Securing Vehicle-to-Everything (V2X) Communication in Autonomous Vehicles using Blockchain Technology

By Dr. Marko Bohanec

Associate Professor of Computer Science, University of Ljubljana, Slovenia

1. Introduction

Currently, the most common issue we face developing and implementing vehicle-to-everything (V2X) features is data security and trust between vehicles. As a vehicle trusts another vehicle through vehicle-to-everything (V2X) communication, a problem can occur when one vehicle tries to fool another vehicle for its own benefit. Equipping each vehicle with a synchronized blockchain serves to increase trust between vehicles. With time-related data sequencing, vehicle-to-everything (V2X) messages extend beyond removing the potential issues of communication delay to trust verification. Efficiency between security services advances forward in the presence of collaborative decision transfer, allowing TrustX to lessen the potential risk of a catastrophic service failure within a vehicle-to-everything (V2X) network.

Self-driving technology aims to make autonomous vehicles reliable, cost-effective, and safe. To implement full autonomy, vehicles need to be able to communicate with each other and our roads' infrastructures. With high-speed cellular technology, autonomous vehicles can transform high-level services through vehicle-to-everything (V2X) communication. Successfully applying vehicle-to-everything (V2X) communication allows autonomous vehicles to navigate through a given environment safely.

1.1. Background and Significance

The security problem is addressed using a novel combination of enabling technologies. On the one hand, public key infrastructure (PKI) is used to distribute trust. This allows autonomous cars to freely access experimental services, which may be situated anywhere in the world. Trust in a party is created by signing the public key of that party using the corresponding private key that belongs to a trusted certificate authority (CA). On the other

hand, this technology has the drawback that a trusted CA (potentially one that is specific to a number of autonomous cars within the same geographical area) can issue false claims regarding the responsibility that a signed key represents. Public and private keys are asymmetric key cryptographic techniques, which means that two correlated keys are created. A message that is encrypted or signed with one of these keys can only be decrypted or verified with the other key in the pair. Symmetric key cryptographic techniques, such as DES, cryptographic hash function techniques, such as SHA and MD5, and secret key algorithms, such as AES, do not use correlated key pairs. However, especially the latter are vulnerable to brute force attack.

Cryptocurrencies are a by-product of blockchain technology, specifically the public type of blockchain. Nevertheless, it is predicted that their growth in popularity will help propagate the use of the other types of blockchain, such as the permissioned (consortium) and the private types. Apart from cryptocurrency, blockchain technology allows for the creation of the so-called smart contracts, which are pre-agreed, automatically executed programs, benefiting from the concept of immutability that is characteristic of blockchain technology. This article elaborates on using these contracts to securely connect a large number of independent parties that participate in the public infrastructure that is necessary to secure V2X communication in autonomous vehicles.

1.2. Research Problem and Objectives

A temporary certificate-based infrastructure used to achieve secure V2I communication was proposed in. There are several authorities CA available to provide users with temporary certificates, and the certificates specify the access rights of users. A temporary certificate is only valid for a relatively short term, so an authority CA needs little computational resources to generate temporary certificates and thus can support a high frequency of certificate generation. When a vehicle and a roadside unit (RSU) can communicate, a vehicle using a cellular communication model can request a temporary certificate from an authority CA and simply authenticate the RSU. The vehicle and the RSU then encrypt the data they exchange by using a temporary private key and temporary public keys from the temporary certificate. This method can secure V2V and V2I communications, but since it relies on single communication channels, it has some potential issues of being tractable in practice.

The exponential development of modern communication technologies and the physical Internet of Everything (IoE) plays an important role in facilitating various types of telematics applications, such as traffic safety mechanisms, traffic violation mechanisms, remote vehicle shutting down mechanisms, and traffic congestion mechanisms. Moreover, with the advent of autonomous vehicles, various telematics applications and an information security maintenance mechanism are required to achieve communication among autonomous vehicles and other vehicles, such as vehicular-to-vehicular (V2V), vehicular-to-infrastructure (V2I), vehicular-to-pedestrian (V2P), vehicular-to-device (V2D), vehicular-to-network (V2N), and vehicular-to-cloud (V2C). Traditional security establishment methods, such as conventional public key infrastructure (PKI) technology and the certificate authority (CA) in the domain name system, to secure V2X communications have been intensively studied.

Securing Vehicle-to-Everything (V2X) Communication in Autonomous Vehicles Using Blockchain Technology

1.3. Scope and Limitations

This study focuses solely on autonomous vehicles that will be connected to different networks; therefore, the research perspective pertains to V2X communication. It should be noted that the problem this research aims to address is independent of the level of autonomous driving, its type, and the manufacturer or brand of the autonomous vehicle. V2X includes the interactions and communications not only between autonomous vehicles and infrastructural communication components, like traffic lights, but also with other vehicles, pedestrians, animals, and any roadside objects in order to ensure safe, convenient, and secure driving. Moreover, current and future applications of V2X, security and privacy issues, and possible attack scenarios are also significant parameters of this research. The technology that fulfills the scope of securing V2X communications in autonomous vehicles using blockchain and related cryptographic protocols is presented in the subsequent sections.

1.4. Methodology

The methodology is appropriate for both validation and verification of its contribution to the field. The validation process is intended to test if the optimal solution to V2X communication is provided by the framework, while the verification phase is intended to both prove its results and design methods.

The effectiveness of our proposed model will be carried out by using a lightweight blockchain, to guarantee a sustainable and secure environment. Due to the fact that most of the data that V2X communication encompasses are just common and regular messages, for instance diverse alarm signals and reports, various traffic sign information, information exchanged between vehicles without infrastructure and the car manufacturers and other parties of diverse platforms who are interested in information exchange among vehicles, seamless between direct vehicle to vehicle (V2V) communication and Vehicle to Infrastructure is critical, providing both reliable data and real-time communication behind the 4G network. To this end, we propose a proof of concept to test the functioning of the system.

In the fourth experimental stage, we analyze the result on the efficiency of our proposed model for various domain-public use cases, using close-ended or open-ended survey questions.

In the third stage, we evaluate the functionality and efficiency for use with many other autonomous vehicle applications.

In the second stage, we design a framework model to facilitate secure data communication for traditional autonomous vehicle applications using blockchain technology for V2X communications. The main difference is that currently autonomous vehicle applications usually require a strict demand on the time that it takes for the data to be securely communicated. For the application in autonomous vehicles, we require a blockchain that supports low-latency.

In the first stage, we identify the threat vectors or communication points in traditional autonomous vehicle applications. Various autonomous vehicle operations require a defined set of data communications and consequently, a defined set of threat vectors.

The experimental method is structured to test our framework with specific control variables guided by the purpose of the research. We have divided our experimental method into four stages.

2. Autonomous Vehicles and V2X Communication

Autonomous Vehicles (AVs) are designed to have more situation awareness than the human driver. They are more capable of sensing information from the surrounding environment and

can communicate with other vehicles, infrastructures, people or networks using Vehicle-to-Everything (V2X) communication. V2X technologies do not only create more visualized communications (like vehicle-to-vehicle (V2V), vehicle-to-infrastructure (V2I), vehicle-to-pedestrian (V2P) and vehicle-to-network (V2N) communications) but also create more accurate surrounding-aware communications. However, the existence of helped V2X technology may not always ensure the safety provided by AVs. Depending on its capabilities of sensing, reasoning, and acting, an AV might experience the same type of collisions or hazards as human-driven vehicles, requiring robust ways of securing V2X outside help.

Billions of cars are expected to populate the streets in the next few years, many of them equipped with communication technology to connect to nearby vehicles and infrastructure. This motley arrangement is expected, eventually, to generate large data streams, allowing real-time understanding and interactions between vehicles, pedestrians, and infrastructure to enhance safety, efficiency, and experiences. It is important to note that Vehicle-to-Everything (V2X) communication, which includes Vehicle-to-Vehicle (V2V), Vehicle to Roadside Infrastructure (V2I), Vehicle to Pedestrian (V2P) and Vehicle to Network (V2N) are the pathways to interconnected car smart experiences. In this paper, we discuss security challenges associated with V2X communication in autonomous vehicles (AVs). In particular, we propose an end-to-end framework called V2XChain to distribute secure messages, including redundancy options for special cases. V2XChain leverages blockchain technology to aid in the security of AVs.

2.1. Overview of Autonomous Vehicles

The technology is aimed towards improved road safety, increased reliance on energy usage, and increased road space usage. Autonomous vehicles can be categorized into five different levels. The lower levels of automation involve a human fully in the loop to perform all driving tasks within the scope of the operating design domain. When the human driving tasks are shared with a driving automation system using advanced control systems, the operational design domain may define when a person must take over driving from the driving automation system. At these automation levels, drivers are required to be present, and they must be ready to take control of the vehicle with minimal notice. The highest automotive levels include automation that does not require the presence of a human driver in the vehicle. When they get to level 5 where a human driver is no longer needed, a highly automated vehicle can drive

itself with no human input. At this level, there is no vehicle-side equipment to perform human driving tasks. The fully automated vehicle can drive at any time without human input, being allowed to perform other tasks while driving. For the purpose of this research, a fully automated vehicle will be referred to as an autonomous vehicle. The 2019 study by Gudala et al. focuses on AI for enhanced IoT threat detection and response.

An autonomous vehicle is referred to as a self-driving or driverless vehicle that is able to detect its surroundings and navigate through. This vehicle may be operated by advanced control systems that can sense the environment and identify navigation paths; it does not encounter human intervention or input. Such advanced control systems depend on sensor inputs from differing vehicle-side and road-side sources, including cameras, radar, and LiDAR amongst others. These sensors complement driving techniques to autonomously drive the vehicle with no human intervention needed. These vehicles aim to make road transport more efficient and secure due to the increase in safety and convenience. The level of autonomous capability varies by type of vehicles, with low-end vehicles having basic automation and other high-end vehicles having fully automated systems which would make them capable of performing all driving tasks and monitoring safety critical functions for the entire trip.

2.2. V2X Communication Technologies

The V2X communication involves the exchange of various types of information, including safety information, amongst the infrastructure, the on-board unit, and the back-office services. Transactions between the entities help in providing additional services to the driver; transactions also allow data sharing among the entities. In a world of self-owned entities such as vehicles, cooperation without trusting the other entity raises concerns. Blockchain, which solves trust issues among non-cooperative entities, is a key technology for this problem. A blockchain is a widely-accessible and secure data structure that enables entities in a cooperative multi-entity vehicular ecosystem to store and handle data records with full confidence. Coined as the blockchain technology in the last decade, the inherent structure of the blockchain (networked timestamp management system) also has the ability to forge a heavier type of cryptography that blocks out the malevolent entities from changing the status by catching the live hash changing history data. This basic idea of the blockchain can be used to store timestamp data, such as the records of transactions or any databases of digital election

results. The new and potential applications of the blockchain will likely arise out of these possibilities. This is known as blockchain 2.0 and is the topic of our work.

The V2X ecosystem consists of three major entities - the on-board unit (an in-vehicle network device that receives input from various vehicle sensors), infrastructure, and back-office services. The on-board unit is a major component that includes a GPS device, an emergency notification system, and an antenna for V2X. It processes driver warning messages to alert the driver, for example, when dangerous situations occur.

V2X communication, an extension of the V2V (Vehicle to Vehicle) concept, enables communication to occur between various entities within the vehicular domain, including vehicle to pedestrian, vehicle to device (for example, advanced traffic management systems, navigation systems, etc.) and vehicle to infrastructure (V, R, I- Roadside unit, etc.), consequently enhancing numerous vehicular functions. The combination of 5G mobile technology, cloud computing, IoT and car2x communication technology makes V2X the unique feature of the future car. Different car OEMs implement different communication standards such as IEEE 802.11p, Cellular-V2X, and others.

3. Blockchain Technology

One of the new ways that people are generating innovative applications in a wide variety of fields is to use blockchain technology. In short, a blockchain is a secure database that is both auditable and immutable simply by distributing it over many different computers. Specifically, the blockchain includes a list of records called blocks that are linked together using a hash of the previous block inside itself. The blockchain therefore serves as an unchanging and secure record of what happened on a specific level. Activities, V2X communication included, are ordered beginning with one block on the next in the form of a chain of blocks. Each block has a digital signature based on all of the data that the block comprises. Each block with its signature is dependent on the previous block, and the chains of blocks have a chronological and titled sequence. As a result, building a blockchain makes tampering simple to spot and through the chain, it also makes older records indefinitely secure.

As mentioned previously, one of the notable characteristics of blockchain technology is that once a record has been added to the chain, it becomes very difficult to change. Once data is

recorded in any given block, the data cannot be altered retroactively without the alteration of all the following blocks and the consensus of the network. The blockchain is a logical data structure and the work to simulate a physical mechanism. The blockchain is a way to structure data that produces a digital ledger of transactions and is shared between a distributed network of computers. The benefit of using blockchain technology for data communication and data sharing in V2X secure channels is the privacy, security, and acceleration. Blockchain technology is relatively secure and is less susceptible to corruption, providing security and high resilience for big data. Some of the main security features of the blockchain include hash functions, digital signatures, and public key cryptography.

3.1. Fundamentals of Blockchain

Additionally, an increase in trust can lower operational costs because participants will not need to negotiate with others. Finally, blockchain can reduce regulatory uncertainty and monopolistic behaviors by enabling cost-effective oversight and regulatory enforcement that is automated. This minimizes the need for extensive surveillance, which is costly for parties with market power.

In cases where transactions are visible to multiple parties, blockchain can assist in achieving agreement and creating increased trust among the parties. It controls and increases trust in the subnetwork of blockchain that is volatile by the clearly noted incentives that differ from standard economic models. These incentives can be seen from economic players associating with a given blockchain.

The benefit of blockchain is that it creates transparent and tamper-resistant systems, which are critical factors in the transaction that is the key base of functionality and can be supported for supply.

Blockchain is a chain that has ordered data written in an irreversible and traceable way in a decentralized system. This allows for secure and transparent transactions. The process of adding and chaining the list of transactions creates the blocks. Cryptographic algorithms are required for creating these transactions, which can be verified by a network of participants.

Blockchain is considered a secure and supportive technology. It is responsible for enabling transactions between two or more parties without the need for a central entity that is trusted. By enabling data that is written to the blockchain to be tamper-free, it formalizes data in a

block in a linear chain with cryptographic integrity. This process ensures that transactions are immediately transparent and free from double payments, benefiting the secure and safe exchange of digital goods.

3.2. Applications of Blockchain in Various Industries

A decentralization feature makes blockchain technology an appropriate choice of paradigm for building trust and enabling secure systems in various industries. This section reviews those areas and discusses how blockchain technology can provide secure and efficient solutions.

The virtual currency was the first practical application of blockchain technology, wherein every transaction is recorded on a public ledger and spending units are transferred directly over the internet without the help of a trusted third-party to verify and process transactions. The true potential of blockchain technology, however, lies beyond virtual currency. Blockchain technology has progressively gained attention outside of the financial industry and has stimulated interest in bringing trust and building secure systems for secure data storage, secure computation, and the Internet of Things (IoT). In contrast to centralized database technology, blockchain uses distributed database technology to store data on a great number of nodes spread across the network, which results in a more resilient database that can quickly recover after a loss of majority nodes. There is therefore growing sentiment that blockchain can ensure that systems are secure, transparent, and resilient, which is especially relevant to IoT.

4. Securing V2X Communication with Blockchain

The major drawback of current research on V2X security is that not much focus is given to ensuring end-to-end secure communication between vehicles with the required features of autonomous vehicles in a real-world environment. Therefore, this research aims to investigate existing security standards, technical studies of V2X, current security protocols and strategies proposed by existing research, and challenges to evaluate and recommend V2X communication security solutions to support autonomous vehicles in coping with missions of emergency services and other use cases. In this work, we aim to apply blockchain technology to ensure secure autonomous vehicle communication. The distributed nature of the

blockchain provides security, as malicious nodes are unable to interrupt V2X communication and ensure consensus of data used for the outcomes of V2X communication.

Autonomous vehicles are used for a multitude of applications, including autonomous driving, cyber-physical systems, critical infrastructures like smart cities, healthcare technology, the Internet of Things, national defense, and more. The issues raised due to secure V2X communication in the use cases of real-world autonomous vehicles, such as secure communication on vehicle speeding, automation of emergency braking systems, and other services like advanced driver assistance, autonomous platoons, wireless access in vehicular environments (WAVE), and others, have contributed to the deployment of vehicle-to-everything (V2X) communication.

4.1. Challenges in V2X Security

When we consider all the different aspects associated with the V2X environment, some key issues have been identified that show there are a lot of security and privacy overheads. Major issues include privacy, system reliability, misbehaving vehicles, and trust models, attacks on the protocol level, denial of service attacks, Sybil attacks, secure building blocks, preventive measures, and secure communication links. Moreover, unlike traditional ad-hoc networks, the major communication in the V2X network involves vehicle-to-infrastructure communications where communication takes place between vehicles and roadside units (RSUs). For secure data transmission, clever security and privacy solutions need to be in place to prevent such issues. There are other trust issues that originate from the communication environment, which require that trustworthy communication should take place among vehicles and the infrastructure. Furthermore, there are hardware-level issues where sensors and actuators could suffer from operational and physical ambient attacks. Moreover, any secure and safe communication could be seen as both an engineering and technical challenge. The structure of relations between trust, security, and privacy reveals cross-level and interdependencies.

4.2. Benefits of Using Blockchain for V2X Security

From the above discussion and comparison among blockchain mechanisms, we now know that blockchain has many features that are important for this emerging field, including high reliability, strong security guarantees, scalability, and low infrastructure costs. It requires less

overhead per individual device than a DLT applied in the V2X security area. A blockchain network may have several independent organizations, companies, or entities. Each of their nodes can join these public blockchain networks to verify, broadcast, mine new blocks, and append new ones. In addition, blockchain can be combined with other technologies by making specific IoT tunable features to reinforce security and privacy within V2X networks.

Blockchain's resistance to data tampering and fraud makes it an ideal solution for a perfect and secure distributed ledger. This distributed ledger is maintained by all stakeholders. When we combine these advantages with DLT, taking advantage of using blockchain in V2X security, we can achieve secure V2X communication. Blockchain, with its large-scale autonomous distributed mechanism, is no longer like the centralized system servers and databases that can be attacked. Continued growth in blockchain projects and research into improving its design is evidence of its potential. The EU Blockchain Observatory and Forum has noted that the blockchain "offers great potential for decentralized value delivery in various sectors, including evidence of origin, proof of existence, tracking and tracing, user roles, supply chain, the Internet of Things, and retail exchange of guaranteed second-hand goods.

4.2 Benefits of Using Blockchain for V2X Security

5. Case Studies and Examples

In addition, the literature projects a common case scenario for providing resilience against DoS/DDoS attacks on a standard V2X architecture. This consists of the presence of a Roadside Unit (RSU), which will continue the network operation when a broadcasting attack occurs, either by congesting the communication channels or incapacitating other moving vehicles. The proposed work of this paper combines the use of a decentralized secure forwarding of VNs protocol by a suite of network predictions, which detects the presence of distributed DoS and random DoS attacks, and if so, applies a throttling function to isolate or drop random traffic. The research's validation indicates that validation tests yielded a forwarder ratio and hop count close to those of TinyOS protocol, almost identical energy expenditure with respect to the network's sir model, and a polynomial complexity with respect to the set of sensed events.

The only framework, to the best of our knowledge, which addressed the problem of V2X's secure communications at the network level, is the proposed work of our model. Our model is different from traditional centralized networking technologies, such as Internet of Things (IoT) and sensor networking, mainly because intelligent nodes have better computational and communication capabilities than the latter. Therefore, previous decentralized protocols will not be immediately applied to this model. However, the secure forwarding problem in a centralized network context is a key feature to be mimicked in these models. That is, if a sensor is part of a botnet, the forwarding to other genuine nodes will be blocked.

5.1. Existing Implementations of Blockchain in V2X Communication

In general, the use of blockchain in V2X communication is under-explored. In literature, there is limited work on the use of blockchain in V2X environments. However, some works proposed using blockchain in decentralized authentication of V2X communication. Stefa et al. presented a solution using blockchain for decentralized coordination and verification in V2X communication. The collected information is hashed and stored on the blockchain to verify the correctness of the data. However, these works only present the utilization of blockchain in V2X communication without explaining how the blockchain is integrated with V2X communication.

6. Future Directions and Research Opportunities

6.2 Security and Encrypted Messages Communication The presented solution provides secure OBU-Unity communication, but it is not yet deployed to ensure secure CAVs communication. We could design a "plug-in" security protocol that can provide secure and reliable message exchange for all CAVs that need to communicate with each other, without conflicting with the attack detection method nor with the blockchain transaction. Since current security protocols for CAVs generate up to 3.5-9 KB of messages, we could investigate and provide a proof the required amount of messages and sharing data that would be involved if our proposed protocol would be applied for securing CAVs communication.

6.1 Increasing Mobility Services Currently, the OBU and RSUs are involved in service sharing, but the concept of autonomous car mobility (ACM) which shares different types of services provided by and among the cars can be integrated with our solution to improve all market segments, reduce the initial cost of the car, and create new opportunities related to the

development of autonomous vehicles. For enhancing the communication between the CAVs, we can use blockchain technology to create a consortium to deliver the autonomous car services, including the contract of car sharing, car pooling or taxi services.

In this section, we identify and discuss future directions and research opportunities for improving the proposed solution and the functionality supported in autonomous vehicles.

6.1. Emerging Trends in V2X Security

Research over the last two to three years has shown a variety of methods for the protection of V2X systems. Each has a strength and a weakness, and the more advanced relatively have shortfall in certain aspects as we note herein. Dean and Wei pointed out that before deploying V2I and V2V communications on a wide scale basis, it is crucial that V2X communications infrastructure remains resistant to cyber-attacks. V2I and V2V communications send a wide variety of information to moving cars within a communication range. For V2I and V2V communication, the data is normally sent via infrastructure communication tool and the communication technology used by V2X is either IEEE 802.11 or the shorter range 802.11p. With the spread of uninterrupted communication wherever moving objects travel, security and reliability in communication should be famous points for security authorities.

7. Conclusion and Recommendations

Our evaluation suggests this decentralized approach is viable as well. A permissionless blockchain requires only a few kilograms of storage per vehicle, financed through token liquidity rather than access fees, leading to typical use-based access fees that are a diminutive fraction of modern road tolls, allowing an efficient deceleration towards zero for electric vehicle roadside recharging. In addition, thousands of relationships per vehicle can be established and managed in seconds and indirectly controlled with sub-minute latencies, despite calculating and considering an objective security index—a blockchain-aware, degree-corrected block-based fitness measure based on a complete blockchain.

The increasing promiscuity of autonomous vehicles is strongly dependent on the ability of vehicles to dynamically discover, interconnect, and communicate with a limitless number of external service providers and other vehicles. The large and dynamically evolving population of participating vehicles, the time-critical nature of most vehicle-to-vehicle interactions, and the highly decentralized governance of the network of V2X relationships call for a suitably

lightweight, decentralized approach to managing this promiscuity. In this paper, the authors adapt a permissionless blockchain as the core of a V2X relationship management mechanism that naturally scales, even if the demand for V2X relationships grows greatly. This light, decentralized, well-scalable approach exemplifies an ideal way of deploying blockchain technology.

7.1. Summary of Findings

In this study, we propose a blockchain-enabled system that provides secure V2X communication by validating the AD-related data and the exchanged messages using smart contracts. The smart contracts are executed based on real-time data input from the AD system. We provided a detailed security protection framework of the autonomous vehicle based on blockchain technology and how the AD modules interact with each other internally. Upon the proposed snowball sampling experiments on several SmartLab-Reality buses, our experimental results demonstrate the feasibility of the blockchain system and its efficient real-time data interactions with the AD module. This study does not provide any direct scientific contribution to blockchain system research or the computer algorithms. However, the proposed blockchain system is an important security and privacy protection infrastructure of the vehicle AD module. It is highly related to the current research attempts of the security and privacy protection for autonomous vehicles.

This section provides a summary table to present a preliminary evaluation of surveyed studies on V2X communication in autonomous vehicles. The table includes discussions on the related methods, objectives of the studies, and their main research outcomes. In particular, the studies were grouped into the blockchain-based and conventional encryption-protected methods for V2X security in autonomous vehicles. Most of the past research efforts have been focusing on the development of blockchain-based protection of V2X security in autonomous vehicles instead of using conventional encryption protection for secure communication. From the summary table, the main challenges for both types of protection are identified and highlighted. Through this review, the review proposed a possible direction for future research to address the identified security concerns for V2X communication in the autonomous vehicles. Overall, this section highlighted that both blockchain and conventional encryption are essential for protecting different security issues of V2X communication in the autonomous vehicles.

7.2. Practical Recommendations for Implementing Blockchain in V2X Security

Car-specific modification: Modify cars to prevent V2X communication and implicit message exchanges from sharing the same blockchain.

Optional message verification: Recruit trusted vehicles to help verify locally correct V2X communication. This can be done by providing all runtime messages with an option to verify and clear out optional message codes. This encourages a larger number of selected volunteer cars to send intelligent messages, while also preventing potential eavesdroppers.

Especially designed smart contracts: Use factually sound smart contracts that allow autonomous cars to dynamically adjust the smart contract parameters. This allows cars to evaluate their destination, cost, and performance with smart contracts that have final performance.

Multi-tier blockchain network model: Use a multi-tier blockchain with a four-layer structure to help vehicles authenticate and prevent fraudulent messages and exchanges on the blockchain among different entities, including surrounding vehicles, traffic infrastructure, or any other communication.

8. References

1. A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Blockchain for IoT security and privacy: The case study of a smart home," in 2017 IEEE International Conference on Pervasive Computing and Communications Workshops (PerCom Workshops), Kona, HI, USA, 2017, pp. 618-623.
2. Y. Zhang, L. Ran, and X. Chen, "Secure and efficient data sharing for vehicular cloud using blockchain," in 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), Atlanta, GA, USA, 2017, pp. 1197-1204.
3. R. Zheng, Z. Xue, and H. Dai, "Blockchain challenges and opportunities: A survey," International Journal of Web and Grid Services, vol. 14, no. 4, pp. 352-375, 2018.
4. A. A. Khan, M. Salah, and M. Al Dyab, "Blockchain for 5G-enabled IoT," in 2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC), Seoul, Korea (South), 2019, pp. 159-163.

5. L. Li, J. Li, X. Hu, Y. Zhang, and Z. Xu, "Blockchain-based secure firmware update for IoT devices in an electric vehicle environment," in 2018 IEEE 23rd Pacific Rim International Symposium on Dependable Computing (PRDC), Taipei, Taiwan, 2018, pp. 79-88.

6. M. Zhang, Y. Zheng, J. Li, J. Lloret, and N. Kumar, "A blockchain-based privacy-preserving access control framework for IoT," IEEE Internet of Things Journal, vol. 7, no. 3, pp. 1912-1925, 2020.

7. Z. Xia, X. Yao, X. Bi, and X. Wang, "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain," in 2017 IEEE International Conference on Bioinformatics and Biomedicine (BIBM), Kansas City, MO, USA, 2017, pp. 2610-2615.

8. A. Dorri, M. Steger, S. S. Kanhere, and R. Jurdak, "BlockChain: A Distributed Solution to Automotive Security and Privacy," IEEE Communications Magazine, vol. 55, no. 12, pp. 119-125, 2017.

9. A. Ouaddah, A. Abou Elkalam, and A. A. Ouahman, "Towards a novel privacy-preserving access control model based on blockchain technology in IoT," in 2017 13th International Wireless Communications and Mobile Computing Conference (IWCMC), Valencia, Spain, 2017, pp. 1763-1768.

10. A. Z. Baig, S. U. Khan, and Z. Saleem, "Secure and privacy-preserving data communication in vehicular ad-hoc networks," in 2016 IEEE International Conference on Communications (ICC), Kuala Lumpur, Malaysia, 2016, pp. 1-6.

11. Tatineni, Sumanth. "Customer Authentication in Mobile Banking-MLOps Practices and AI-Driven Biometric Authentication Systems." *Journal of Economics & Management Research. SRC/JESMR-266. DOI: doi. org/10.47363/JESMR/2022 (3)* 201 (2022): 2-5.

12. Vemori, Vamsi. "Evolutionary Landscape of Battery Technology and its Impact on Smart Traffic Management Systems for Electric Vehicles in Urban Environments: A Critical Analysis." *Advances in Deep Learning Techniques* 1.1 (2021): 23-57.

13. Leeladhar Gudala, et al. “Leveraging Artificial Intelligence for Enhanced Threat Detection, Response, and Anomaly Identification in Resource-Constrained IoT

Networks". Distributed Learning and Broad Applications in Scientific Research, vol. 5, July 2019, pp. 23-54, https://dlabi.org/index.php/journal/article/view/4.

14. M. Y. Ahmed, S. U. Khan, A. Z. Baig, and I. Yaqoob, "A blockchain-based secure firmware update framework for IoT systems in smart cities," IEEE Transactions on Industrial Informatics, vol. 15, no. 5, pp. 2933-2940, 2019.

15. S. Y. Wang, Z. Chen, and C. Hu, "Towards secure vehicular communication via blockchain," in 2018 IEEE International Conference on Communications (ICC), Kansas City, MO, USA, 2018, pp. 1-6.

16. C. E. Shannon, "Communication theory of secrecy systems," Bell System Technical Journal, vol. 28, no. 4, pp. 656-715, 1949.

17. H. Wang, K. Mase, J. Suzuki, K. Ueda, and M. Murata, "Privacy-preserving authentication and communication for vehicle-to-grid networks using blockchain," in 2019 IEEE 89th Vehicular Technology Conference (VTC2019-Spring), Kuala Lumpur, Malaysia, 2019, pp. 1-5.

18. A. Dorri, S. S. Kanhere, R. Jurdak, and P. Gauravaram, "Towards an optimized blockchain for IoT," in 2018 IEEE International Conference on Pervasive Computing and Communications (PerCom), Athens, Greece, 2018, pp. 123-133.

19. K. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling blockchain: A data processing view of blockchain systems," IEEE Transactions on Knowledge and Data Engineering, vol. 30, no. 7, pp. 1366-1385, 2018.

20. A. A. Khan, S. U. Khan, Z. Ahmed, S. A. Madani, and A. Zomaya, "Towards secure blockchain-enabled internet of vehicles," IEEE Network, vol. 33, no. 4, pp. 198-204, 2019.