A comprehensive survey on the application of blockchain/hash chain technologies in V2X communications

Hassan Farran[1], David Khoury[2], and László Bokor[3]

***Abstract*—The Vehicle-to-Everything (V2X) technology and protocols are the main cornerstones for advanced transportation and autonomous vehicle applications. V2X has several subsets, including Vehicle-to-Vehicle (V2V) and Vehicle-to-Infrastructure (V2I) communication contexts. The main benefit of applying V2X technologies is increased safety by facilitating predicted warnings supporting automated driving and traffic applications. Wirelessly transmitted messages are the information sources; therefore, security is critical in V2X systems. The V2X exchanged messages are sent wirelessly and must fulfill the security requirements, such as integrity, authenticity, and privacy support. The messaging between vehicles and networks must be trusted. Lately, promising and proliferating blockchain/hash chain technologies have been introduced in V2X communications and cope with the cooperative vehicular applications security and related efficiency aspects. This paper provides a comprehensive survey about the V2X use-cases based blockchain/hash chain and introduces the available solutions and methods in this domain.**

***Index Terms*—blockchain, hash chain, V2X/C-ITS security/privacy**

I. Introduction

COOPERATIVE Intelligent Transport Systems (C-ITS) introduce a new ecosystem of linked vehicles, roadside networks, and mobile connectivity valuable to the climate, society, and economy. Vehicle-to-Everything (V2X) creates infrastructures that ensure optimal transport facilities, decrease traffic loads, environmental emissions, and increase road safety and transport quality [1]. Specifically, C-ITS performance relies on V2X communications since it is responsible for sharing data between the underlying communication technologies. This provides input and alerts from on-board sensors, such as the vehicle's current location and speed. V2X is a protocol family designed to exchange messages that include vehicle information and sensor data from a vehicle to another vehicle or any individual/infrastructure element capable of influencing the vehicle and vice versa. Some of the applications based on V2X are autonomous driving, improving road safety, reducing fuel consumption, and traffic efficiency. V2X systems will make the road safer in decreasing the number of accidents, managing traffic flows, and providing environmental benefits. V2X is a combination of different communication contexts. As shown in Figure 1 below, V2X is based on a cooperative exchange of data between vehicles, and anything else that is Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), Vehicle-to-Network (V2N), Vehicle-to-Pedestrians (V2P) [2], Vehicle-to-Device (V2D) [3], Vehicle-to-Cloud (V2C) [4], Vehicle-to-Home (V2H) [5], or even Vehicle-to-Grid (V2G) [6].

For example, a vehicle that uses a navigation system based on GPS and other sensors can use V2V to indicate vehicle's location, speed, and direction. By broadcasting this information maximum of 10 times per second to the surrounding cars. When a vehicle receives this information, it will calculate the trajectories of the surrounding vehicles. Without entering into a hazardous situation or crash, it will warn the driver by visual alert to make them more aware of what is going around.

V2I is used, for example, as a communication protocol between the vehicle and the traffic lights. It may advise the driver to select the optimal speed to travel through a set of intersections. Furthermore, V2G is an example of a game-changing emerging technology that, along with smart charging, could change the electricity grid. In the case of V2C the ability to provide services from the vehicle maker and other suppliers directly over the Internet is established. V2N is a communication context used, e.g., for warning signs of impending barriers or road jams; and implementing centralized positioning systems [7]. V2D is applied, for example, as a communication method to transmit information between the vehicles and any electronic system to which the vehicle is connected. V2H refers to the exchange of data between vehicles and applications in the home. V2P establishes communication that involves exchanging information between vehicles and pedestrians, such as when the driver sends a message to a pedestrian alerting them to their location and that they are close.

Independently of the applied communication context, the application of V2X includes multiple facets, such as intelligent travel, intelligently linked vehicles, and autonomous driving.

[1] Department of Networked Systems and Services, Faculty of Electrical Engineering and Informatics, Budapest University of Technology and Economics, Műegyetem rkp. 3., H-1111 Budapest, Hungary. (e-mail: hfarran@hit.bme.hu)

[2] Department of Computer Science and information and communication technology, American University of Science and Technology, Beirut, Lebanon (e-mail: dkhoury@aust.edu.lb)

[3] Department of Networked Systems and Services, Faculty of Electrical Engineering and Informatics, Budapest University of Technology and Economics, Műegyetem rkp. 3., H-1111 Budapest, Hungary. (e-mail: bokorl@hit.bme.hu)

DOI: 10.36244/ICJ.2022.1.4

Various applications have various specifications for latency, durability, throughput, user density, and protection in the V2X environment; protection and autonomous driving system need exceptionally low latency and a safe network environment; therefore, security is the highest priority for V2X [8]. Any vehicular network infrastructure requires comprehensive security mechanisms to enable vehicles and other actors to communicate securely and efficiently.

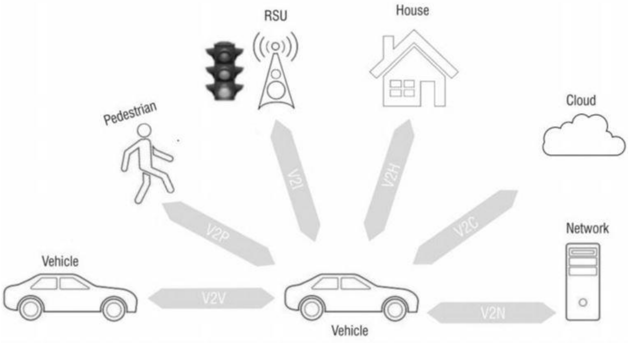

Fig. 1. Vehicle-to-Everything communication contexts.

Two types of V2X communication technologies are currently available: the Wi-Fi-based and the mobile cellular-based solutions (known as V2X and C-V2X, the latter using the 3G, 4G (LTE)/LTE-A, and 5G networks). The benefit of the short-range Wi-Fi-based techniques is low latency compared to the C-V2X networking systems [9]. The additional advantage is that network complexity is significantly lower than mobile cellular technology [10], and the cost is comparatively low [11]. However, the cellular-based system has advantages in targeting far broader areas, pre-existing infrastructure networks, deterministic security, QoS, and improved scalability guarantees [11].

The existing standards for V2X communication are DSRC (Dedicated Short-Range Communication) in the US, and ITS-G5 in Europe (referencing the used 5.9 GHz frequency band) [12].

In DSRC/ITS-G5, the vehicles use on-board units (OBUs) that send messages known as (BSM) Basic Safety Messages in the US that transmit the information about the vehicle, including the speed and location, acceleration, etc. In Europe the (CAM) Common Awareness Messages include similar status and attribute information [13], which have latency less than 100ms with a range of approximately 1600m.

In contrast, the Roadside Unit (RSU) is meant to be wirelessly accessed by the OBUs and usually backhauled by wired technologies. Among the ITS Facilities layer services, RSUs send the Decentralized Environmental Notification Messages (DENM) that include, e.g., alerts for road work. However, DSRC/ITS-G5 could open the door for malicious attacks or cause harm by sending or alerting false safety messages, rendering vehicles unsafe [14]. Both DSRC and ITS-G5 operate in the 5.9 GHz ITS band [15].

Radio technology is a part of the IEEE 802.11 family of standards [16]. IEEE 802.11p was the initial name of the ad hoc Wi-Fi mode of operation IEEE 802.11-2016-OCB (Outside the Context of a Basic Service Set) [17]. Network architectures and security protocols are specified in IEEE 1609 WAVE [18], and SCMS (Security Credential Management System) [19] on which US DSRC is based, and ITS-G5 with CCMS (EU C-ITS Credential Management System) specifications [20] in the EU.

Communication between vehicles is fundamental because the sensors cannot detect all the risky situations. This makes vehicle networks more vulnerable to various cyber threats that are internal or external attacks. The cooperative system between vehicles can only work when vehicles can trust the neighboring car's messages and the network where it is connected. In order to forge this trust, there are some privacy and security levels the message should pass through.

This paper manifests a comprehensive survey on vehicular communications relying on blockchain networks and technology, which can be used to solve privacy and security issues.

This paper is structured as follows. Section II gives an overview of the types of security attacks in the V2X domain. Section III introduces V2X security basics. Section IV presents background information on blockchain/hash chain technologies. Section V surveys the literature of different V2X topics combined with blockchain/hash chain paradigm. Finally, Section VI concludes the article.

II. TYPES OF V2X SECURITY ATTACKS IN A NUTSHELL

Protection of V2X communication is essential. Vehicular networks are especially susceptible to attacks due to their wireless communication properties. There are six main areas where attention is required to ensure V2X security. These are Validity, Non-Repudiation, Honesty, Confidentiality, Affordability, and Real-time constraints [8].

- Validity: means that the recipient is guaranteed to accept communications from a legitimate source [25].
- Honesty: all communications should be secured to deter hackers from modifying them and ensure that messages' content is trusted. This ensures that it is protected if the communications' contents are not edited or changed when the message is being sent [26].
- Affordability: The network must be affordable at all times to transmit and receive messages [27].
- Real-time constraints: Vehicles drive at high speed, which will demand real-time action in certain situations; otherwise, the outcome will be catastrophic [26].
- Confidentiality: Community messages sent to all participants should not be decryptable by non-group vehicles. A group message sent to a dedicated member should only be decryptable by the dedicated recipient; other vehicles should not be able to decipher the message [27].
- Non-repudiation: A sender node can attempt to deny that a message has been sent to escape responsibility for its contents. Non-repudiation is especially useful for the detection of corrupted nodes [27].

1. Attacks on Validity: Sybil attack, also known as Ghost attack, is an intruder that generates several vehicles

with the exact identification on the lane. It gives delusions to other cars by sending out incorrect signals to benefit this intruder [28].

2. Attacks on Non-Repudiation: Traceability lack of incidents. When an attacker tries to tamper with the database, it must access the majority of the nodes in the network, which is very complex in realistic application scenarios [29].
3. Attacks on Honesty: GPS spoofing by having nodes that believe they are in various positions; attackers easily trick nodes. This form of assault can be carried out by having incorrect readings on GPS units. It allows attackers to produce a stronger signal than the signal produced by an actual satellite using a GPS satellite emulator [30].
4. Attacks on Affordability: Denial of Service (DOS) is the most common intrusive assault against availability; an attacker attempts to make tools and facilities inaccessible to users on the network. Either by jamming a physical channel or by "Sleep Deprivation" [31].
5. Attacks on confidentiality: This can be achieved by the well-known Man in the Middle Attack (MiM), which can intercept the conversation between two other vehicles. This attack is feasible in a vehicle network in various situations. The intruder positions himself between the two pairs of nodes that communicate. The intruder also assumes care of the communication between the two cars. Honesty, validity, and non-repudiation concerns in-vehicle networks and can be violated by the MiM attack [25]. Moreover, it pretends to be the answer of either of them and inserts fake information between them [32].
6. Attack on Real-time constraints: e.g., period of assault, timing attack [8], Real-time constraints should be enforced since vehicles can travel in and out of a group of a Vehicular Ad Hoc Network (VANET) at random for a brief period of time [32].

To minimize all potential threats that could affect the protection of V2X contact, we need to ensure the effective deployment of adequate security services.

III. V2X SECURITY BASICS

A. *V2X messages security*

V2X security should operate to check the message's integrity, test that the message's contents did not change, stay stable, and authenticate the sender to check whether the constructed data came from a trusted source. Current V2X standards use a trusted Public Key Infrastructure (PKI) and a trustworthy third-party Certificate Authority (CA) in the US, and a Certificate Policy Authority (CPA) in Europe. PKI uses elliptic curve cryptography (ECC) that facilitates message authentication and integrity [21]. CA and CPA have the highest management authority for issuing vehicle identification details and related certificates, identity verification, and pseudonym management of vehicles. Digital signatures are used to provide the authenticity of the message sent by a vehicle. Both Security Credentials Management System (SCMS) [22] and C-ITS Credential Management System (CCMS) [20] rely on digital signatures for authentication and validating V2X messages.

B. *Security and privacy methodology*

V2X message transmissions relay on asymmetric key pairs [23]. These public key; private key pairs are used to verify/encrypt and sign/decrypt messages (respectively) to avoid malicious eavesdropping tampering[23]. The public key is known by any user and is extracted and sent to CCMS.

In contrast, the private key is stored securely inside the vehicle and used exclusively for signing transactions and messages. Signed transactions are needed to avoid surveillance, shield the driver's identification, and conceal actual identities. The private and public keys will be changed every short period to achieve privacy [24]. On the other hand, CCMS uses this public key, generates specific vehicle certificates, and signs the certificate using the root CPA. The root CPA is the root of trust for all certificates. Both the vehicle certificates and the root CPA are then sent back to the vehicle. Information shall be given to an accredited PKI auditor for auditing. After being audited, the root CPA application form should be signed with its authorized representative. The CPA appoints the Trust List Manager (TLM), ensuring that all PKI participants have confidence in the TLM's service. The CPA grants permission for the root CA activity and agrees that the TLM will depend on the root CA (s). The TLM generates the European Certificate Trust List (ECTL), which provides all PKI participants with confidence in the accepted root CA's [20] (Figure 2).

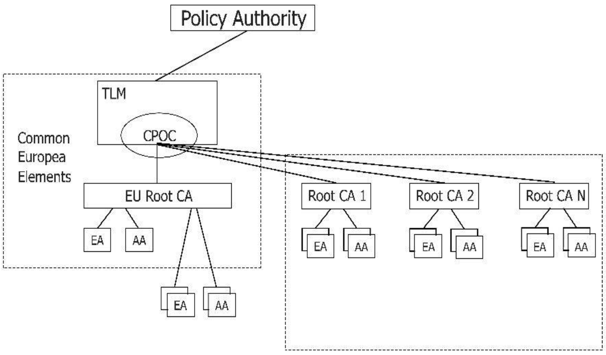

Fig. 2. The C-ITS Trust model architecture.

In the European C-ITS Platform's V2X security proposal implementations [20], the root CA sends the application to the sub-CA Enrolment Authority (EA) and Authorization Authority (AA) entities. In EA and AA, they check the integrity of the message since each message will contain the content, hash, and hash of the previous block (Figure 3). The contents are a set of transactions that could be information about the Vehicle, ID, speed, direction, braking, and even intention, etc. The hash part of the message is a string calculated based on the content. This hash depends on the content, and any alteration in a particular block or the content will eventually break the chain's integrity. However, each part of the message hashed and included the previous part, creating a hash chain for all these parts. After this process, EA and AA transmit their signed request electronically and deliver its application form to root

CA, verifying the request and the received documents. Suppose all checks lead to a positive result. In that case, the root CA issues the corresponding sub-CA certificate and then send the certificate of conformity to C-ITS Point of Contact (CPOC) and TLM. The main task of CPOC and TLM is to verify all documents and the self-signed certificates and send them back to CPA that transmit them to C-ITS (Figure 4). In system management, both TLM and CPOC are a single agency sub-role that operates in the EU CCMS and reports to the Operation Regulatory Body and the Credential Decision Authority [19] [20].

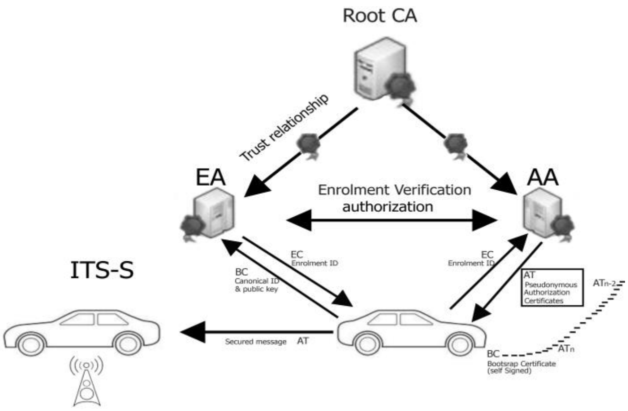
Root CA
Trust relationship
EA
AA
Enrolment Verification authorization
ITS-S
EC
Enrolment ID
BC
Canonical ID & public key
EC
Enrolment ID
AT
Pseudonymous Authorization Certificates
ATn-2
Secured message AT
BC
Bootsrap Certificate (self Signed)
ATn

Fig. 3. The C-ITS PKI architecture.

Furthermore, communications between V2X devices are about implemented messages being sent to and from vehicles or Road-side Units (RSUs). After receiving the hash, the vehicle can verify that the contents received from another vehicle have not been modified in transit by calculating and comparing the hash of the content with the one received by the vehicle. In the hash chain, the only packet in the chain that is not integrity protected is the first packet. Subsequently, we can use the private key's role to provide the first packet's integrity and protection to make the integrity safe. The signature calculation involves computing the hash of the message and encrypting the hash with the private key. Also, the benefit of the hash chain is the lightweight computing power requirements compared to other cryptographic algorithms.

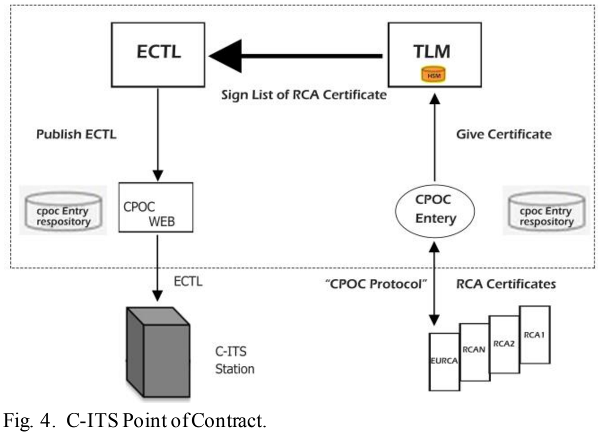

Fig. 4. C-ITS Point of Contract.

IV. OVERVIEW OF THE BLOCKCHAIN TECHNOLOGY

A. *Background on the hash chain*

The hash chain is the sequential implementation of the hash function encoded over a piece of data. Also, it is a transaction that takes an input length that passes through a hashing algorithm and then gives an output with a fixed length, as seen in Figure 5. Moreover, the hash chain helps to protect the security of sending any message against tampering. To be considered as a secure hash chain, some requirements of the hash function should be satisfied. The first case should be deterministic, implying that the hash function's input gives the same output every time. Second, a quick computation, the hash function, should be able to return the hash's input quickly. The thirdv is preimage resistance; after knowing the output of the hash function H(x), it will be impossible to see the input of the function (x). Furthermore, any change to the content data would produce a different hash, as stated above. Finally, collision resistance means that two different inputs will have two different hash outputs with high probability.

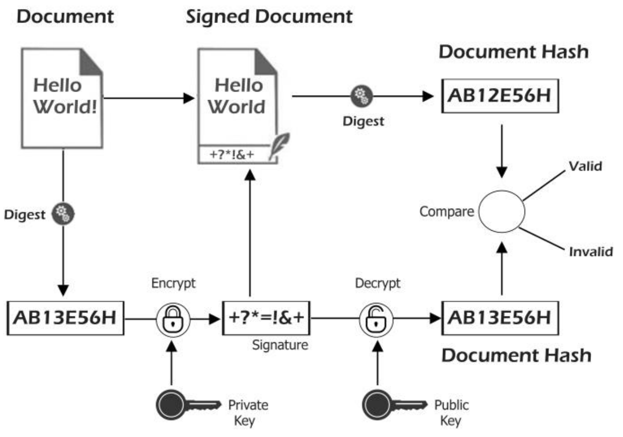

Fig. 5. Digital signature based on cryptographic hash (digest).

The hash chain is a technology used in Bitcoin to transfer digital coins from one individual to another and later the blockchain network's cornerstone. Consequently, all the above process is the key to creating the chain between messages that are called the Blockchain.

One application of the hash chain was the DHT (Distributed Hash Tables) network.

B. *Basics of Blockchain*

For the first time, the Blockchain was introduced by Satoshi Nakamoto as a peer-to-peer electronic cash system in 2008 [33]. When he published a paper entitled "Bitcoin": "A peer-to-peer electronic cash system, " which introduced an innovative and novel way to transfer (send and receive) digital money (called crypto-currency) without the need of going through a trusted third party.

The Blockchain is based on an immutable digital ledger that records all transactions verifiably and consistently. The ledger is replicated across several nodes, which means that no single authority owns or maintains it. The ledger's version validity is established through consensus among the participating nodes, also called miners. The transactions are stored in blocks linked using cryptography (hence the term Blockchain), explicitly using hash functions: each block stores the previous block's hash, timestamp, and transactions data. Therefore, data on a specific block cannot be altered without changing subsequent blocks, which requires the network's consensus. Each block holds a set of transactions and the previous block's hash, as seen in Figure 6 [34] below.

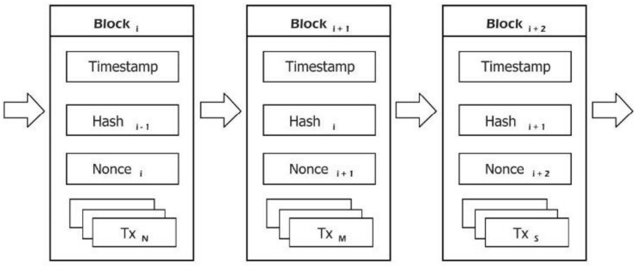

Fig. 6. General Blockchain blocks sequence.

The transactions are stored after verification throughout the network. The verification is via consensus between the nodes; there are different methods to achieve consensus. Information in Blockchain cannot be added or modified until the consensus is reached, making it fraud-proof.

C. *Ethereum and decentralized applications (DApps)*

The exchange of digital currency was the primary purpose of Bitcoin. Afterward, researchers started developing platforms based on Blockchain technology for running distributed software called decentralized applications (DApps) development through "Smart Contracts". A smart contract is a computer code running over Blockchain capable of exchanging any value a third party needs. They offer the following advantages over the existing computer programs: 1) Autonomous: the network, 2) Manage their execution Trust-less: the ledger's version is validated with consensus among nodes, 3) Data safe: the application's data remain permanently in the Blockchain, 4) Transparent: smart contract's code and storage are publicly available. Ethereum is one example of a DApps blockchain network [35].

V. V2X EXTENSIONS/MODIFICATIONS USING BLOCKCHAIN

Blockchain technology started to be considered in V2X systems research areas. The Blockchain n etworks can be applied in many use cases not limited listed briefly below. The Blockchain offers information trust because event data is maintained on a publicly achievable blockchain. It provides the secure flow of data between network objects (Vehicle, RSU servers). The Blockchain can solve the safety for the transfer of important data and reliable information transmission, while preventing deformation, which may result in negative outcomes. To avoid these outcomes, Blockchain technology is based on rules and principles. Because of the nature of blockchain trust management, it can be successfully implemented across nodes in decentralized networks. Using blockchain could prevent harmful nodes from accessing the network and disseminating misleading information on the network, creating disruptions of the transportation network. In some use cases, blockchain can be applied to rate a road user in V2X system, taken against offenders. This will guarantee that harmful messages that harm the V2X system or degrade its efficiency are decreased. The use of trust management algorithms and priority separation allows traffic users to assess if a received message is credible with a high degree of certainty.

Blockchain could provide the flexibility to store and distribute the public keys or the vehicle certificates without the need of a 3rd party (trusted or not trusted) and, therefore, the generation of secure sessions between devices. It enables security between devices from different organizations. In some use cases, the immutably shared data among many devices and organizations. But on the other hand, Blockchain is not a mature technology yet. The transaction cost is increasing with digital currency prices and the scalability of the network should be also considered.

There were some proposals to use blockchain technology to ensure the security of V2X and mitigate the security issues listed above. The main advantage of Blockchain technology's application in V2X is the simple implementation of the trust authentication between vehicles, including the messages' integrity and confidentiality. The standard mechanism of security and privacy of the messages described by, e.g., the C-ITS could be simplified using the Blockchain.

Here we provide a summary of two existing survey papers on V2X and Blockchain. The document [36] lists articles around the integration of three technologies in one network: the 5G, Edge Cloud nodes, and Blockchain, showing this approach's advantages in Cellular V2X networks. The paper lists a comparative study of Blockchain in advanced vehicular networks with 5G-based edge computing and introduces the open issues like the storage in Blockchain with a massive volume of data transactions, the performance due to the limited throughput in terms of the number of transactions per second, delay, and network resource usage when blockchain and 5G-based MEC are integrated. The survey lists papers indicating that Blockchain consumes large network resources related to the mining and emphasizes that the consensus mechanism could result in high latency. The survey provides a future direction for research which could be to develop an efficient and robust incentive mechanism to encourage all parties and miners to engage in the blockchain. In addition, it suggests penalty systems to discourage any harmful activities. As a conclusion, the paper states that the Blockchain has emerged as a promising technology to solve most issues and challenges related to privacy, security, and networking faced by the existing and next-generation V2X technologies.

Whereas, survey document [37] lists research articles around the processing power and efficient trust mechanisms for information exchange in V2X communications and Intelligent Transportation Systems (ITS). Traditional access to the remote cloud may degrade the V2X services due to incurred latency. This survey lists and examines important solutions written around Edge solutions and Blockchain applied to V2X or what is called Internet of Vehicles (IoV) and provides a related technical classification from access technology, IoV architecture layers, network layers including SDN and NFV, blockchain layers execution and finally algorithms and applicability of machine learning through a comparative summary. It highlights their main features, advantages, and limitations to provide subsidies for further proposals.

Our actual survey includes the latest written papers onV2X solutions where the Blockchain is also the main component. Our survey is general, not limited to any specific technical topics or feature areas within Blockchain applications in V2X. On the contrary, the survey [36] covers only papers related to V2X, 5G, edge computing, and Blockchain integration only. After an exhaustive explanation of the V2X systems and their issues, the security and V2X evolution are the main focus. They list research papers related to this subject and do a comparative study of Blockchain with 5G and edge computing from system characteristics, considering the following parameters: the Blockchain type / consensus algorithm / edge solution / cellular technologies.

On the other hand, the survey [37] provides a taxonomy of bockchain and edge computing technologies for papers written in the context of IoV by analyzing the Blockchain type, the Blockchain layer, the adopted consensus algorithm, and the architectural approach.

Based on the identified gaps, we have reviewed several recent works not covered by the above available surveys but related to V2X systems and blockchain/hash chain technologies. We highlight the proposals' main idea, advantages, and weaknesses for each selected paper in the below sections.

A. Traceable and Authenticated Key Negotiations via Blockchain for Vehicular Communications:

In paper [38], authors analyze the communication between vehicles and between vehicles and people, and analyze requirements of low latency, high reliability, and traceability. The paper gets the Master Key (MK) information on blockchain and realize the master key negotiation. The proposed scheme utilizes a transaction data structure to generate key pairs like the Diffie–Hellman key-exchange process. This is achieved through four algorithms where the system parameters are generated and stored in blockchain, master key parameters in blockchain, and one algorithm to generate from the master key parameters the master key in the blockchain. This proposal can resist MiM and packet dropping attacks, and others. The key materials can be traced back by timestamps upon request and can be confirmable to avoid decryption failure attacks. The main issue is the long and unpredictable time to create secure connectivity due to blockchain latency.

B. A Secure Priority Vehicle Movement based on Blockchain Technology in Connected Vehicles:

A novel blockchain architecture was presented in paper [51], which protects vehicles from any attack, isolates them from other vehicles, and reduces the number of potential threats they will encounter. Their proposal could be modified to accommodate the priority vehicles' speeds to accommodate the Blockchain architecture. According to the specified maximum speed, the priority vehicle can travel through all the RSUs and reach its destination without any information-sharing mechanism between the RSUs and the priority vehicle. This is what we consider the proposal's vulnerability. On the other hand, the system is based on an ideal security system that exchanges information between priority vehicles and the RSUs without allowing anyone to communicate with them.

This system builds the authenticity and integrity between the RSU and the authentication center and the vehicles with the RSU in another way. Also, the hash chain makes the communication between the vehicle and the RSU secure.

C. A Tiered Blockchain Framework for Vehicular Forensics:

The authors of [52] developed a concept for vehicle forensics using blockchain technology,. An analysis of the security levels that a car should pass through in the aftermath of an accident using blockchain technology and their resiliency to attack. The authors have contrasted and studied their proposed blockchain system (Block4Forensic) with other Blockchain systems for conflict resolution and responsibility attribution, demonstrating the strength of their proposed structure.

D. Block-VN: A Distributed Blockchain-Based Vehicular Network Architecture in Smart City:

In paper [39], the authors Proposed a distributed system based on blockchain for the ad hoc vehicle network. This modern network was called Blockchain-Based Vehicular Network (Block-VN) and allowed vehicles to explore and exchange their resources to build a network of vehicles that work together to deliver value-added services like forensics after a car accident occurs. The car's security level passed through a blockchain and analyzed. Furthermore, the authors discuss the architecture's security and dependability.

E. A Novel Sender Authentication Scheme Based on Hash Chain for Vehicular Ad-Hoc Networks:

The authors of paper [40] presented a hash chain scheme for promoting VANET security and secure communication between the vehicle, RSU, and authentication center. The authors used the symmetric key in hash chaining. The asymmetric keys were not considered because the symmetric key provides faster encryption and decryption in a secure network compared to the asymmetric keys.

The idea of this paper was to develop the symmetric hash chain process to strengthen the authenticity and integrity between the RSU and authentication center in one sense and the vehicles with the RSU in another sense. As a result of the hash chain, the communication between the Vehicle and RSU is secure and resistant to various attacks.

F. Comparative Experiments of V2X Security Protocol Based on Hash Chain Cryptography:

In paper [53], the authors proposed a lightweight message authentication and privacy preservation protocol for V2X communications. The proposed protocol achieves highly secure message authentication by introducing a hash chain of secret keys for a Message Authentication Code (MAC). The reason is that V2X security protocols based on the Elliptic Curve Digital Signature Algorithm (ECDSA) provide a high-security level at the cost of excessive communication and computation overhead. The proposed protocol was tested in a stationary state using their proposed test platform using commercial DSRC devices (Cohda wireless MK5 (5th Generation Market) devices that provide two types MK5-OBU that are installed on the Vehicle and MK5-RSU installed on the road) [41]. By using the well-known Wireshark utility, they measured the messaging performance.

Furthermore, they enabled security by using the cryptographic Library (Aerolink Library) configuration that uses the Hardware Security Model (HSM). Moreover, for signing and verifying the messages, they used ECDSA National Institute of Standards and Technology (NIST) P256 with SHA 256. Therefore, using IEEE 1609.2 and ETSI-103-097 standards, the result for the number of messages per second was 183 messages. In contrast, for non-standard protocol, the number of messages per second was only 54 messages. The authors conclude that the proposed protocol significantly decreases the average end-to-end delay and proves its performance advantages over the standard and non-standard protocols.

G. Hash-Chain-Based Cross-Regional Safety Authentication for Space-Air-Ground Integrated VANETs:

Authors of article [42] presented a new concept of connectivity between vehicles, RSUs, and Certificate Authorities (Cas), with drones or Security Manager (SM) acting as intermediaries, sending information and data between them through a space air-ground integrated network (SAGIN) which establishes higher security standards. The authors developed a consensus framework based on the Hash chain, combined with the Radio Frequency (RF) fingerprint theory, simplifying the Blockchain, introducing the Kafka distributed messages, and Practical Byzantine Fault Tolerance Algorithm (PBFT). According to the simulation-based on Hyperledger–Fabric architecture, it shows that the average delay of the block produced by a single transaction is approximately 0.9ms, which achieves effective and low latency authentication.

H. A New-Type of Blockchain for Secure Message Exchange in VANET:

A new Blockchain form is presented in this paper [54] to address issues of critical message propagation in VANET environments. This Blockchain doesn't use any crypto coins to handle safety event messages. After determining the vehicle's location with the aid of proof of location (POL), the VANET messages don't have to go beyond the country's boundary. The scheme depends on each geographical area isolated from the other, which ensures that traffic information of one country is unrelated to vehicles based in another country. Furthermore, after the vehicle receives the message, it tests it against the Blockchain. It then verifies the event messages to see if they are trustworthy before broadcasting them to the surrounding vehicles and storing the message in the local memory pool or discarding them. The results of this paper's assessment and review suggest that the proposed local Blockchain can be used effectively in the VANET without the need for additional storage.

I. Secure V2X environment using Blockchain Technology:

In article [55], the authors' purpose is to provide a hypothetical scenario that depicts the effect of challenging factors on applying the Blockchain in the V2X paradigm. However, the authors have discussed considerations that may hurt the application of Blockchain in V2X context. A total of 10 of the most critical challenges are established using the Systematic Literature Review (SLR) method, and their corresponding hypothesis was also developed. Some studies were considered for the data extraction process by applying the tollgate method. They have explored in this study the factors that could have a negative impact on the implementation of blockchain in V2X environment. By considering both studies' results (SLR and case study), the authors have created a hypothetical model that helps practitioners revise their strategies and create an efficient method for successfully implementing Blockchain in the V2X context.

J. A Remote Attestation Security Model based on Privacy-Preserving Blockchain for V2X:

Intelligent, V2X-based applications require the real-time integration of all kinds of information on roads, pedestrians, the environment, and vehicles themselves. This information also needs to be shared and integrated privately with other vehicles. The authors of paper [29] suggest a remote attestation protection mechanism built on a privacy-preserving blockchain called the remote attestation model (RASM). This scheme entails two main stages. The first is the credible verification of identification. The second uses estimation for decision-making to classify the node trusted or malicious, for example.

K. BloCkEd: Blockchain-based Secure Data Processing Framework in Edge Envisioned V2X Environment:

The authors of article [56]. proposed a Blockchain-based data processing platform (BloCkEd) for the V2X environments, where the V2X users are connected to the EDGE nodes. The scheme allows V2X users' requests to be handled/processed by nodes at the edge of the network; thus, reducing latency; and preserving the privacy of user data/activities. BloCkEd comprises an optimal container-based data processing scheme; and a blockchain-based data integrity management scheme; designed to minimize link breakage and reduce latency. The program implementation of the proposed architecture was tested against a plausible scenario in Chandigarh City, Punjab, India. The results showed that the proposed solution promotes less migration due to an efficient allocation strategy, decreasing regular connection breaks and service disturbances.

L. Efficient Mining Cluster Selection for Blockchain-Based Cellular V2X Communications:

Using game theory, paper [57] demonstrates how to balance the load on mining clusters while ensuring unloading vehicles' justice. As mining tasks are unloaded in cellular V2X networks, they can cause congestion and disproportionate vehicle network resources. Moreover, a short block length transmission design was considered to meet the low-latency standards of safety applications. The proposed solution guarantees decent transmission speeds and preserves justice between the unloading of vehicles. The findings show that the proposed methodology's efficiency rises as the number of mining clusters in the network increases.

M. A Blockchain Approach for Decentralized V2X (D-V2X)

As we introduced above, the current V2X solutions rely on using a Public Key Infrastructure that enables secure collaboration between the different entities in the V2X ecosystem. However, managing such infrastructure requires reaching agreements between many parties with conflicts of interest between automakers and telecommunication operators.

In paper [43], the authors propose a decentralized V2X (D-V2X) solution based on Blockchain that does not need any trusted authority and can be applied on top of any communication protocol. The authors describe a proof-of-concept to build the D-V2X on top of a low-cost and high-security System-on-Chip (SoC) that could enable widespread D-V2X adoption.

N. PF-BVM: A Privacy-aware Fog-enhanced Blockchain Validation Mechanism

In paper [44], the authors suggested a Privacy-aware Fog-enhanced Blockchain Validation Mechanism (PFBVM) to reduce the load on the network by implementing a new validation mechanism and equivalent consensus feature, where trusted authenticated fog nodes can validate trans actions on behalf of blockchain nodes. It integrates fog computing, the Internet of Things, and Blockchain techniques. The PF-BVM algorithm aims to reduce the approval of a transaction and, in that way, to reduce the latency in Blockchain. PF-BVM allows trusted rich fog nodes to perform transaction validation on behalf of other blockchain nodes as a conceptual criterion. The trust is gained by randomly running matching tests which adds to the integration of fog computing. According to the findings, the greater the number of transactions per block, the higher the blockchain system's un-reliability metric. The authors used a specially formulated simulation code to analyze the proposed mechanism. The experimental results demonstrated that PF-BVM could significantly improve a blockchain system validation in time consumption, energy efficiency, and storage capacity.

O. Blockchain-based Service Sharing Via Roadside Unit-Performance Evaluation:

Using Blockchain technology, the authors proposed a model for services sharing via RSU [45], which has just one RSU that receives and saves services on Blockchain, and vehicles interact with each other via RSU. A simulation was implemented to estimate the performance of the system using Python. There are two forms of communication discussed: communication between vehicles and communication between vehicles and RSUs. When the vehicle agrees to share its services with a requested vehicle, a smart contract will be established between two vehicles, provided both agree to the smart contract regulations.

P. Technological Aspects of Blockchain Application for Vehicle-to-Network:

In paper [46], the authors suggested using Blockchain technology in V2N to tackle the problem of maintaining information security, which is very sensitive related to the specifics of the operation of transport networks. Four experiments were conducted to demonstrate the numerical features for resource allocation on devices engaged in arranging V2N communication. The findings show that the nodes' activity determines the channel bandwidth consumed. During blockchain operation, the latency of packets between nodes decreased significantly, and there was almost no influence on the delay with the nodes of another network. In comparison, the latency variation in operating the blockchain failed nodes simultaneously without synchronizing the mining interaction did not occur significantly between the nodes.

Q. Blockchain Enhanced V2X Communication System and Method:

In this patent application [47], the authors propose an authentication system for V2X communication systems based on a private blockchain. The system includes a blockchain-based V2X decentralized Certificate Authority (CA) instead of a third-party CA. A blockchain-based V2X CA provides an open, distributed ledger that can efficiently record transactions between multiple parties in a verifiable and permanent way.

R. Distributed Edge Computing with Blockchain Technology to Enable Ultra-Reliable Low-Latency V2X Communications:

Paper [48] aims to solve the problem of building a vehicular network for reliable delivery data according to the V2X standard and improving road users' safety using blockchain technology and Mobile Edge Computing (MEC). Again, here the authors of this paper consider the four technology 5G, V2X, MEC, and blockchain. The proposed work provides a mathematical model of the system, considering the interconnection of objects and V2X information channels and an energy-efficient offloading algorithm to manage traffic offloading to the MEC server.

The proposed system architecture consists of roadside participants like vehicles, several RSUs, distributed MEC units, and the application server. The blockchain technology can be used to manage information trustworthiness, as event information would be stored in a publicly accessible blockchain. Blockchain can solve major problems faced by V2X systems and provide security for the distribution of critical information. One scenario is that Malicious nodes can infiltrate the network and spread false information, causing the transport network to fail. The blockchain can rate a road user is also an effective solution for use in the V2X system. A rating facility would allow action against offenders and encourage decent users.

The paper provides a framework of V2X based on distributed edge computing integrated with blockchain technologies. A model for the interaction of blockchain technology in the system was introduced to achieve the required level of security. The developed Blockchain–MEC model was evaluated over an NS-3 environment for various simulation scenarios, and the results validate the system in terms of reliability, latency, and energy efficiency. The results showed that Blockchain–MEC V2X system achieved higher reliability than existing V2X models.

S. Blockchain for V2X: A Taxonomy of Design Use Cases and System Requirements:

Article [49] provides an overview of V2X blockchain architecture applications and examines them in order to define the needs of a V2X blockchain. The study investigates possible blockchain applications in the V2X space, identifying and assessing use cases based on their underlying blockchain needs. The authors classify blockchain into two categories: permissionless and permissioned blockchains. According to the authors, permissioned blockchains are the greatest solution for enabling the largest range of applications while also ensuring that throughput, user privacy, and Know Your Costumer (KYC) requirements are all satisfied.

T. A blockchain-based V2X communication system:

A new blockchain-based V2X secure communication platform was proposed in this paper [50], which integrates PKI/CA model aspects with blockchain technology. The authors describe a typical PKI/CA-based alternative solution to the European standard C-ITS' authentication. The solution attempts to alleviate trust problems in the existing PKI/CA infrastructure while also facilitating vehicle authentication and security in the V2X network. The platform is based on the Ethereum blockchain to store and retrieve the Public keys of the roadside participants and RSU.

Table 1: A comparative analysis of the surveyed V2X papers related to Blockchain technologies.

Author	Technology	Use case	Description	Brief Summary of Results
Y. Chen et al. [38], 2019	Blockchain/ Authenticated key negotiations	Vehicular communication	A Blockchain to resolve the key negotiation between two vehicles to be authenticated and traceable.	The Key materials can be publicly tracked back by timestamps and confirmed to prevent decryption failure attacks.
A. Saini et al. [51], *2019*	Blockchain/ Privacy and security	Connected Priority vehicles	A novel blockchain architecture that protects vehicles from many attacks and isolates them from other vehicles.	The proposed scheme will efficiently and safely address priority vehicle movement.
M. C. Ugwu et al. [52], 2018	Blockchain/ Watchdog entity	Vehicular Forensics	A blockchain concept for vehicular forensics; after an accident occurs, the car's security level should pass through blockchain technology and analyze them against attack.	Demonstrates the proposed architecture's effectiveness compared to the current Blockchain-based system.
Pradip Kumar Sharma et al. [39], 2017	Blockchain/ Block-VN	Ad hoc Vehicle network	An ad hoc network application and discovered capabilities that the current infrastructure cannot quickly provide.	The Block-VN paradigm encourages vehicles to explore and exchange their resources, resulting in a network of vehicles cooperating to create value-added services.
N. V. Vighnesh et al. [40], 2011	Blockchain/ Hash chain	Vehicular ad hoc network (VANET)	Hash chain scheme that promotes VANET security and secure communication between the vehicle, RSU, and authentication center.	Its widespread use in crypto-graphy explains the popularity of the hash function.
S. A. A. Hakeem et al. [53], 2020	Blockchain/ MAC algorithm	Vehicle-to-Everything (V2X)	Security protocols have been tested in a stationary state using commercial DSRC devices.	The proposed protocol significantly decreases the average end-to-end delay.
G. Luo et al. [42], 2020	Hash chain/ space–air–ground integrated network (SAGIN)	VANETs	A new idea of communication between vehicles that plays the role of sending information and data between them and use the space-air-ground integrated network (SAGIN) to set out higher security standards.	The average delay of the block produced by a single transaction is approximately 0.9ms to achieve effective and low latency authentication.
R. Shrestha et al. [54], 2020	Blockchain/ Mobile Edge Computing	VANET	A new form of Blockchain to address issues of critical message propagation in VANET.	The proposed local Blockchain can be used effectively in the VANET without the need for additional storage.
Ms. Taiyaba et al. [55], 2020	Blockchain/ Systematic literature review (SLR)	V2X	Provides a hypothetical scenario that depicts the effect of challenging factors on applying the Blockchain in the V2X paradigm.	A hypothetical model was created that helps practitioners revise their strategies and develop efficient methods for successfully implementing Blockchain in the V2X context.
C. Xu et al. [29], *2018*	Blockchain/ Remote attestation security Model (RASM)	V2X	A remote attestation protection mechanism built on a privacy-preserving blockchain called the remote attestation model RASM.	The findings demonstrate that a high proportion of progress can be attained with the scheme.
G. S. Aujla et al. [56], 2020	Blockchain/ BlockED	V2X	A blockchain-based protected data processing system for an EDGE node of the V2X area called BloCkEd.	The proposed solution promotes less migration due to an efficient allocation strategy, decreasing regular connection breaks and service disturbances.
F. Jameel et al. [57], 2020	Blockchain/ Blocklength transmission	V2X	A game-theoretic approach to balance the load on mining clusters while ensuring the justice of unloading vehicles.	The findings show that the proposed methodology's efficiency rises as the number of mining clusters in the network increases.

I. *Agudo et al.* [43], 2020	Blockchain/ System-on-Chip (SoC)	V2X	Decentralized V2X (D-V2X) solution based on Blockchain, that does not need any trusted authority and can be applied on top of any communication protocol.	The Current V2X solutions rely on using a public key infrastructure that enables secure collaboration between the different entities in the V2X ecosystem.
H. Baniata et al. [44], 2020	Blockchain/ Internet of things, Fog computing	Vehicle	Privacy-aware Fog-enhanced Blockchain Validation Mechanism (PFBVM).	PF-BVM could significantly improve a blockchain system validation in terms of time consumption, energy efficiency, and storage capacity.
I. Kiran et al. [45], 2019	Blockchain/ Proof of Work (PoW)	V2V, V2I	They are examining the performance of the vehicle to vehicle and vehicle to RSU communication at the time of service sharing. Its primary purpose is to minimize average time delay.	RSU helps to minimize the average delay time to achieve maximum throughput.
V. Elagin et al. [46], 2020	Blockchain	V2N	Blockchain is employed as a system platform to serve the demands of transportation systems for safe information sharing.	The usage of blockchain technology is not an appropriate solution for V2N.
Qi. Jimmy et al. [47], 2020	Blockchain/ Certificate Authority (CA), PKI	V2X	Patent Application for V2X decentralized CA based on blockchain instead of third-party CA.	Authentication system for V2X communication based on private blockchain.
A. Vladyko et al. [48], 2022	Blockchain/ mobile edge computing (MEC)/ 5G	V2X	The simulation model consists of roadside participants (vehicles, RSUs, distributed MEC units, and application server). The model was evaluated over an NS-3 environment for various simulation scenarios.	Validation of the system in terms of latency, reliability, and energy efficiency. Blockchain-MEC V2X system achieved higher reliability than existing V2X models.
J. Meijers et al. [49], 2021	Blockchain/ IoT	V2X	Investigating potential blockchain applications in the V2X, finding and evaluating use cases based on their underlying blockchain requirements.	Permissioned blockchains are the greatest solution for enabling the largest range of applications.
H. Farran et al. [50], 2021	Blockchain/ Public Key Infrastructure (PKI), CA	V2X	A blockchain to resolve the existing PKI/CA infrastructure's trust concerns and facilitate the authentication and security of the vehicles in the V2X network.	A platform based on Ethereum blockchain to store and retrieve the public keys of the roadside participants and RSU.

II. CONCLUSION

By way of inference, safety is the primary issue for road drivers using highly advanced applications in the future's highly cooperative ITS environments. V2X has the potential to comply with safety criteria providing updates to drivers on the road. Hence, it is necessary to ensure the network's security and establish confidence in V2X interactions. This paper provides a comprehensive survey on different vehicular applications using blockchain technologies to enhance the main message from the studied articles is that the Blockchain offers reliability, trust, and simplification in implementing security to V2X networks. Blockchain-based solutions construct durability and reliability in V2X, together with distributed operation and data storage.

Based on this survey, we conclude that blockchain networks and technology can play an important role in V2X applications from different aspects and resolve many technical issues. We enumerate the following: 1) traceable key negotiation between two vehicles; 2) protection of vehicles from many attacks and isolates them from other vehicles; 3) security and secure communication between the vehicle, RSU, and authentication center; 4) ad hoc network application and discovered capabilities; 5) vehicular forensics after an accident incidence; 6) security between devices from different organizations; 7) the immutably shared data among many devices and organization; 8) simplifying the distribution of the participants' CA in V2X; 9) improving the performance of the V2X system when combined with EDGE node in terms of latency, reliability, and energy efficiency; and 10) trust authentication between vehicles, including the messages' integrity and confidentiality. We expect that the list of functions will further improvse, and implementation of V2X systems based on Blockchain will increase in the coming years.

On the other hand, Blockchain is not mature technology yet and requires a lot of improvements in scalability, transactions latency, and cost.

Preparing this survey taught us that Blockchain quickly became an important topic also in V2X communications. As a part of our future work, we design a novel Blockchain-based proof-of-concept V2X security solution to highlight possibilities and implement security on such new based in the C-ITS domain. Our primary purpose is to increase awareness of Blockcahin+V2X and to create a lightweight, distributed pilot alternative to the PKI-based current schemes and the complicated assignment of the CAs to the vehicles or IoT devices in general by a more generic and simplified method based on the Ethereum Blockchain.

REFERENCES

[1] 5GAA, "White Paperon ITS spectrum utilization in the Asia Pacific [22] Region White paper on ITS spectrum utilization in the Asia Pacific Region," p. 20, 2018.

[2] 5G American, "5G Americas White Paper: Cellular V2X Communications Towards 5G," Http://Www.5Gamericas.Org, 2018.

[3] A. Boudguiga, A. Kaiser, and P. Cincilla, "Cooperative-ITS Architecture and Security Challenges: a Survey," *22th ITS World Congr.*, no. October, pp. 5–9, 2015.

[4] S. Rangarajan, M. Verma, A. Kannan, A. Sharma, and I. Schoen, "V2C: A secure vehicle to cloud framework for virtualized and on-demand service provisioning," in *ACM International Conference Proceeding Series*, 2012, pp. 148–154, **DOI**: 10.1145/2345396.2345422.

[5] D. P. Tuttle, R. L. Fares, R. Baldick, and M. E. Webber, "Plug-In Vehicle to Home (V2H) duration and power output capability," in *2013 IEEE Transportation Electrification Conference and Expo: [26] Components, Systems, and Power Electronics - From Technology to Business and Public Policy, ITEC 2013*, 2013, **DOI**: 10.1109/ITEC.2013.6574527.

[6] Alfonso Damiano, Gianluca Gatto, Ignazio Marongiu, Mario Porru, and Alessandro Serpi, "Vehicle-to-Grid Technology: State-of-the-Art and Future Scenarios," *J. Energy Power Eng.*, vol. 8, no. 1, 2014, **DOI**: 10.17265/1934-8975/2014.01.018.

[7] I. S. Victor Sandonis and M. U., Maria Calderon, "Vehicle to Internet communications using the ETSI ITS GeoNetworking protocol," *Trans. Emerg. Telecommun. Technol.*, vol. 25, no. 3, pp. 294–307, 2016, **DOI**: 10.1002/ett.

[8] J. Wang, Y. Shao, Y. Ge, and R. Yu, "A survey of vehicle to everything (V2X) testing,"*Sensors (Switzerland)*, vol.19, no. 2, pp. 1–20, 2019, **DOI**: 10.3390/s19020334.

[9] "Vehicle-to-everything-Wikipedia." [Online]. Available: https://en.wikipedia.org/wiki/Vehicle-to-everything. [Accessed: 29-Apr-2020].

[10] H. Leung, N. E. El Faouzi, and A. Kurian, "V2X Communication Protocol in Vanet for Co-Operative Intelligent transportation system (ITS)," Inf. Fusion, vol. 12, no. 1, pp. 2–3, 2011, **DOI**: 10.1016/j.inffus.2010.06.003.

[11] C. R. Storck and F. Duarte-Figueiredo, "A Survey of 5G Technology Evolution, Standards, and Infrastructure Associated with Vehicle-to-Everything Communications by Internet of Vehicles," *IEEE Access*, vol. 8, pp. 117593–117614, 2020, **DOI**: 10.1109/ACCESS.2020.3004779.

[12] M. Lu, O. Turetken, O. E. Adali, J. Castells, R. Blokpoel, and P. Grefen, "Cooperative Intelligent Transport Systems (C-ITS) [34] deployment in Europe: Challenges and key findings," *25th ITS World Congr.*, no. September, p. EU-TP1076, 2018.

[13] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym Schemes in Vehicular Networks: A Survey," *IEEE Commun. Surv. Tutorials*, vol. 17, no. 1, pp. 228–255, 2015, **DOI**: 10.1109/COMST.2014.2345420.

[14] M. H. Eiza and Q. Ni, "Driving with Sharks: Rethinking Connected Vehicles with Vehicle Cybersecurity," *IEEE Veh. Technol. Mag.*, vol. 12, no. 2, pp. 45–51, Jun. 2017, **DOI**: 10.1109/MVT.2017.2669348.

[15] J. B. Kenney, "Dedicated short-range communications (DSRC) standards in the United States, "*Proc. IEEE*, vol. 99, no. 7, pp. 1162–1182, 2011, **DOI**: 10.1109/JPROC.2011.2132790.

[16] D. Jiang and L. Delgrossi, "IEEE 802.11p: Towards an international standard for wireless access in vehicular environments," *IEEE Veh. Technol. Conf.*, no. June 2008, pp. 2036–2040, 2008, **DOI**: 10.1109/VETECS.2008.458.

[17] F. Arena, G. Pau, and A. Severino, "A review on IEEE 802.11p for intelligent transportation systems," *J. Sens. Actuator Networks*, vol. 9, no. 2, pp. 1–11,2020, **DOI**: 10.3390/jsan9020022.

[18] I. V. T. Society, IEEE Standard for Wireless Access in Vehicular Environments - Security Services for Applications and Management Messages, vol. 2017. 2016.

[19] J. Kolleda et al., "National Security Credential Management System (SCMS) Deployment Support : Literature Search Report," 2018.

[20] C-ITS Platform, "Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS)," no. June, pp. 1–79, 2018.

[21] T. Giannetsos et al. "Securing V2X Communications for the Future: Can PKI Systems offer the answer?" [Online]. Available: https//www.researchgate.net/publication/335089342_Securing_V2X_Communications_for_the_Future_Can_PKI_Systems_offer_the_answer. [Accessed: 19-Feb-2021].

[22] B. Brecht et al., "A Security Credential Managment System for V2X Communications," vol. 19, no. 12, pp. 3850–3871, 2018, **DOI**: 10.1109/TITS.2018.2797529.

[23] "Public key encryption (article) | Khan Academy." [Online]. Available: https://www.khanacademy.org/computing/computers-and-internet/xcae6f4a7ff015e7d:online-data-security/xcae6f4a7ff015e7d:data-encryption-techniques/a/public-key-encryption. [Accessed: 20-Feb-2021].

[24] A. Sulaiman, S. V. Kasmir Raja, and S. H. Park, "Improving scalability in vehicular communication using one-way hash chain method,"Ad Hoc Networks, vol. 11, no. 8, pp. 2526–2540, 2013, **DOI**: 10.1016/j.adhoc.2013.05.017.

[25] A. Ghosal and M. Conti, "Security issues and challenges in V2X: A Survey," Comput. Networks, vol. 169, no. March 2019, 2020, **DOI**: 10.1016/j.comnet.2019.107093.

[26] G. Samara, W. A. H. Al-Salihy, and R. Sures, "Security analysis of Vehicular Ad Hoc Networks (VANET)," *Proc. - 2nd Int. Conf. Netw. Appl. Protoc. Serv. NETAPPS 2010*, pp. 55–60, 2010, **DOI**: 10.1109/NETAPPS.2010.17.

[27] Xin Wang University of California, Santa Cruz, "Mobile Ad-Hoc Network Applications". Iva Lipovic, 2011.

[28] T. Zhou, R. R. Choudhury,P. Ning, and K. Chakrabarty, "P2DAP - Sybil attacks detection in vehicular ad hoc networks," *IEEE J. Sel. Areas Commun.*, vol. 29, no. 3, pp. 582–594, Mar. 2011, **DOI**: 10.1109/JSAC.2011.110308.

[29] C. Xu, H. Liu, P. Li, and P. Wang, "A remote attestation security model based on privacy-preserving blockchain for V2X," *IEEE Access*, vol. 6, no. c, pp. 67809–67818, 2018, **DOI**: 10.1109/ACCESS.2018.2878995.

[30] M. A. Hezam Al Junaid, A. A. Syed, M. N. Mohd Warip, K. N. Fazira Ku Azir, and N. H. Romli, "Classification of Security Attacks in VANET: A Review of Requirements and Perspectives, "*MATEC Web Conf.*, vol. 150, pp. 1–7, 2018, **DOI**: 10.1051/matecconf/201815006038.

[31] M. Pirretti, S. Zhu, N. Vijaykrishnan, P. McDaniel, M. Kandemir, and R. Brooks, "The sleep deprivation attack in sensor networks: Analysis and methods of defense," Int. J. Distrib. Sens. Networks, vol. 2, no. 3, pp. 267–287, 2006, **DOI**: 10.1080/15501320600642718.

[32] V. Hoa La and A. Cavalli, "Security Attacks and Solutions in Vehicular Ad Hoc Networks: A Survey," Int. J. AdHoc Netw. Syst., vol. 4, no. 2, pp. 1–20,Apr.2014, **DOI**: 10.5121/ijans.2014.4201.

[33] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," SSRN Electron. J., 2019, **DOI**: 10.2139/ssrn.3440802.

[34] E. F. Kfoury, J. Gomez, J. Crichigno,E. Bou-Harb, and D. Khoury, "Decentralized Distribution of PCP Mappings over Blockchain for End-to-End Secure Direct Communications," *IEEE Access*, vol. 7, no. August, pp. 110159–110173, 2019, **DOI**: 10.1109/ACCESS.2019.2934049.

[35] "Ethereum Whitepaper | ethereum.org." [Online]. Available: https://ethereum.org/en/whitepaper/.[Accessed: 15-May-2021].

[36] R. Shrestha, S. Y. Nam, R. Bajracharya, and S. Kim, "Evolution of V2X communication and integration of blockchain for security enhancements," *Electron.*, vol. 9, no. 9, pp. 1–33, 2020, **DOI**: 10.3390/electronics9091338.

[37] A. Queiroz, E. Oliveira, M. Barbosa, and K. Dias, "A Survey on Blockchain and Edge Computing applied to the Internet of Vehicles," I*nt. Symp. Adv. Networks Telecommun. Syst. ANTS*, vol. 2020-December, 2020, **DOI**: 10.1109/ANTS50601.2020.9342818.

[38] Y. Chen, X. Hao, W. Ren,andY. Ren,"TraceableandAuthenticated Key Negotiations via Blockchain for Vehicular Communications," *Mob. Inf. Syst.*, vol. 2019, 2019, **DOI**: 10.1155/2019/5627497.

[39] P. K. et al. Sharma, "Block-VN: A Distributed Blockchain Based Vehicular Network Architecture in Smart City." .

[40] N. V. Vighnesh, N. Kavita, S. R. Urs, and S. Sampalli, "A novel sender authentication scheme based on hash chain for Vehicular Ad-Hoc Networks," *ISWTA 2011 - 2011 IEEE Symp. Wirel. Technol. Appl.*, pp. 96–101, 2011, **DOI**: 10.1109/ISWTA.2011.6089388.

[41] O. Unit, "MK5OBUCohda Wireless'5th generation market ready."

[42] G. Luo, M. Shi, C. Zhao, and Z. Shi, "Hash-chain-based cross- regional safety authentication for space-air-ground integrated VANETs," Appl. Sci., vol. 10, no. 12, p. 4206, 2020, doi: 10.3390/APP10124206.

[43] I. Agudo, M. Montenegro-Gomez, and J. Lopez, "A Blockchain Approach for Decentralized V2X (D-V2X)," *IEEE Trans. Veh. Technol.*, 2020, DOI: 10.1109/TVT.2020.3046640.

[44] H. et al. Baniata, "PF-BVM: A Privacy-aware Fog-enhanced Blockchain Validation Mechanism." [Online]. Available: https://www.researchgate.net/publication/341482783_PF-BVM_A_Privacy-aware_Fog-enhanced_Blockchain_Validation_Mechanism. [Accessed: 20-Mar-2021].

[45] I. Kiran and N. Javaid, "Blockchain-based Service Sharing Via Roadside Unit-Performance Evaluation, "no. July, 2019.

[46] V. Elagin, A. Spirkina, M. Buinevich, and A. Vladyko, "Technological aspects of blockchain application for vehicle-to-network," Inf., vol. 11, no. 10, pp. 1–19, 2020, DOI: 10.3390/info11100465.

[47] Q. Jimmy et al. "Blockchain Enhanced V2x Communication System And Method." [Online]. Available: https://uspto.report/patent/app/20200145191.[Accessed:22-Feb-2022].

[48] A. Vladyko, V. Elagin, A. Spirkina, A. Muthanna,and A. A. Ateya, "Distributed Edge Computing with Blockchain Technology to Enable Ultra-Reliable Low-Latency V2X Communications," *Electron.*, vol. 11, no. 2, pp. 1–18, 2022, DOI: 10.3390/electronics11020173.

[49] J. Meijers et al., "Blockchain for V2X: A Taxonomy of Design Use Cases and System Requirements," *2021 3rd Conf. Blockchain Res. Appl. Innov. Networks Serv. BRAINS 2021*, pp. 113–120, 2021, DOI: 10.1109/BRAINS52497.2021.9569796.

[50] H. Farran, D. Khoury, E. Kfoury, and L. Bokor, "A blockchain-based V2X communication system," *2021 44th Int. Conf. Telecommun. Signal Process. TSP 2021*, pp. 208–213, 2021, DOI: 10.1109/TSP52935.2021.9522599 .

[51] A. Saini, S. Sharma, P. Jain, V. Sharma, and A. K. Khandelwal, "A secure priority vehicle movement based on blockchain technology in connected vehicles," *ACM Int. Conf. Proceeding Ser.*, 2019, DOI: 10.1145/3357613.3357631.

[52] M. C. Ugwu, I. U. Okpala, C. I. Oham, and C. I. Nwakanma, "A Tiered Blockchain Framework for Vehicular Forensics," *Int. J. Netw. Secur. Its Appl.*, vol. 10, no. 5, pp. 25–34, 2018, DOI: 10.5121/ijnsa.2018.10503.

[53] S. A. A. Hakeem, M. A. A. El-Gawad, and H. Kim, "Comparative experiments of V2X security protocol based on hash chain cryptography," *Sensors (Switzerland)*, vol. 20, no. 19, pp. 1–23, 2020, DOI: 10.3390/s20195719.

[54] R. Shrestha, R. Bajracharya, A. P. Shrestha, and S. Y. Nam, "A new type of blockchain for secure message exchange in VANET," *Digit. Commun. Networks,* vol. 6, no. 2, pp. 177–186, 2020, DOI: 10.1016/j.dcan.2019.04.003.

[55] M. Taiyaba, M. A. Akbar, B. Qureshi, M. Shafiq, M. Hamza, and T. Riaz, "Secure V2X Environment using Blockchain Technology," *ACM Int. Conf. Proceeding Ser.,* no. April, pp. 469–474, 2020, DOI: 10.1145/3383219.3383287.

[56] G. S. Aujla et al., "BloCkEd: Blockchain-based secure data processing framework in edge envisioned V2Xenvironment, "*IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 5850–5863, 2020, DOI: 10.1109/TVT.2020.2972278.

[57] F. Jameel, M. A. Javed, S. Zeadally, and R. Jäntti, "Efficient Mining Cluster Selection for Blockchain-based Cellular V2X Communications," arXiv, pp. 1–9, 2020, DOI: 10.1109/tits.2020.3006176.

Hassan Farran received a B.S. degree in Computerand Communication Engineering from the American University of Science and Technology (AUST) Beirut, Lebanon in 2015 and an M.Sc. degree from the same University in 2017. Currently, he is a Third-year Ph.D. student at the Budapest University of Technology and Economics (BME) Budapest, Hungary, at the Department of Networked Systems and Services (HIT). He has worked as a researcher and teaching assistant at Budapest University of Technology and Economics for the last three years. His research focuses on Networking and Vehicular Communications (V2X).

David Khoury received the M.E. degree in telecommunications from ESIB, in 1983. He held different positions at Ericsson mainly in France and Sweden in Research and Development and Product and System management. He was involved in early studies of them GSM and the evolution toward an IP-based network and the early studies of 3G/WCDMA, HSPA, and LTE. In 2010, he has established his own start-up company (Secumobi) developing advanced military grade secure communications system and security solutions based on hardware encryption and trusted execution environments (TEE) in Stockholm. For the past 8 years, Full-time Faculty member and Research & Innovation fellow at AUST (American University of Science & Technology) in Beirut. From 2018 he is Strategy consultant for Wone, a startup located in Switzerland. He holds 5 US patents and has published many research papers in international and local conferences. His research interests include the IoT, information security, and blockchain technology.

László Bokor received the M.Sc. degree in computerengineering from the Department of Telecommunications, Budapest University of Technology and Economics (BME) in 2004, informatics from the Faculty of Economic Informatics, BME. He has researched in multiple EU-funded and national research and development projects for several years. He is currently with the Department of Networked Systems and Services (HIT) as an Associate Professor and leads the Commsignia–BME HIT Automotive Communications the M.Sc.+ degree in bank and Social Sciences, BME, and the Ph.D. degree from the Doctoral School of Research Group at BME and the Vehicle Communication Working Group of the Mobility Platform at KTI Institute for Transport Sciences. He is a member of the HTE (Scientific Association for Infocommunications Hungary), the Hungarian Standards Institution's Technical Committee for Intelligent Transport Systems (MSZT/MB 911), the TPE GoverC-ITS Task Force within the TPEG Application Working Group of TISA, the ITS Hungary Association (the Hungarian organization of ERTICO's Network of National ITS Associations), a nd the BME' the UNKP-16-4-I. Post-Doctoral Fellowship in 2016 from the New National Excellence Program of the Ministry of Human s Multimedia Networks and Services Laboratory, where he participates in different R&D projects. In recognition of his professional work and achievements in mobile telecommunications, he received the HTE Silver Medal (2013), the HTE Pollák-Virág Award (2015), and the HTE Gold Medal (2018). He was a recipient of Capacities of Hungary. In 2018 he was awarded the Dean's Honor (BME VIK) for education and research achievements in the field of communication of autonomous vehicles; in 2020, he received the BME HIT Excellence in Education Award.