A blockchain-based V2X communication system

Hassan Farran*, David Khoury†, Elie Kfoury‡, and László Bokor*
*Department of Networked Systems and Services, Faculty of Electric Engineering and Informatics, Budapest University of Technology and Economics, Budapest, Hungary
†Department of Computer Science and information and communication technology
American University of Science and Technology, Beirut, Lebanon
‡Integrated Information Technology Department, University of South Carolina, Columbia, SC, 29201 USA
hfarran@hit.bme.hu, dkhoury@aust.edu.lb, ekfoury@email.sc.edu, bokorl@hit.bme.hu

***Abstract*—The security proposed for Vehicle-to-Everything (V2X) systems in the European Union is specified in the ETSI Cooperative Intelligent Transport System (C-ITS) standards, and related documents are based on the trusted PKI/CAs. The C-ITS trust model platform comprises an EU Root CA and additional Root CAs run in Europe by member state authorities or private organizations offering certificates to individual users. A new method is described in this paper where the security in V2X is based on the Distributed Public Keystore (DPK) platform developed for Ethereum blockchain. The V2X security is considered as one application of the DPK platform. The DPK stores and distributes the vehicles, RSUs, or other C-ITS role-players' public keys. It establishes a generic key exchange/ agreement scheme that provides mutual key, entity authentication, and distributing a session key between two peers. V2X communication based on this scheme can establish an end-to-end (e2e) secure session and enables vehicle authentication without the need for a vehicle certificate signed by a trusted Certificate Authority.**

***Index Terms*—Vehicle-to-Everything (V2X); Blockchain; Cooperative Intelligent Transport System (C-ITS); Distributed Public Keystore (DPK); Ethereum, Public key, PKI/CA, RSU;**

I. Introduction

The Vehicle-to-Everything (V2X) technology enables vehicles to communicate and interwork built on a C-ITS (Cooperative Intelligent Transport System) ecosystem. V2X consists of Vehicle-to-Vehicle (V2V), and Vehicle-to-Infrastructure (V2I), Vehicle-to-Pedestrian (V2P), Vehicle-to-Network (V2N), Vehicle-to-Grid (V2G), contexts, amongst others and creates the base for advanced autonomous applications. The C-ITS introduced an architecture of interconnected vehicles, road-side networks, and mobile transportation services, which reduces traffic loads and environmental pollution while improving road safety and transport efficiency [1]. The C-ITS's success depends on V2X communications since it oversees data exchange between the underlying communication technologies. This provides onboard sensor feedback and warning, such as the vehicle's current position and speed. V2X comprises several protocols for exchanging messages containing data and vehicle information, sensors information, etc. In V2X environments, the applications have varying requirements for latency, durability, throughput, user density, and security. Safety features and autonomous driving systems need exceptionally low latency, but security and trust are the highest priority for V2X. It is crucial to validate the reliability and credibility of the communication messages that contain location, velocity, and heading. Around the same time, privacy should be kept to a minimum. To achieve these primary goals, a security model based on a Public Key Infrastructure (PKI) and frequently changing pseudonym certificates has been built for V2X. V2X messages exchanged should fulfill authenticity, confidentiality, and integrity. V2X systems use the trusted PKI concept. In the US, the trustworthy third-party Certificate Authority (CA) and in Europe, the Certificate policy authority (CPA) are considered. However, CA and CPA have the highest management authority for issuing vehicle registration information, associated certificates, identity checking, and vehicle pseudonym management. Digital signatures ensure the reliability of the message sent by a vehicle. Security Credentials Management System (SCMS) is the standard for authentication and validating V2X messages in the US [2], and C-ITS Credential System (CCMS) in Europe [3].

C-ITS can provide a wide variety of services. Depending on the framework (e.g., information supply, awareness, assistance, warning to avoid an accident, traffic management), C-ITS will improve for example road safety by preventing and minimizing the severity of collisions, decreasing congestion, by optimizing performance and available capacity of current road transport network, to strengthening vehicle fleet management, by rising travel time reliability and lowering energy consumption and negative environmental effect. Furthermore, C-ITS is regarded as the first step towards higher stages of automation in road transportation [4]. This paper proposes a new method of implementing trust in C-ITS networks without using the PKI infrastructure concept. The solution described below uses the blockchain concept to store and distribute public keys of vehicles, road-side units, and other C-ITS role-players. This mechanism enables vehicle authentication without the need for a vehicle certificate signed by a trusted Certificate Authority.

The method is built on the generic DPK platform based on Ethereum blockchain, developed in previous work and referenced in the paper ”Distributed Public Key Infrastructure and PSK Exchange Based on Blockchain Technology” [5]. The DPK platform provides a service to store and distribute any device's public keys and could be adapted and applied to the V2X domain. It establishes a generic key exchange/ agreement scheme that provides mutual key, entity authentication, and distributing a session key between two peers. V2X communication can establish an end-to-end (e2e) secure session and enable client authentication without the need for a client certificate signed by a CA. Another advantage of the proposed solution that it solves the issue of a device or a vehicle behind a NAT (Network Address Translation). The IoT devices, vehicles and other ITS (Intelligent Transport System) stations are considered no addressable identities behind a NAT where they contain a client to access the Blockchain. This problem was solved in by the Ethereum access client and the RLPx protocol in the Ethereum blockchain. The RLPx framework is responsible for the plumbing of communications in Ethereum. It is split into two protocols: discovery and wire protocol. The protocol allows Ethereum nodes to discover nodes and connect to them efficiently to maintain the network's decentralized factor. RLPx's node discovery protocol is a Kademlia-like protocol [6].

A unique identity is provided for any client behind a NAT device, facilitating the addressing challenge and management of devices. This is considered one of the main advantages of the proposal as nowadays ITS-G5 PKI certificates are disseminated over 4G LTE (IPv4) and the IPv6 could not be needed if this method is implemented.

The platform's primary contributions consist of (1) authenticating vehicle clients without the use of a PKI/CA, (2) ensuring that session keys are distributed among communication parties, (3) providing protection against public key modification due to Blockchain's immutability, (4) enabling protection between vehicles from various organizations, (5) providing a specific identity for each system to enable addressing and management, and (6) resolving the problem of the vehicles behind the NAT without the need to enforce the IPv6.

The remainder of this article is structured as follows. Section II describe the background of C-ITS and related work of Blockchain. Section III describes the proposed approach based on the blockchain paradigm and its high-level benefits over the current V2X security architecture. Section IV summarizes our initial measurement results from the first vision of the implementation. Finally, Section V contains our closing remarks and the planned future work.

II. Background and Related Work

The C-ITS infrastructure sketched in figure 1 comprises the Trust List Manager (TLM) appointed by the CPA. The TLM generates the European Certificate Trust List (ECTL), giving all PKI participants confidence in the accepted root CA's [3]. The CPA grants permission for the root CA activity.

There will be many PKI participants in C-ITS ecosystem. PKI roles are classified into two types, 1) authoritative functions, i.e., in which each function is individually instantiated; 2) organizational functions, in which roles may be executed in one or more organizations. For example, a private organization, a mutual interest community, a national association, or a European organization may be adopting a root CA.

The C-ITS trust model platform comprises an EU Root CA and additional Root CAs managed in Europe by member state authorities or private organizations offering certificates to individual users.

The CCMS uses public keys, generates vehicle-specific certificates, and signs them with the root CPA. The root CPA serves as the foundation for all certificates. The vehicle certificates, as well as the root CPA, are then returned to the vehicle. For auditing purposes, information must be provided to an approved PKI auditor. After being audited, the root CPA application form should be signed with its authorized representative.

This certificate policy establishes the European C-ITS Trust model, which is built on PKI. The EU C-ITS Credential Management System specifies the legal and technological specifications for issuing institutions to manage public-key credentials for C-ITS applications and their use by European end-entities. The PKI is composed at its highest level of a series of root CAs "enabled" by the TLM, i.e., whose certificates are placed in ECTL, which is distributed and released by central body TLM.

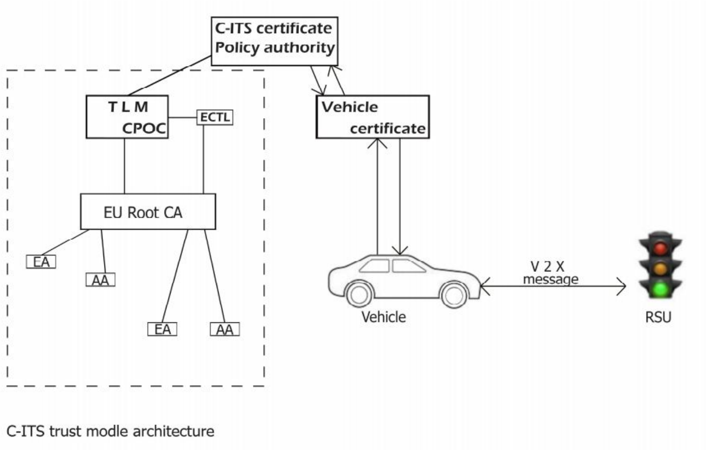

Fig. 1. V2X communication system architecture.

The C-ITS proposed and being implemented in the European Union is based on the V2X PKI designed to secure the message exchange in V2X communications. The V2X is based on trusted identities and digital signatures: each message's integrity and its sender's authorization can be guaranteed while preserving privacy.

The V2X attempts to make the transportation infrastructure smarter by linking everything with moving vehicles. PKI-based schemes offer essential security services for vehicle ad hoc networks. Furthermore, owing to the peculiar features of networks, confidence and privacy remain unanswered questions. Blockchain, as a promising technology, will provide shared protection against unauthorized entry. This idea was already introduced in the literature, used by many papers that summarize the promise of Blockchain in the V2X domain.

In paper [7], the author offers an analysis of ITS focused on telecommunications, highlighting the system security and durability, and describes the technical implications of deploying blockchain technologies in V2N applications. Additionally, an experiment was conducted to demonstrate the numerical features of resource distribution on devices used in arranging V2N correspondence. In paper [8], the author analyzed and discussed in depth the integration of Blockchain in V2X communications, which opens up new ways to enable advanced V2X networks, capabilities, and services. Moreover, the incorporation of blockchain technologies in 5G-based Multi-access Edge Computing (MEC) vehicular networks for authentication, privacy safety, and content caching was then investigated in both papers [7] and [8], there was no indication of any proposed solution.

In paper [9], the authors suggest a privacy security scheme for the Internet of Vehicles (IoV) based on blockchain technology. The method integrates the Blockchain with the IoV system to create a secure and robust two-way authentication and key agreement algorithm via encryption and signature algorithm, thus resolving the conventional IoV system's central dependence issue. It proposes a solution to distribute generated public keys to the vehicles after the Trusted Authority (TA) has generated and stored this information and others on Blockchain networks where the RSUs play the role of Blockchain nodes. Our solution follows a different approach where the Public Keys are generated by vehicles and RSUs, not by the TAs. The advantage of our scheme that vehicle's clients are authenticated without the need of a third party and therefore protecting against public key alteration and finally enabling security between devices from different organizations.
In paper [10], the authors introduce a stable protocol for sharing inter-vehicular messages based on consensus power. It provides a first approach to the requirements, Blockchain architecture, business processes, and reference architecture of a Blockchain-based Mobility-as-a-Service concept design operated by autonomous vehicles.

In paper [11], the critical novelty is creating a Blockchain-based IoT framework for encrypted communication and providing an entirely open cloud computing network. The authors modify Blockchain technologies for real-time application (RTA) to address V2X connectivity issues. The paper provides a high-level approach to develop a Blockchain-based IoT system to establish secure communication and create an entirely decentralized cloud computer. But the paper is missing a detailed security implementation solution. In both articles, the writers emphasize the importance of securing the message without relying on Public Key Infrastructure-based authentication. Our work is not focused on tailor-made security for V2X, instead our solution is generic and consistent, and it can be applied by replacing the PKI with Blockchain.

III. THE PROPOSED SOLUTION: A BLOCKCHAIN-BASED V2X SECURITY SCHEME

This section introduces the proposed structure, its design, and illustrates the various components and interactions. The proposed solution for V2X security is based on the DPK (Distributed Public Key-store) platform described in the papers [5] and [12] figure 3 high-level V2X system architecture based on Blockchain.

A. Background on Blockchain

Satoshi Nakamoto introduced the Blockchain technology as a peer-to-peer electronic cash system in 2008 [13]. When a paper titled "Bitcoin": A peer-to-peer electronic cash system," was released. He proposed an inventive and novel way to transmit (send and receive) digital money (called crypto-currency) without the need for a trustworthy third party, Blockchain can be described as a collection of records connected together that are highly resistant to alteration and protected through cryptography. Blockchain is considered a transparent, distributed, and public ledger framework. Each block includes a timestamp for transactions or records pertaining to programs and data. Additionally, this scheme provides advantages such as security, honesty, and privacy.

The Blockchain is based on an immutable digital ledger that tracks all transactions in a transparent and consistent. Since the ledger is mirrored across several nodes, no central authority manages or maintains it. The validation of the transactions uses the Proof of Work (PoW) algorithm, which is a decentralized consensus mechanism that requires the nodes of a network (called miners) to expend effort solving an arbitrary mathematical puzzle to prevent anybody from disturbing the system. Proof of work is used widely in cryptocurrency mining.
The transactions are stored in blocks interconnected using cryptography (hence the term blockchain), explicitly using hash functions: each block stores the hash of the previous block, timestamp, and transaction details. Therefore, data on a single block cannot be changed without affecting corresponding blocks, which requires the network's consensus. Each block contains a sequence of transactions and the previous block's hash, as seen in figure 2 [14] below.

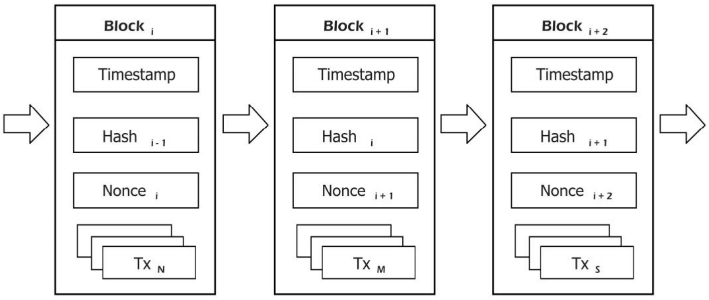

Fig. 2. The general Blockchain blocks series.

Blockchain 2.0, which was released in 2014, was another step ahead in its development. The word blockchain 2.0

distinguishes between Bitcoin as an asset and ”blockchain as a programmable distributed trust infrastructure” more broadly, including modern modular capabilities of on-chain functionality and extensibility [15]. Instead of seeing the Blockchain as a component of the decentralization of money and transfers, Blockchain 2.0 rather broadens the application possibilities of the platform. It allows the decentralization of economies more broadly, and transactions will include other categories of properties by offering repositories for certificates and rights and responsibilities of real estate, intellectual property, vehicles, etc.

B. Ethereum Blockchain

Ethereum is an open-source, transparent Blockchain-based computing network that allows smart contracts to be executed [16] [17]. The Ethereum Virtual Machine (EVM) serves as the runtime environment. Its smart contracts are written in high-level programming languages such as Solidity, Serpent, Mutan, and are compiled to EVM bytecode for execution. In Ethereum Smart contracts are considered as treated as accounts and are managed by their code. Once deployed, the contract is marked with an address, and the data associated with it is made public. The Externally Owned Account (EOA) is another account type. It is a user account that is linked to a keypair generated when the account is created. The holder of a wallet’s private key manages it, and signatures transactions initiated from the wallet address. The EOA address is used to refer to the account, while the private key is used for transactions signing. In Ethereum, performing smart contract functions is regarded a transaction. Ether is the crypto-fuel or cryptocurrency name at Ethereum. It is transferred between the users, but it is often used to rewards miners who operate the Blockchain network.

- **Light Client (LES):** A light client is created to enable restricted devices (mobile, IoT, etc.) to communicate with the Blockchain securely. The devices only download the block headers and retrieve data from the Blockchain as needed. The Light Ethereum Protocol (LES)is used in Ethereum, and its protection is built on Merkle proofs.
- **Public and private Blockchain:** A Blockchain can exist in two modes: public and permissioned. In the public Blockchain, anyone can participate in the network (mining node or user) as it is entirely open, and no trust is needed between members. The permissioned (also referred to as private) third party maintains its ledger.
- **Ethereum 2.0:** is an update to the Ethereum Network that increases the network’s speed, reliability, and scalability. It will be able to execute more transactions and reduce the high gas costs drastically. The main features improvements are staking: Proof of Stake (PoS) instead of proof of work (PoW) a much more energy-efficient method of maintaining the network. Shared chains – Ethereum will be broken into 18 Shards that operate at the same time. This will drastically improve efficiency.

C. Overview of the DPK platform

The DPK platform is built on the Ethereum Blockchain and consists of a public key store for configuring the device’s public keys. The DPK includes a client-side consisting of an Ethereum wallet, a management module on the server-side used for the configuration of the devices and transfer of Ether to their wallets, and some transfer of Ether to their wallets. This intelligent contract functionality has been deployed on the Ethereum Blockchain network. Many applications may use this generic platform for client and server authentication, secure peer-to-peer communications, and data integrity. Furthermore, this promising framework can remove the confidence obligation placed on clients by the current PKI/CAs infrastructure.

D. The proposed V2X security system architecture

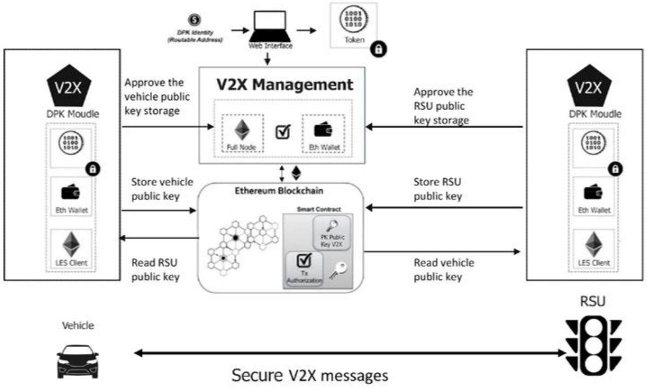

Fig. 3. V2X communication system based on DPK.

The V2X security system is depicted in figure 3. It is considered one of the applications of the DPK platform. The system’s functionality includes the following parts of the below subsections.

1) V2X management platform *:* The V2X management platform is a Network function within the DPK platform that is hosted on shared servers operated by an organization belonging to, e.g., a government. It specifies the legal and technological specifications for managing public keys in C-ITS applications. It authenticates the ITS stations and approves the Blockchain public keys storage requests. It is a vehicle and authentication platform. The DPK client module download, or installation produces the public/ private keys and provides an empty Ethereum wallet. The primary role of V2X management is to authenticate the DPK client module in the vehicle. The primary functions of the V2X platform are described in the following sub-sections:

a) Transferring Ether to the V2X client-Wallet management: An empty Ethereum wallet is generated when the DPK client is installed. The Ethereum wallet is filled with the needed Ether from the V2X managment during the vehicle device configuration. The Ether in the client’s wallet is required to execute the transactions in the smart contract. Storing data or changing a contract's state in the Blockchain requires processing power translated into transaction fees priced in Ether. Therefore, the vehicle client wallet is filled with Ether from the V2X management during the vehicle device configuration. During the configuration, the most critical parameters are the provided wallet address, Mobile Station International Subscriber (if the 3GPP mobile cellular networks are used), and the signed token as an encrypted payload.

b) Configuration: Vehicles accessing the DPK platform should be registered and installed in the V2X management platform through a web interface (or other means). This platform could be part of the C-ITS or an evolution of the exiting C-ITS. The setup entails assigning a one-of-a-kind Token to the DPK client module. This token is crucial to identifying and authenticating the DPK client module installed on the Vehicle device and ensuring that the device's wallet is filled with needed Ether.

The vehicle part of the V2X network should request a DPK module to be installed in the vehicle.

The DPK identity will be Non-Addressable. A non-addressable identity, known as a Universally Unique Identifier (UUID) is established. This form of identification is typically used on devices that don't have a reachable address (behind NATs), such as browsers, IoT devices, and mobile devices. Additional authentication of the client devices could be considered (based on SIM or E-SIM).

The setup entails assigning a special Token to each DPK client module. This token is critical for defining and authenticating the DPK client module mounted on the ITS station device and ensuring that the device's wallet is filled with needed Ether.

2) Client module for V2X DPK:*:* Software installed on the ITS station device transparently creates an Ethereum address, securely stores the created public keys in the Blockchain, and distributes session keys to communicating parties. It includes a light Ethereum client that connects to the Blockchain through LES (Light Ethereum Subprotocol) and a dedicated module (Eth Wallet) to interwork with the V2X manager. This module may be downloaded or included in the firmware of a light device with LES, referred to as a light Ethereum Node.

3) Smart contracts in the Ethereum Blockchain network:*:* This part of the DPK platform contains the significant functions needed to store and retrieve the keys. The smart contract holds the public keys of the vehicle's clients by using a mapping data structure indexed by the vehicle identity. The smart contract's main functionalities: store and read the vehicle or and RSU's public keys. Any user can call the function addClient and insert a new record containing its public keys in the Blockchain and getClient to get the public keys of the requested client. The V2X management approves the storage of the public keys through the smart contract function approveClient. The contract code is written in Solidity, a high-level language with a syntax like JavaScript designed to be used with the Ethereum Virtual Machine (EVM).

IV. IMPLEMENTATION AND RESULTS

In this section, we provide the Proof Of Concept implementation of the system. It should be mentioned that we have focused and the feasibility of use the DPK platform for client vehicles. The client at the vehicle side is considered as one application of the DPK platform. We have implemented the same interface like the ones specified in the DPK platform. The technologies used in the development process are: 1) Ropsten Testnet: A public network that simulates Ethereum and 2) the DPK smart contract running on EVM 3) Web3j: Lightweight Java application for interfacing the Ethereum Blockchain including the LES: Light client running on the vehicle device. The results showed the feasibility of implementing the proposed solution on the DPK platform. We have focused on the following:

- Measure the time needed to establish secure sessions between two V2X clients, and the results showed a similar result to the one described in the paper [18]. The secure session setup time took around 1s.
- The time used for registering devices public keys in the Ethereum is related to the block mining time, therefore we do not evaluate the required storage time.
- The storage cost: we have analyzed the costs required to store a transaction in Ethereum, by estimating the GAS required for executing the transaction. Creating a record (public keys) in the DPK platform costs 0.00548 ETH. Retrieving the public key of a device from the smart contract is free since the function is not modifying or storing data in the Blockchain.

In the next phase, we intend to implement the complete solution as described in the paper but implemented on Ethereum 2.0 where the PoS (Proof of Stake) is applied. The main advantage of Eth2.0 is the increased number of transactions per second and cheaper storage transactions cost. The exiting figures measured today will be modified substantially.

V. CONCLUSION AND FUTURE WORK

In this paper, we have proposed a Blockchain-based V2X secure communication platform that combines elements of the PKI/CA model with Blockchain technology. It describes an alternative solution to the European standard C-ITS'authentication, integrity, and confidentiality based on the traditional PKI/CA. The method aims to resolve the existing PKI/CA infrastructure's trust concerns and facilitate the authentication and security of the vehicles in the V2X network. The scheme is considered one of the possible applications of the DPK platform. The next step of the work will be implementing and testing the proposed system on Ethereum 2.0 blockchain, which requires the DPK platform to be upgraded to Eth 2.0. We aim to present this solution as a potential alternative to the existing techniques and provide an in-depth analysis of the proposed architecture's pros and cons compared to the current standards. This method requires simple infrastructure and management components compared to the C-ITS. Were it needs of TLM management and the presence of different trusted root CAs.

References

[1] 5GAA, “White Paper on ITS spectrum utilization in the Asia Pacific Region White paper on ITS spectrum utilization in the Asia Pacific Region,” p. 20, 2018.

[2] B. Brecht et al., “A security credential management system for V2X communications,” IEEE Trans. Intell. Transp. Syst., vol. 19, no. 12, pp. 3850–3871, 2018, doi: 10.1109/TITS.2018.2797529.

[3] [1] C-ITS Platform, “Certificate Policy for Deployment and Operation of European Cooperative Intelligent Transport Systems (C-ITS),” no. June, pp. 1–79, 2018.

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

[5] E. Kfoury and D. Khoury, “Distributed Public Key Infrastructure and PSK Exchange Based on Blockchain Technology,” Proc. - IEEE 2018 Int. Congr. Cybermatics 2018 IEEE Conf. Internet Things, Green Comput. Commun. Cyber, Phys. Soc. Comput. Smart Data, Blockchain, Comput. Inf. Technol. iThings/Gree, pp. 1116–1120, 2018, doi

[6] P. Maymounkov and D. Mazières, “Kademlia: A peer-to-peer information system based on the XOR metric,” Lect. Notes Comput. Sci. (including Subser. Lect. Notes Artif. Intell. Lect. Notes Bioinformatics), vol. 2429, no. April 2002, pp. 53–65, 2002, doi: 10.1007/3-540-45748-

[7] 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.

[8] 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.

[9] T. Su, S. Shao, S. Guo, and M. Lei, “Blockchain-Based Internet of Vehicles Privacy Protection System,” Wirel. Commun. Mob. Comput., vol. 2020, 2020, doi: 10.1155/2020/8870438.

[10] J. A. L. Calvo and R. Mathar, “Secure Blockchain-Based Communication Scheme for Connected Vehicles,” 2018 Eur. Conf. Networks Commun. EuCNC 2018, pp. 347–351, 2018, doi: 10.1109/EuCNC.2018.8442848.

[11] R. Jabbar, M. Kharbeche, K. Al-Khalifa, M. Krichen, and A. K. Barkaoui, “Blockchain for the internet of vehicles: A decentralized IoT solution for vehicles communication using ethereum,” Sensors (Switzerland), vol. 20, no. 14, pp. 1–27, 2020, doi: 10.3390/s20143928.

[12] E. F. Kfoury and D. J. Khoury, “Secure end-to-end VoIP system based on ethereum blockchain,” J. Commun., vol. 13, no. 8, pp. 450–455, 2018, doi: 10.12720/jcm.13.8.450-455.

[13] C. S. Wright, “Bitcoin: A Peer-to-Peer Electronic Cash System,” SSRN Electron. J., 2019, doi: 10.2139/ssrn.3440802.

[14] 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.

[15] Blockchain: I Chapter, Blockchain technology and its applications - Diritto.net.” [Online]. Available: https://www.diritto.net/blockchain-chapter-blockchain-technology-and-its-applications/. [Accessed: 19-Apr-2021].

[16] G. Wood, “Ethereum: a secure decentralised generalised transaction ledger,” Ethereum Proj. Yellow Pap., pp. 1–32, 2014.

[17] GitHub - ethereum/eth2.0-specs: Ethereum 2.0 Specifications.” [Online]. Available: https://github.com/ethereum/eth2.0-specs. [Accessed: 20-Apr-2021].

[18] E. F. Kfoury, D. Khoury, A. Alsabeh, J. Gomez, J. Crichigno, and E. Bou-Harb, “A Blockchain-based Method for Decentralizing the ACME Protocol to Enhance Trust in PKI,” 2020 43rd Int. Conf. Telecommun. Signal Process. TSP 2020, no. May, pp. 461–465, 2020, doi: 10.1109/TSP49548.2020.9163555.