of Communicable Nodes over Time.

Next, based on the list of CAVs that can communicate, as obtained from Artery, the blockchain is performed to verify the success probability of consensus formation under two scenarios, namely without communication bypass between RSUs (w/o bypass route) and with communication bypass between RSUs (w/ bypass route). At this point, the validator members for consensus formation are determined each time based on the communication list at each instance. We then analyzed the logs of each validator member, and consensus was considered successful if all members had a consensus completion log. In a scenario without communication bypass between RSUs, any CAV leaving the RSU's communication range during consensus would fail to receive the completion log, leading to consensus failure. However, in the scenario with communication bypassing between RSUs, the completion log could be relayed to CAVs outside the RSU's communication range, ensuring successful consensus formation. The results of the probability of successful consensus when the CAV speed was changed to 40 km/h, 60 km/h, and 80 km/h are shown in Fig. 10. It can be confirmed that consensus is always successful when data exchange is facilitated between neighboring RSUs. However, the results indicate that the success rate increases with increasing speed when data exchange is not enabled between RSUs. This is attributable to the fact that, as the speed increases, the number of CAVs that remain within the communication range decreases (Fig. 9), thereby reducing consensus formation time. In contrast, in a scenario where CAVs enter at a constant speed, the frequency with which CAVs leave the RSU's communication range remains unchanged, regardless of speed. As a result, the success rate increases with speed, likely due to a reduction in the average number of CAVs associated with each RSU.

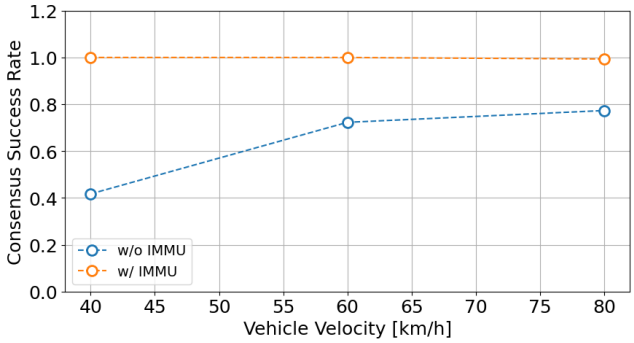


Fig. 10. Consensus Success Rate vs. CAV Speed w/ and w/o IMMU.

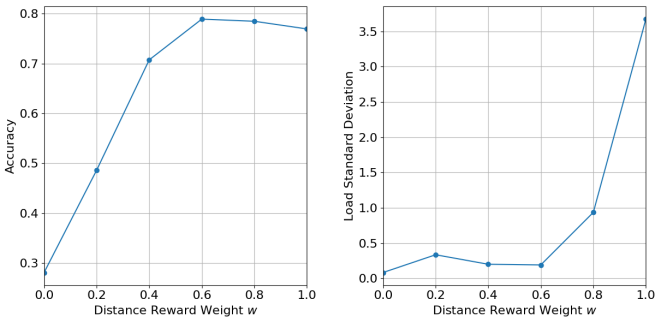
2) Reinforcement Learning-based Optimization: We incorporated reinforcement learning based on the reward explained in Section III and evaluated system performance. Similar to the previous experiments, the road setting for SUMO was 1,500 m, and three RSUs were installed 5 m from the roadside at 400, 900, and 1300 m, respectively. In the reinforcement learning model training, the training data were based on 120 CAVs randomly placed on the road within the range where their communication with the simulated RSUs (i.e., RSU#1, RSU#2, RSU#3) was possible (within approximately 300 m of the RSU). We used the Advantage Actor Critic (A2C) reinforcement learning algorithm from Stable-Baselines3 (v2.3.2) [54] in Python as the learning model. The parameters for the AC2 algorithm are listed in Table IV.

TABLE IV
THE SETUP OF THE A2C ALGORITHM.

Item	Value
Learning Rate	0.0001
Entropy Coefficient	0.003
Total Timesteps	100,000
Policy Network	Hidden layer 3 layers (512 units per layer)

For the evaluation, we used two metrics: the probability of being assigned to the nearest RSU and the standard deviation of the number of CAVs in the RSU. We ran the training with different weights for the $Distance\_Reward$ and $Load\_Balance\_Reward$ rewards and evaluated the results by averaging the results of 500 assignments using random test data with 60 vehicles for each. The results are presented in Fig. 11. The distance reward weight w on the horizontal axis represents the distance reward weight. The vertical axis shows the probability of a CAV being assigned to the closest RSU, and the Load Standard Deviation shows the standard deviation of the number of CAVs assigned to three 3 RSUs. We can see that as the distance reward weight w increases, load balancing is neglected, and the standard deviation increases. However, the accuracy shows a convex trend, reaching its maximum when the Distance Reward Weight w is 0.6, and

then maintains a high level. Therefore, in this model, the model with a Distance Reward Weight w of 0.6 has the highest accuracy, and it also achieves load balancing. Therefore, in the IMMU assignment for the subsequent experiments, the distance reward weight is set to 0.6, unless otherwise specified.



(a) Performance Accuracy **(b)** Performance Load Standard Deviation

Fig. 11. Training results of the envisioned Reinforcement Learning algorithm.

C. The Evaluation of Scenarios on Congested Roads

We evaluated the model using a distance reward weight w of 0.6 and considering a congested road scenario, and compared the results between i) when the RSU and CAVs that can communicate with it are used as the constituent nodes of the blockchain (w/o IMMU) and ii) when CAV assignment is performed using IMMU (w/ IMMU). The road was the same as that used to create the learning model. In addition, CAVs appear on the road from both sides every 5 s and drive to the opposite side while maintaining a safe distance from the CAVs in front of them. In this case, the CAV speed was set to $70\,\mathrm{km/h}$ and, to emulate congestion, 5% of CAVs were constrained to $30\,\mathrm{km/h}$ while the remainder maintained $70\,\mathrm{km/h}$. The communication between RSUs and their respective CAVs is based on the IEEE 802.11p protocol [46], [55], operating in the 5.9 GHz frequency band and 10 MHz bandwidth. At this point, the communication coverage radius of the RSU is approximately 300 m. The results of running the CAVs on the Artery and measuring the number of CAVs that can communicate with the RSU are presented in Fig. 12. We observe a large difference in the number of CAVs that can communicate with RSU#1 and RSU#3 compared to RSU#2, when communications are primarily based on the distance between CAVs and RSUs. For RSU#1 and RSU#3, the number of CAVs that can communicate with them is the same because the CAVs enter from both sides under the same conditions. However, because RSU#2 is located between RSU#1 and RSU#3, the trend in the number of CAVs that can communicate with it changes.

The CAV location data obtained from Artery were applied to the A2C model after completing the policy training, and the RSUs to which the CAVs should connect were dynamically assigned. Specifically, whenever the set of CAVs that can communicate with a particular RSU changes, the CAV assignment at that time is determined based on the Artery timestamp and

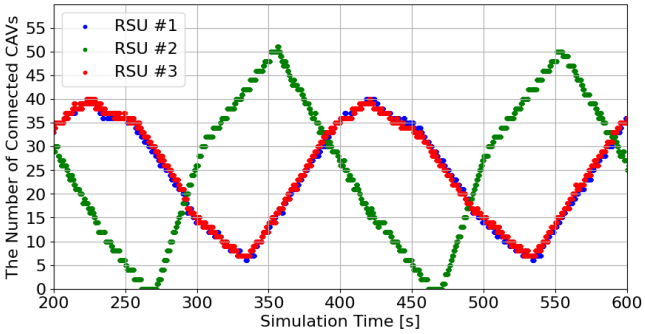


Fig. 12. Communicable Node Size under Congestion Scenarios.

CAV location data. The results of the CAV allocation using the A2C model in IMMU reinforcement learning are shown in Fig. 13. We clearly observe that the numbers of CAVs connected to RSU#1, RSU#2, and RSU#3 are almost equal. From this, we can conclude that load balancing is achieved using reinforcement learning in IMMU, even though the load status is not uniform when the allocation is performed within the communication range of each RSU.

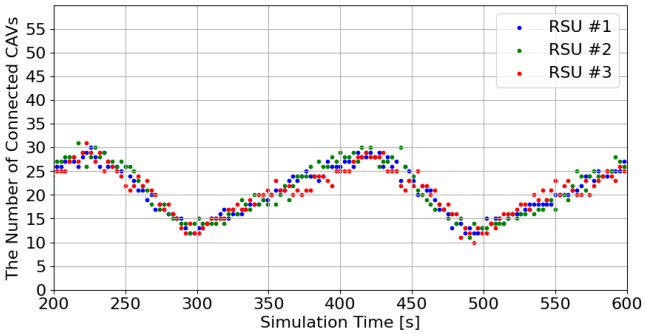


Fig. 13. Participant Node Size w/ IMMU Assignment.

The V-Guard blockchain formation process was executed using CAV allocation results cached in JSON format files for each formation instance. Upon loading the JSON configuration, the system performs consensus formation and measures performance metrics. In our simulation, consensus is formed at 0.5 s intervals. We compare the results of this consensus formation time with and without the IMMU. The variation in the consensus formation time when the CAVs that can communicate are used as validator members for consensus formation without an IMMU is shown in Figs. 14 and 15. The results of IMMU allocation are shown in Fig. 16. Comparing these three figures, it is evident that the IMMU helped even out the consensus time. In addition, when the IMMU is used, the results exhibit a similar trend to those of CAV assignment shown in Fig. 13, and we can confirm that the IMMU effectively contributes to balancing the consensus time.

Furthermore, the cumulative distribution function (CDF) in scenarios w/o IMMU and w/ IMMU is displayed in Fig. 17. In this case, it was again confirmed that the time taken to reach consensus was less variable when IMMU was used. The results demonstrate that the proposed IMMU approaches achieves optimal overall performance across all RSU configurations,

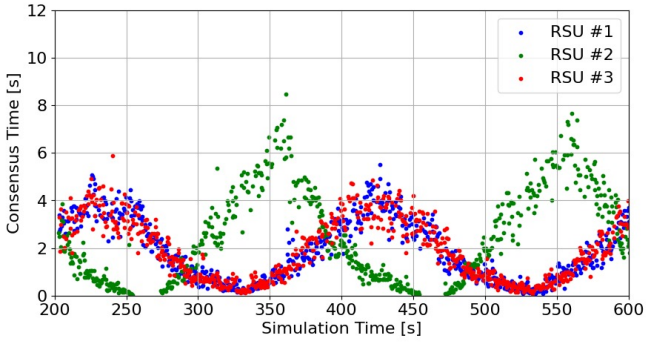


Fig. 14. Consensus Time: Nearest Policy w/o IMMU Assignment.

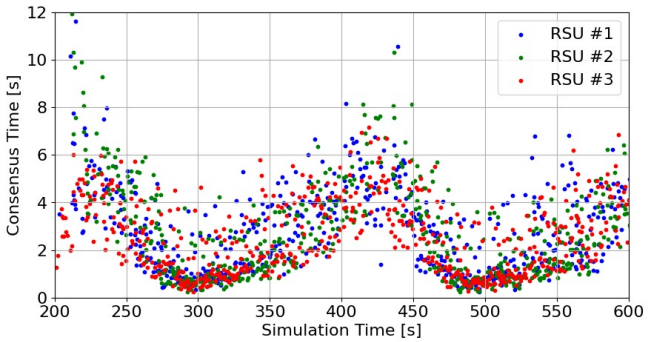


Fig. 15. Consensus Time: Random Policy w/o IMMU Assignment.

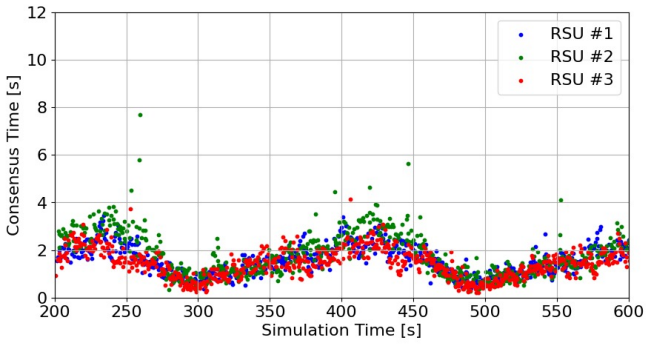


Fig. 16. Consensus Time: Proposed Approach w/ IMMU Assignment.

enabling over 97% consensus formation time less than 4 s, effectively reduce maximum consensus time. Although the Nearest Policy exhibits a higher proportion of cases with consensus times below 1 s, this effect primarily arises from unbalanced load distribution. Specifically, in situations where only a small number of CAVs are associated with a particular RSU, the consensus time is considerably reduced. Nevertheless, this imbalance simultaneously increases the consensus time for other RSUs subjected to heavier loads, thereby offsetting the perceived advantage. The Random Policy, lacking effective allocation strategies, shows high variance and unpredictable performance characteristics, failing to meet real-time application requirements. When comparing each RSU under the Proposed Approach w/ IMMU, it is evident that the consensus times are shortened across all RSUs. However, RSU#2 exhibits a wider variation in its consensus time than RSU#1 and

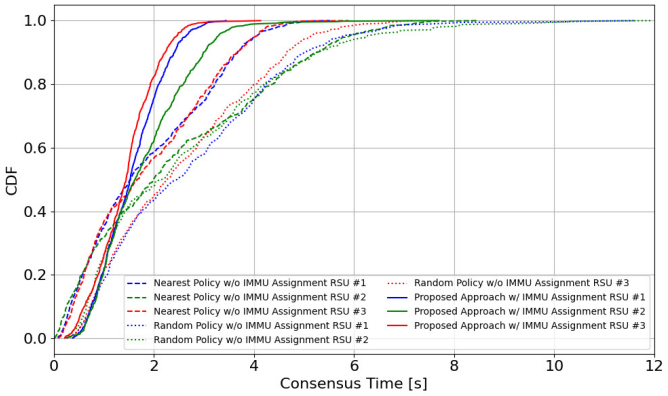


Fig. 17. CDF Result: w/o IMMU vs. w/ IMMU.

RSU#3. As shown in Fig. 16, this variation stems from the presence of outlier values for RSU#2, which implies that the IMMU was not able to fully alleviate the load concentration at RSU#2 during certain simulation periods. We can conclude that the proposed IMMU method achieves a trade-off of "local time increase, global time optimization" through intelligent load distribution, potentially increasing consensus time for some lightly-loaded RSUs while significantly reducing the system's overall maximum consensus time.

Furthermore, the average consensus time for each proposer was calculated at each simulation time, and the standard deviation among the proposers was summarized in Fig. 18 In this figure, the red dotted line labeled "w/o IMMU" represents the time periods where RSU#3 failed to reach consensus due to an insufficient number of participating vehicles. The figure also includes results for a Random Policy in which RSUs assign vehicles arbitrarily. From this figure, it can be observed that using IMMU reduces the standard deviation of consensus time across proposers more effectively than the Random Policy, particularly during congested periods. While the Random Policy partially mitigates the proposer imbalance compared to the baseline w/o IMMU, it still exhibits notable fluctuations due to the lack of vehicle-aware control logic. In contrast, the proposed approach achieves a more consistent load distribution across the RSUs.

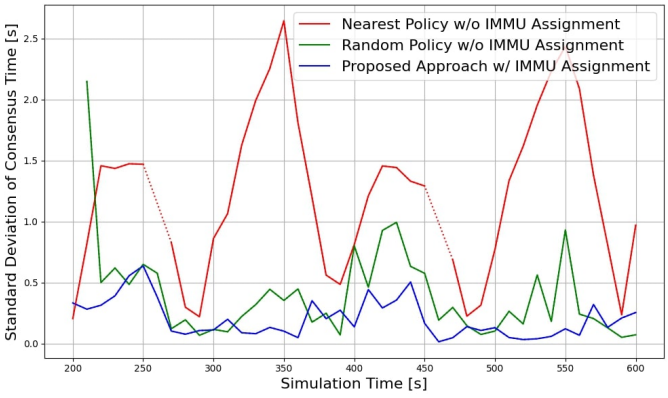


Fig. 18. Standard Deviation of Consensus Time: w/o IMMU vs. w/ IMMU.

The CDF for this standard deviation is presented in Fig. 19.

The results show that the IMMU achieves a lower variation in consensus time than both the Random Policy and Nearest Policy w/o the IMMU. For example, at the 20 % CDF point, the standard deviation improves by approximately 0.05 s compared to Random Policy and 0.4 s compared to the Nearest Policy w/o IMMU case. Similarly, at the 60 % CDF point, IMMU achieves an improvement of approximately 0.2 s and 1.2 s over the Random Policy and Nearest Policy, respectively, w/o IMMU. These results confirm that IMMU contributes to achieving more stable consensus durations and robust RSU load balancing, thereby reducing consensus formation time and enabling real-time blockchain formation.

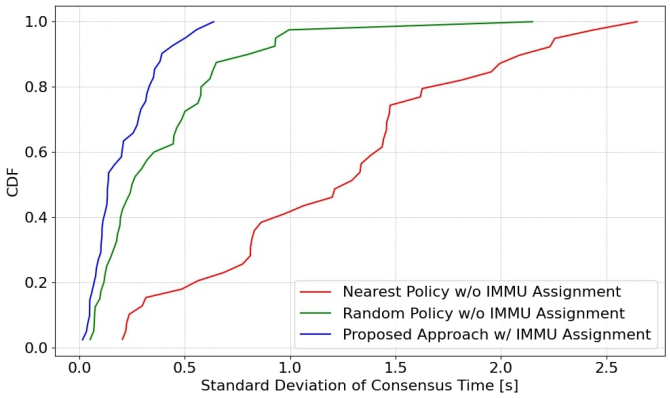


Fig. 19. Standard Deviation of Consensus Time CDF Result: w/o IMMU vs. w/ IMMU.

VI. Conclusion and Discussion

In this study, we proposed an IMMU architecture for applying blockchain to dynamic V2X to address the mobility of CAVs during blockchain formation. The problem was formulated as an MDP and then reinforcement learning-based approach was developed to optimize the CAV assignment during blockchain construction for each RSU. The simulation results demonstrated that the proposed architecture and approaches can improve the consensus formation performance in terms of consensus-formation time and load balancing. However However, our work only considers the positions of vehicles, which may result in slightly higher overhead for updating the blockchain in a practical system. For future work, the integration of vehicle mobility patterns and social information could be explored, along with the adoption of more advanced AI models, to enable more stable decision-making with fewer required updates. Besides, we assume that one server will be responsible for the IMMU, but this will partially undermine the decentralization and elimination of a single point of failure, which are the strengths of the blockchain. Therefore, in the future, we will also need to consider a design that achieves the functions of the IMMU solely through peer-to-peer communication between the proposers.

Acknowledgments

This work is also partly conducted at ICTFICIAL Oy, Finland. The paper reflects only the authors' views, and the European Commission bears no responsibility for any utilization of the information contained herein.

References

[1] A. Aissioui, A. Ksentini, A. M. Gueroui, and T. Taleb, "On enabling 5g automotive systems using follow me edge-cloud concept," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 6, pp. 5302–5316, 2018.

[2] A. Ghosh, A. Maeder, M. Baker, and D. Chandramouli, "5g evolution: A view on 5g cellular technology beyond 3gpp release 15," *IEEE Access*, vol. 7, pp. 127 639–127 651, 2019.

[3] Telecom.com, "China mobile launches groundbreaking 5.5g service for tailored user experiences." [Online]. Available: https://www.telecoms.com/5g-6g/china-mobile-launches-groundbreaking-5-5g-service-for-tailored-user-experiences

[4] European Commission, "Smart Networks and Services Joint Undertaking (SNS JU)," 2025, accessed: 2025-01-07. [Online]. Available: https://digital-strategy.ec.europa.eu/en/policies/smart-networks-and-services-joint-undertaking

[5] K. Trichias, A. Kaloxylos, and C. Willcock, "6g global landscape: A comparative analysis of 6g targets and technological trends," in *2024 Joint European Conference on Networks and Communications & 6G Summit (EuCNC/6G Summit)*, 2024, pp. 1–6.

[6] 6G-IA Vision Working Group, "European Vision for the 6G Network Ecosystem," 6G Infrastructure Association, Tech. Rep., Nov. 2024. [Online]. Available: https://doi.org/10.5281/zenodo.13708424

[7] National Highway Traffic Safety Administration. (2022) National highway traffic safety administration. Accessed: May 2022. [Online]. Available: https://www.nhtsa.gov/

[8] O. E. Wing, W. Lehman, P. D. Bates, C. C. Sampson, N. Quinn, A. M. Smith, J. C. Neal, J. R. Porter, and C. Kousky, "Inequitable patterns of us flood risk in the anthropocene," *Nature Climate Change*, vol. 12, no. 2, pp. 156–162, 2022.

[9] Y. Asabe, E. Javanmardi, J. Nakazato, M. Tsukada, and H. Esaki, "Enhancing reliability in infrastructure-based collective perception: A dual-channel hybrid delivery approach with real-time monitoring," *IEEE Open Journal of Vehicular Technology*, vol. 5, pp. 1124–1138, 2024.

[10] K. Abboud, H. A. Omar, and W. Zhuang, "Interworking of dsrc and cellular network technologies for v2x communications: A survey," *IEEE Transactions on Vehicular Technology*, vol. 65, no. 12, pp. 9457–9470, 2016.

[11] S. L. Kok and S. Siripipatthanakul, "The challenges and opportunities of geely: A marketing case study," 2023.

[12] T. Taleb and A. Ksentini, "Vecos: A vehicular connection steering protocol," *IEEE Transactions on Vehicular Technology*, vol. 64, no. 3, pp. 1171–1187, 2015.

[13] H. Masuda, O. E. Marai, M. Tsukada, T. Taleb, and H. Esaki, "Feature-based vehicle identification framework for optimization of collective perception messages in vehicular networks," *IEEE Transactions on Vehicular Technology*, vol. 72, no. 2, pp. 2120–2129, 2023.

[14] P. Team. (2018) Parq—green, smart and connected city platform. Accessed: Mar. 7, 2020. [Online]. Available: https://parkres.org/Parkreswhitepaper.pdf

[15] J. Meijers, G. D. Putra, G. Kotsialou, S. S. Kanhere, and A. Veneris, "Cost-effective blockchain-based iot data marketplaces with a credit invariant," in *2021 IEEE international conference on blockchain and cryptocurrency (ICBC)*. IEEE, 2021, pp. 1–9.

[16] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE transactions on industrial informatics*, vol. 13, no. 6, pp. 3154–3164, 2017.

[17] G. Zhang, Y. Mao, S. Zhang, S. Motepalli, F. Pan, and H.-A. Jacobsen, "V-guard: An efficient permissioned blockchain for achieving consensus under dynamic memberships in v2x networks," *arXiv preprint arXiv:2301.06210*, 2023.

[18] R. Riebl, H.-J. Günther, C. Facchi, and L. Wolf, "Artery: Extending veins for vanet applications," in *2015 International Conference on Models and Technologies for Intelligent Transportation Systems (MT-ITS)*. IEEE, 2015, pp. 450–456.

[19] A. Yoshimura, J. Nakazato, M. Tsukada, and H. Esaki, "Towards robust communication in its: A comprehensive study of blockchain for v2i," in *2024 Fifteenth International Conference on Ubiquitous and Future Networks (ICUFN)*, 2024, pp. 112–117.

[20] J. R. Douceur, "The sybil attack," in *Peer-to-Peer Systems*, P. Druschel, F. Kaashoek, and A. Rowstron, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002, pp. 251–260.

[21] T. Zhou, R. R. Choudhury, P. Ning, and K. Chakrabarty, "Privacy-preserving detection of sybil attacks in vehicular ad hoc networks," in

2007 Fourth Annual International Conference on Mobile and Ubiquitous Systems: Networking & Services (MobiQuitous). IEEE, 2007, pp. 1–8.
[22] B. D. Deebak, F. H. Memon, S. A. Khowaja, K. Dev, W. Wang, N. M. F. Qureshi, and C. Su, "A lightweight blockchain-based remote mutual authentication for ai-empowered iot sustainable computing systems," *IEEE Internet of Things Journal*, vol. 10, no. 8, pp. 6652–6660, 2022.
[23] Q. Feng, D. He, S. Zeadally, and K. Liang, "Bpas: Blockchain-assisted privacy-preserving authentication system for vehicular ad hoc networks," *IEEE Transactions on Industrial Informatics*, vol. 16, no. 6, pp. 4146–4155, 2019.
[24] C. Oham, S. S. Kanhere, R. Jurdak, and S. Jha, "A blockchain based liability attribution framework for autonomous vehicles," *arXiv preprint arXiv:1802.05050*, 2018.
[25] R. Tyagi, S. Sharma, and S. Mohan, "Blockchain enabled intelligent digital forensics system for autonomous connected vehicles," in *2022 International Conference on Communication, Computing and Internet of Things (IC3IoT)*. IEEE, 2022, pp. 1–6.
[26] M. Cebe, E. Erdin, K. Akkaya, H. Aksu, and S. Uluagac, "Block4forensic: An integrated lightweight blockchain framework for forensics applications of connected vehicles," *IEEE communications magazine*, vol. 56, no. 10, pp. 50–57, 2018.
[27] M. Castro and B. Liskov, "Practical byzantine fault tolerance and proactive recovery," *ACM Transactions on Computer Systems (TOCS)*, vol. 20, no. 4, pp. 398–461, 2002.
[28] M. Yin, D. Malkhi, M. K. Reiter, G. G. Gueta, and I. Abraham, "Hotstuff: Bft consensus with linearity and responsiveness," in *Proceedings of the 2019 ACM symposium on principles of distributed computing*, 2019, pp. 347–356.
[29] G. Danezis, L. Kokoris-Kogias, A. Sonnino, and A. Spiegelman, "Narwhal and tusk: a dag-based mempool and efficient bft consensus," in *Proceedings of the Seventeenth European Conference on Computer Systems*, 2022, pp. 34–50.
[30] S. Seng, X. Li, C. Luo, H. Ji, and H. Zhang, "A d2d-assisted mec computation offloading in the blockchain-based framework for udns," in *ICC 2019-2019 IEEE International Conference on Communications (ICC)*. IEEE, 2019, pp. 1–6.
[31] F. Jameel, M. A. Javed, S. Zeadally, and R. Jäntti, "Efficient mining cluster selection for blockchain-based cellular v2x communications," *IEEE Transactions on Intelligent Transportation Systems*, vol. 22, no. 7, pp. 4064–4072, 2020.
[32] J.-P. Martin and L. Alvisi, "A framework for dynamic byzantine storage," in *International Conference on Dependable Systems and Networks, 2004*, 2004, pp. 325–334.
[33] Y. Xu, J. Shao, J. Liu, Y. Shen, T. Taleb, and N. Shiratori, "Bwka: A blockchain-based wide-area knowledge acquisition ecosystem," *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 6, pp. 5617–5634, 2024.
[34] K. Salah, M. H. U. Rehman, N. Nizamuddin, and A. Al-Fuqaha, "Blockchain for ai: Review and open research challenges," *IEEE Access*, vol. 7, pp. 10 127–10 149, 2019.
[35] S. K. Poorazad, C. Benzaïd, and T. Taleb, "Blockchain and deep learning-based ids for securing sdn-enabled industrial iot environments," in *GLOBECOM 2023 - 2023 IEEE Global Communications Conference*, 2023, pp. 2760–2765.
[36] M. L. Adjou, C. Benzaïd, and T. Taleb, "Topotrust: A blockchain-based trustless and secure topology discovery in sdns," in *2022 International Wireless Communications and Mobile Computing (IWCMC)*, 2022, pp. 1107–1112.
[37] M. Mylrea and S. N. G. Gourisetti, "Blockchain for smart grid resilience: Exchanging distributed energy at speed, scale and security," in *2017 Resilience Week (RWS)*. IEEE, 2017, pp. 18–23.
[38] H. F. Atlam, M. A. Azad, A. G. Alzahrani, and G. Wills, "A review of blockchain in internet of things and ai," *Big Data and Cognitive Computing*, vol. 4, no. 4, p. 28, 2020.
[39] A. Baldominos and Y. Saez, "Coin. ai: A proof-of-useful-work scheme for blockchain-based distributed deep learning," *Entropy*, vol. 21, no. 8, p. 723, 2019.
[40] M. Liu, F. R. Yu, Y. Teng, V. C. Leung, and M. Song, "Computation offloading and content caching in wireless blockchain networks with mobile edge computing," *IEEE Transactions on Vehicular Technology*, vol. 67, no. 11, pp. 11 008–11 021, 2018.
[41] D. C. Nguyen, P. N. Pathirana, M. Ding, and A. Seneviratne, "Privacy-preserved task offloading in mobile blockchain with deep reinforcement learning," *IEEE Transactions on Network and Service Management*, vol. 17, no. 4, pp. 2536–2549, 2020.
[42] Y. Chen, Y. Sun, H. Yu, and T. Taleb, "Joint task and computing resource allocation in distributed edge computing systems via multi-agent deep reinforcement learning," *IEEE Transactions on Network Science and Engineering*, vol. 11, no. 4, pp. 3479–3494, 2024.
[43] Y. Chen, Y. Sun, C. Wang, and T. Taleb, "Dynamic task allocation and service migration in edge-cloud iot system based on deep reinforcement learning," *IEEE Internet of Things Journal*, vol. 9, no. 18, pp. 16 742–16 757, 2022.
[44] K. Peng, P. Xiao, S. Wang, and V. C. Leung, "Scof: Security-aware computation offloading using federated reinforcement learning in industrial internet of things with edge computing," *IEEE Transactions on Services Computing*, vol. 17, no. 4, pp. 1780–1792, 2024.
[45] ETSI, "TS 103 324 v2.1.1; Intelligent Transport Systems (ITS); VehicularCommunications; Basic Set of Applications; Analysis of the Collective Perception Service (CPS); Release 2," 2023.
[46] IEEE, *IEEE Standard for Information technology—Telecommunications and information exchange between systems—Local and metropolitan area networks—Specific requirements Part 11: Wireless LAN Medium Access Control (MAC) and Physical Layer (PHY) Specifications Amendment 6: Wireless Access in Vehicular Environments*, Std. 802.11p-2010, 2010.
[47] 3GPP, *Study on LTE-based V2X Services*, 3rd Generation Partnership Project (3GPP) Std. TR 36.885, June 2016, Technical Report (Release 14). [Online]. Available: https://www.3gpp.org/ftp/Specs/archive/36_series/36.885/36885-e00.zip
[48] 3GPP, *Evolved Universal Terrestrial Radio Access (E-UTRA); Physical layer procedures*, 3rd Generation Partnership Project (3GPP) Std. TS 36.213, Release 14 onwards, technical Specification. [Online]. Available: https://www.3gpp.org/ftp/Specs/archive/36_series/36.213/
[49] 3GPP, *Study on NR V2X*, 3rd Generation Partnership Project (3GPP) Std. TR 38.885, June 2020, Technical Report (Release 16). [Online]. Available: https://www.3gpp.org/ftp/Specs/archive/38_series/38.885/38885-g00.zip
[50] 3GPP, *NR; NR and NG-RAN Overall Description*, 3rd Generation Partnership Project (3GPP) Std. TS 38.300, Release 15 onwards, Technical Specification. [Online]. Available: https://www.3gpp.org/ftp/Specs/archive/38_series/38.300/
[51] 3GPP, *Study on NR V2X*, 3rd Generation Partnership Project (3GPP) Std. TR 38.885, June 2020, Includes mmWave (FR2) support for high-speed V2X; Technical Report (Release 16). [Online]. Available: https://www.3gpp.org/ftp/Specs/archive/38_series/38.885/38885-g00.zip
[52] M. Mezzavilla, M. Zhang, R. Ford, S. R. Dutta, and M. Zorzi, "Towards 5G: mmWave vehicular communication," *IEEE Access*, vol. 6, pp. 23 550–23 562, 2018.
[53] D. G. A. Center), "SUMO - Simulation of Urban MObility," http://sumo.dlr.de, 2018, accessed: 22, Jan 2024.
[54] V. Mnih, A. P. Badia, M. Mirza, A. Graves, T. Lillicrap, T. Harley, D. Silver, and K. Kavukcuoglu, "Asynchronous methods for deep reinforcement learning," in *Proceedings of The 33rd International Conference on Machine Learning*, ser. Proceedings of Machine Learning Research, M. F. Balcan and K. Q. Weinberger, Eds., vol. 48. New York, New York, USA: PMLR, 20–22 Jun 2016, pp. 1928–1937. [Online]. Available: https://proceedings.mlr.press/v48/mniha16.html
[55] A. Chandramohan and G. Heijenk, "Modelling the packet delivery of v2v messages based on the macroscopic traffic parameters," in *2022 IEEE 95th Vehicular Technology Conference: (VTC2022-Spring)*, 2022, pp. 1–5.

Atsuki Yoshimura He received B.E. and M.E. degrees from the University of Tokyo, Japan, in 2022 and 2024, respectively. His research interests include ITS and Blockchain.

Yan Chen received the B.E. degree in Information Engineering and the Ph.D. degree in Information and Communication Engineering from China University of Mining and Technology, China, in 2016 and 2022. He is currently a Postdoctoral Researcher with Ruhr University Bochum, Bochum, Germany. He is also a senior researcher with the ICTFICIAL OY, Espoo, Finland. From December 2020 to December 2021, he was also a visiting Ph.D. student at Aalto University, Finland. His research interests include Edge Computing, Internet of Things, Network Intelligence, and Multi-agent systems.

Jin Nakazato is currently an Assistant Professor at Tokyo University of Science. He also works as a technical advisor with Visban Corporation. He received B.E. and M.E. degrees from the University of Electro-Communications, Japan, in 2014 and 2016, respectively. He received a Ph.D. degree from the Tokyo Institute of Technology, Japan, in 2022. From 2016 to 2020, he was with Fujitsu Limited. From 2020 to 2022, he was with Rakuten Mobile, Inc. From 2022 to 2024, he was with specially appointed Assistant Professor at the University of Tokyo. His research interests include Multi-access Edge Computing, NFV/SDN Orchestrator, V2X, Open RAN, UAV networks, and virtualization RAN. He is a Member of IEICE and IEEE. He received the Best Paper Award at the International Conference on Ubiquitous and Future Networks (ICUFN) in 2019 and 2024. He also received the Best Paper Award at the INFOCOM 2024, ICAIIC Excellent Paper Award, and ACM ICEA Best Paper Award. He serves as a peer-reviewed open-access letter journal covering the field of communication, International Journal of Computers Applications Associate Editor, and Computer Networks Software and Datasets Editors.

Traik Taleb received the B.E. degree (with distinction) in information engineering and the M.Sc. and Ph.D. degrees in information sciences from Tohoku University, Sendai, Japan, in 2001, 2003, and 2005, respectively. He is currently a Full Professor at Ruhr University Bochum, Germany. He was a Professor with the Center of Wireless Communications, University of Oulu, Oulu, Finland. He is the founder and the Director of the MOSA!C Lab, Espoo, Finland. He is the fouder of ICTFICIAL Oy. From October 2014 to December 2021, he was an Associate Professor with the School of Electrical Engineering, Aalto University, Espoo, Finland. Prior to that, he was working as a Senior Researcher and a 3GPP Standards Expert with NEC Europe Ltd., Heidelberg, Germany. Before joining NEC and till March 2009, he worked as an Assistant Professor with the Graduate School of Information Sciences, Tohoku University, in a lab fully funded by KDDI. From 2005 to 2006, he was a Research Fellow with the Intelligent Cosmos Research Institute, Sendai. Taleb has been directly engaged in the development and standardization of the Evolved Packet System as a member of the 3GPP System Architecture Working Group. His current research interests include AI-based network management, architectural enhancements to mobile core networks, network softwarization and slicing, mobile cloud networking, network function virtualization, software-defined networking, software-defined security, and mobile multimedia streaming.

Manabu Tsukada is currently an associate professor at the Graduate School of Information Science and Technology, the University of Tokyo, Japan. He is also a designated associate professor at the Center for Embedded Computing Systems at Nagoya University, Japan. He was a visiting professor at Aalto University from February 2021 to November 2021. He received his B.S. and M.S. degrees from Keio University, Japan, in 2005 and 2007, respectively. He worked in IMARA Team Inria, France, during his Ph.D. course and obtained his Ph.D. degree from Centre de Robotique, Mines ParisTech, France, in 2011. During his pre and postdoc research stages, he has participated in a multitude of international projects in the networked ITS area, such as GeoNet, ITSSv6, SCORE@F, CVIS, Nautilus6, and ANEMONE. He served as a board member of the WIDE Project 2014-2022. His research interests are mobility support for the next-generation Internet (IPv6), Internet audio-visual media, and communications for intelligent vehicles.

Hiroshi Esaki is currently a Professor with the Graduate School of Information Science and Technology, University of Tokyo, Bunkyo, Japan. In 1987, he joined Research and Development Center, Toshiba Corporation, where he engaged in the research of ATM systems. From 1990 to 1991, he was with Bellcore Inc., Piscataway, NJ, USA, as a residential Researcher. From 1994 to 1996, he was with Columbia University, New York, NY, USA. He has proposed the CSR architecture that is one of the origin of MPLS (Multi-Protocol Label Switching), to the IETF and to the ATM Forum. From 1998, he was a Professor with The University of Tokyo, and Board Member of WIDE Project. From 1997, he has involved in many of the IPv6 research and development at the WIDE project. He is a cofounder of series of IPv6 special project in the WIDE project, (KAME Project, TAHI Project USAGI Project). He is an Executive Director of IPv6 promotion council, Vice Chair of JPNIC (Japan Network Information Center), and Chair of IPv6 Ready Logo Program run by IPv6 Forum.