Published by :
http://www.ijert.org

International Journal of Engineering Research & Technology (IJERT)
ISSN: 2278-0181
Vol. 12 Issue 11, November-2023

Blockchain's Influence on The Internet Of Vehicles : A Comprehensive Review

Kiranpreet Kaur, Harish Kumar and Sakshi Kaushal
University Institute of Engineering and Technology, Panjab University, Chandigarh 160014, India

Abstract. Blockchain technology has wielded substantial influence through its introduction as a Peer-to-Peer system. This innovation has revolutionized trans- action recording, providing a decentralized, transparent, and exceptionally secure database solution. This technological advancement has garnered considerable research focus in diverse fields, including the realm of Internet of Vehicles (IoVs). By harnessing blockchain, IoVs aim to tackle centralization issues and improve the overall architecture, creating a secure and decentralized vehicular environment. This survey provides a thorough examination of the diverse appli- cations of blockchain technology in the context of the Internet of Vehicles (IoVs). The paper introduces the fundamental concepts of both IoVs and blockchain tech- nology and conducts a review of existing surveys that investigate the utilization of blockchain in IoVs. Following this, the study delves into the integration of blockchain and IoVs from four distinct perspectives. Finally, future research di- rections for integrating blockchain technology in IoVs are outlined.

Keywords: Blockchain, IoV, Security, Data Management

I. INTRODUCTION

The exponential growth of connected vehicles necessitates a robust decentralized sys- tem to validate and secure communication. Blockchain, a revolutionary distributed ledger technology, has garnered significant attention as a potential solution to address the vulnerabilities of Vehicular Ad Hoc Networks (VANETs) [1],[2]. VANETs have emerged as a transformative technology in the automotive industry, enabling real-time vehicle-to-vehicle (V2V) and vehicle-to-infrastructure (V2I) communication to en- hance road safety and transportation efficiency. The Intelligent Transportation System (ITS) leverages advanced technologies, including blockchain and VANETs, to elevate transportation efficiency and safety. By utilizing real-time data analysis and communi- cation networks, ITS optimizes traffic flow, mitigates congestion, and elevates the man- agement of transportation systems. However, as VANETs become integrated into our increasingly connected and autonomous world, new challenges arise, particularly con- cerning data security, privacy, and trust. By harnessing blockchain technology, it is possible to securely store all details regarding the entire lifespan of vehicles. This encompasses vehicle certificates, insurance records, and pertinent data. Additionally, the blockchain can also serve as a tamper-proof ledger for logging data related to in- fractions, mechanical issues, and supplementary certifications for automotive dealers. Incentive mechanisms within the blockchain can promote vehicle cooperation, while smart contracts ensure the secure and efficient execution of processes [3]. While earlier investigations have delved into incorporating blockchain within the Internet of Things (IoT) framework, certain research works have exclusively investigated the utilization of blockchain technology within the context of Internet of Vehicles (IoVs) [4], [5]. For instance, research has delved into trust management in Social IoVs (SIoVs) and ex- plored different blockchain technologies applied in IoVs [6]. Additionally, application examples of blockchain in VANETs encompass scenarios such as preventing forged data, revoking network certificates, vehicular authorization, and transportation ser- vices. This paper aims to comprehensively explore the multifaceted role of blockchain in IoVs, elucidating its potential to revolutionize trust management, data integrity, and privacy preservation aspects of vehicular networks [7]. By thoroughly examining state- of-the-art research and practical implementations [8-11], this paper seeks to provide a comprehensive understanding of how blockchain can create a secure and transparent environment for IoVs, paving the way for the widespread adoption of intelligent and secure vehicular communication systems.

The paper is structured as follows: Section 2 provides a concise introduction to the Internet of Vehicles (IoV) and blockchain, along with highlighting the potential features of both technologies. Section 3 focuses on the integration of blockchain and IoV, cov- ering various aspects such as security, certificate management, data management, and privacy preservation, with in-depth discussions. In Section 4, the paper examines po- tential future directions of blockchain implementation in IoVs. Finally, Section 5 pre- sents the concluding remarks of this survey.

1. BACKGROUND

1.1 Internet of Vehicles

The Internet of Vehicles (IoV) is a groundbreaking concept that represents the conver- gence of two transformative technologies: the Internet of Things (IoT) and vehicular communication systems. IoV envisions a highly interconnected ecosystem where vehi- cles, infrastructure, and other smart devices communicate seamlessly, creating a dy- namic and intelligent transportation network [12], [13]. This paradigm shift has the po- tential to revolutionize the automotive industry, road safety, traffic management, and overall transportation efficiency. At the core of IoV lies the integration of advanced sensors, communication modules, and computing capabilities into vehicles, transform- ing them into "smart" entities [14]. Figure 1 represents the communication of the inter- net of vehicles in different fields. These interconnected vehicles have the capability to share real-time information among themselves and with the surrounding infrastructure, such as traffic lights, road signs, and roadside sensors. This communication is facili- tated through various wireless technologies, including Dedicated Short-Rang Communications (DSRC), Cellular Vehicle-to-Everything (C-V2X), and Wi-Fi, among others.

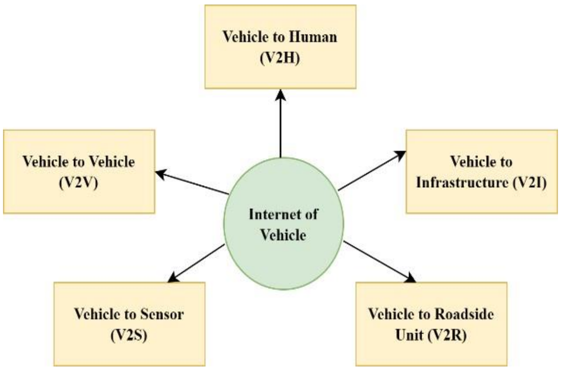

Fig. 1. Internet of Vehicle Communication

One of the primary benefits of IoV is its impact on road safety. Connected vehicles can continuously share information about their speed, location, and trajectory, allowing them to detect potential collisions or hazardous road conditions. This real-time aware- ness enables them to proactively take evasive actions, preventing accidents and poten- tially saving lives. Furthermore, IoV can also contribute to traffic management by providing comprehensive traffic flow data to optimize signal timings, reduce conges- tion, and improve overall transportation efficiency. In addition to safety and traffic management, IoV unlocks a myriad of innovative applications and services. For in- stance, drivers can access real-time navigation assistance based on live traffic updates, road closures, and alternative routes. Entertainment and infotainment services can be seamlessly integrated into the vehicle's infotainment system, providing occupants with an enhanced travel experience. Moreover, IoV can be leveraged to enable remote vehi- cle diagnostics and software updates, streamlining maintenance processes and ensuring optimal vehicle performance.

However, the realization of IoV comes with several challenges. One of the most significant concerns is data privacy and security. As vehicles continuously exchange sensitive information, including geolocation and driver behavior data, protecting this information from unauthorized access and potential cyberattacks becomes paramount. Adopting robust encryption and authentication mechanisms, as well as implementing secure communication protocols, is essential to ensure the confidentiality and integrity of the data transmitted within the IoV ecosystem. Another critical challenge is the standardization and interoperability of IoV technologies. With numerous manufacturers and stakeholders involved, ensuring seamless communication and collaboration be- tween different devices and systems is vital. Standardization efforts are crucial in es- tablishing a unified framework that allows diverse IoV components to communicate effectively, promoting compatibility and scalability across the transportation network.

1.1 Blockchain

Blockchain stands as a highly acclaimed technology that functions on a Peer-to-Peer framework, as demonstrated by the example of Bitcoin [15]. This decentralized struc- ture guarantees that all participants within the network possess an identical and unal- terable replica of the blockchain data. Furthermore, user identities are preserved through a public key system, ensuring both anonymity and privacy. The technology of blockchain provides a transparent, immutable, and secure environment for storing data. The fundamental unit of information in a blockchain is referred to as a "block," and it is generated through cryptographic methods to record valid transaction details, which are then confirmed by each member of the network. A block comprises two primary components: the block header, containing metadata, and the block body, which encom- passes the transaction data. The block header is constructed from three sets of metadata. The first pertains to a reference hash of a preceding block, establishing a connection between the current and previous blocks in the blockchain. The second set of metadata involves elements related to the mining process, which includes difficulty, timestamp, and nonce values. Refer to Figure 2 for a visual representation of the blockchain's block structure.

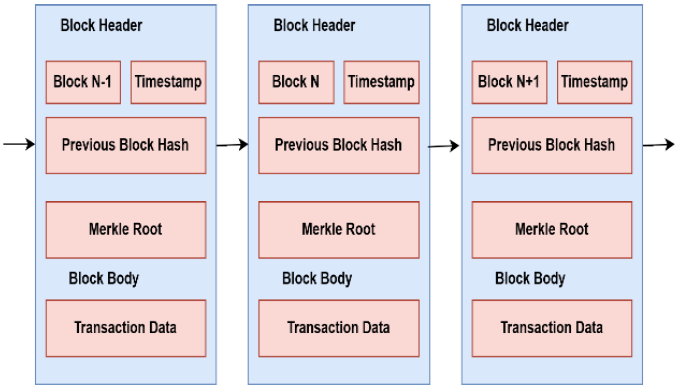

Fig. 2. Data Structure of Blocks

- The consensus process in blockchain technology has been supported by several pro- posed algorithms, each with its unique characteristics. These consensus algorithms in- clude PoW (Proof of Work), PoS (Proof of Stake), DPOS (Delegated Proof of Stake), PBFT (Practical Byzantine Fault Tolerance), Ripple, Tendermint, and Paxos. These al- gorithms determine how agreement is reached among network peers.
Three different Blockchain types are [16]:

- The Public blockchain is decentralized, which means it is completely distributed and permissionless, So any entity can access the communication network of the blockchain, whenever they want to. To store data within the blockchain network, there are some set processing fees required.

- A Private blockchain is run by a single organization and is both partially distributed and permission, with each peer member being well-known to the organization. The private blockchain does not charge a transaction processing fee compared to the pub- lic blockchain network.
- The Federated blockchain, which combines public and private blockchains, does not have a single organization in control (administered by a group). It very certainly offers comparable advantages to a private blockchain.

Initially, Bitcoin was designed mainly for cryptocurrency exchange and did not include support for smart contracts. Smart contracts, introduced by Szabo [17], are digital con- tracts with predefined rules that execute automatically and can be trusted. Contempo- rary platforms such as Ethereum [18] and Hyperledger [19] offer programmable smart contracts, enabling users to deploy various services, applications, or contracts on these platforms. Both R3 Corda [20] and Hyperledger [19] are categorized as consortium blockchains, serving more private and controlled environments compared to public blockchains that prioritize public participation and full transparency. In public block- chains, nodes, referred to as miners, participate in the consensus process to earn re- wards, whereas private blockchains prioritize data privacy and transaction speed, en- suring secure information storage and exchange.

Based on the previous analysis of the Internet of Vehicles (IoVs) and the challenges it faces regarding security, privacy, cooperation, and trust, there is a pressing need for more dependable and scalable solutions. Blockchain possesses several compelling fea- tures that make it an appealing technology to tackle these issues in IoV

Table 1. Key Concepts in Modern Database Management

Decentralization:	Decentralization ensures that all nodes have equal rights and responsibilities. Even if a node becomes inactive, it does not impact the overall functioning of the system.
Transparency:	Transparency in the blockchain is inherent since nodes do not need to develop trusting relationships with one another. The entire system operates openly and transparently, ensuring that nodes cannot deceive one another within the established rules
Collective mainte- nance:	Collective maintenance is a characteristic of the blockchain system where all nodes contribute to its maintenance. Each par- ticipant in the system actively takes part in the maintenance tasks.

Reliable database:	The blockchain ledger is a trustworthy database because every network node has a copy of it. The system automatically com- pares data records across all nodes, invalidating any attempt to alter the database on a single node.
Automation:	Smart contracts facilitate automation in the system, enabling seamless execution of resource and data-sharing services with- out the need for human intervention.

1. Integration of IoV and Blockchain

Integration of the IoV with Blockchain technology holds immense promise in revolu- tionizing the transportation industry. IoV, an emerging paradigm that connects vehicles, infrastructure, and smart devices, aims to enhance road safety, traffic management, and overall transportation efficiency [21]. On the other hand, Blockchain, a distributed ledger technology, ensures trust, transparency, and security in data transactions. Com- bining these two transformative technologies opens up a multitude of possibilities and benefits.

One of the key advantages of integrating Blockchain with IoV is the enhancement of data security and privacy. As vehicles continuously share sensitive information about their location, speed, and behavior, the decentralized and tamper-proof nature of Block- chain ensures that this data remains immutable and secure. By leveraging cryptographic techniques and consensus mechanisms, Blockchain creates an unalterable record of all transactions, making it extremely difficult for malicious actors to tamper with the data or launch cyberattacks. Moreover, the integration of Blockchain in IoV enables secure and efficient peer-to-peer communication among vehicles and infrastructure. Smart contracts, a feature of Blockchain, can facilitate the automatic execution of agreements and predefined rules between vehicles, road authorities, and service providers [22]. For example, in the case of autonomous vehicles, smart contracts can govern interactions between vehicles on the road, ensuring smooth traffic flow and safe coordination. Fig- ure 3 depicts the integration of blockchain in different fields of IoVs.

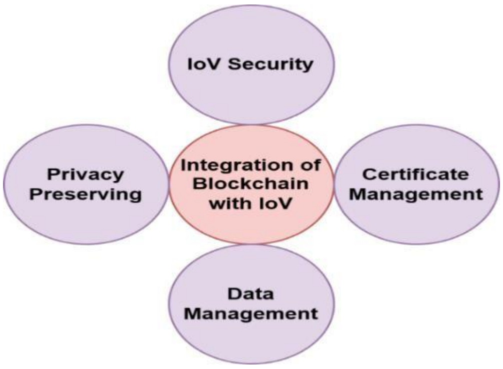

Fig. 3. Integration of Blockchain with IoV

1.1 Integration of Blockchain with IoV

The centralized model of the Internet of Vehicles (IoV), relying on third-party trust authorities, gives rise to several security challenges. Firstly, any failure in the central- ized authority could disrupt the entire system, posing a significant threat to system availability. Additionally, the traditional IoV model necessitates the implementation of access control mechanisms and message validation operations to maintain network se- curity [23]. In the subsequent sections, how the integration of blockchain technology addresses these security concerns by enhancing access control and message validation in the IoV ecosystem is explored.

Access Control in IoV with Blockchain

. Incorporating blockchain technology into the realm of Internet of Vehicles (IoV) tackles security obstacles, specifically in the realms of access control and message val- idation. One strategy involves a three-stage system that utilizes blockchain for vehicle verification and safeguarding privacy. The initial authentication phase utilizes smart contracts to ensure the integrity and confidentiality of the system [24]. Another study introduces two blockchains, local and main, to solve authentication problems in VANETs. The local blockchain stores vehicle movement and message data, while the main blockchain records unusual events. To handle large message traffic, the local blockchain is divided into parallel blockchains for different regions. Additionally, the concept of intelligent vehicle trust points (IVTP) evaluates vehicle trustworthiness. However, the distribution and earning mechanism of IVTP is not extensively detailed. Overall, both approaches demonstrate the potential of blockchain in enhancing access control and security in IoV and VANETs.

Message Validation in IoV with Blockchain

. The advancement of communication technology in Intelligent Transportation Sys- tems (ITSs) have led to increased information sharing in vehicular networks [25]. How- ever, the risk of forged messages and malicious attacks remains a concern. To address this, message verification mechanisms have been explored. One approach is clustering vehicles and electing cluster headers (CHs) to communicate with other CHs, as pro- posed in the paper [26]. Another paper [27] introduces the trust clustering mechanism for VANET (TCMV), which validates the credibility of CHs for secure message ex- changes based on vehicle reputation. To further enhance message verification, the paper
[28] introduces a blockchain-based distributed TCMV (DTCMV) that involves mes- sage transmission, block creation, and validation, where RSUs act as miners. Addition- ally, paper [29] presents the blockchain-based traffic event validation (BTEV) frame- work, which uses a two-pass threshold-based event validation mechanism and a proof- of-event (PoE) consensus to ensure event reliability, incorporating the Merkle Patricia Trie (MPT) structure for efficient event submission through RSUs. This combination of blockchain and message validation mechanisms enhances the security and credibility of information exchange in the Internet of Vehicles (IoV) ecosystem.

1.1 Certificate management in IoV with Blockchain

Certificate management in the context of the IoV with blockchain refers to the process of handling and maintaining digital certificates to ensure secure and authenticated com- munication among vehicles and infrastructure within the IoV ecosystem [30]. Digital certificates play a crucial role in verifying the identities of participants, such as vehicles, drivers, and service providers, and in establishing secure connections for data exchange. In traditional centralized systems, a certificate authority (CA) issues and manages
digital certificates. However, in a decentralized and trustless environment like the IoV, relying solely on a central authority may lead to potential security vulnerabilities and single points of failure. Blockchain technology offers a robust and tamper-proof solu- tion to address these concerns. When implemented in IoV, blockchain serves as a dis- tributed and transparent ledger that securely stores and validates digital certificates. Here's how certificate management in IoVs with blockchain works: Blockchain tech- nology in the IoV enables secure and decentralized certificate issuance, acting as a Cer- tificate Authority. Transactions are transparently recorded on the blockchain, facilitat- ing certificate verification and revocation processes. With digital certificates, IoV par- ticipants can establish secure and encrypted communications, enhancing network secu- rity and trust.

1.1 Data management in IoV with Blockchain

Data management in the IoV with blockchain involves the efficient and secure han- dling of vast amounts of data generated by vehicles, infrastructure, and other connected devices within the IoV ecosystem [31]. Blockchain technology offers unique features that can address data management challenges and enhance data integrity, security, and sharing capabilities within the IoV network.

By leveraging blockchain for data management, the IoV ecosystem can achieve en- hanced data security, transparency, and trust among participants. The decentralized and immutable nature of blockchain ensures that data is tamper-proof and can be seamlessly shared and analyzed, unlocking the full potential of the Internet of Vehicles in trans- forming transportation systems and services [32].

1.1 Privacy preserving in IoV with Blockchain

Privacy preservation in the IoV with blockchain refers to the measures taken to pro- tect the sensitive and personal information of individuals and vehicles while maintain- ing secure and transparent communication within the IoV ecosystem. With the increas- ing volume of data exchanged among vehicles and infrastructure, ensuring privacy be- comes a crucial aspect of maintaining user trust and compliance with data protection regulations [33]. Blockchain-based IoV systems offer enhanced privacy and data secu- rity through techniques like anonymity, encrypted data transmission, and private trans- actions. Participants can use pseudonyms or random identifiers, ensuring their identities remain protected. All data exchanged within the network is encrypted, accessible only to authorized parties. Private blockchains restrict access to sensitive data, and zeroknowledge proofs validate information without revealing actual data. Smart contracts enforce privacy policies and consent mechanisms, and off-chain data storage solutions keep sensitive data private [34]. Consent Management empowers participants to control data sharing, and trusted data aggregation preserves privacy during data aggregation processes. These measures collectively create a secure and privacy-preserving environ- ment in IoV networks.

By incorporating privacy-preserving mechanisms into IoV with blockchain, individ- uals, and vehicles can confidently participate in the network without compromising their sensitive information. Privacy preservation fosters trust among users, encourages data sharing, and ensures compliance with privacy regulations, thus facilitating the re- sponsible and secure development of the IoV [35].

1.1 Future Scope

The adoption of blockchain technology in the IoV space has demonstrated a variety of applications that improve the environment for vehicular networks. Future research tra- jectories in this area, though, deserve consideration.

- Trust in off-chain data remains a pressing concern for blockchain-based IoV ap- proaches. While blockchain has addressed trust challenges for on-chain data, ensur- ing the credibility and security of off-chain data requires further investigation.
- Resource management in blockchain-based IoV systems necessitates efficient han- dling of high transaction volumes, minimizing energy consumption and data trans- mission/storage overheads.
- Standardized evaluation criteria and comparative experiments are essential to high- light advantages and ensure the real-world applicability of IoV architectures and al- gorithms.
- The integration of various technologies (SDN, 5G, NFV) in the IoV architecture presents challenges, particularly in designing a secure and privacy-focused frame- work.

2. Conclusion

Every car is anticipated to be online in the Internet of Vehicles (IoVs) future vision, and blockchain technology is likely to provide affordable financing support for essen- tial vehicle data. Blockchain functions as a useful distributed ledger by getting over the drawbacks of centralized IoV architectures. Although the combination of blockchain and IoVs has been studied in previous surveys, there are still many undiscovered ele- ments in these applications. This study compares and contrasts numerous surveys on blockchain applications with an emphasis on how well they integrate with IoVs. We examine various theories proposed in recent studies, encompassing topics such as se- curity for Internet of Vehicles (IoV) through blockchain, the management of trust and certificates, as well as the safeguarding of privacy within the IoV ecosystem. The study addresses significant obstacles that IoVs are facing by identifying unresolved questions and future research directions

REFERENCES

[1] O. Kaiwartya, A.H. Abdullah, Y. Cao, A. Altameem, M. Prasad, C. Lin, X. Liu, Internet of vehicles: motivation, layered architecture, network model, challenges, and future aspects. IEEE Access 4, 5356–5373 (2016).

[2] J. Contreras-Castillo, S. Zeadally, J.A. Guerrero-Ibañez, Internet of vehicles: architecture, protocols, and security. IEEE Internet Things J. 5(5), 3701–3709 (2017).

[3] Hemani, D. S. Singh and R. K. Dwivedi, "Blockchain Enabled Autonomous Vehicle Based Vehicular IoT System," 2023 International Conference on Intelligent and Innovative Tech- nologies in Computing, Electrical and Electronics (IITCEE), Bengaluru, India, 2023, pp. 762-767, doi: 10.1109/IITCEE57236.2023.10090950.

[4] M. Bharathi, K. Geetha, P. K. Mani., G. N. Samuel Vijayakumar, K. Srinivasan and K. R. Kumar, "AI and IoT-based Electric Vehicle Monitoring System," 2022 Sixth International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Dharan, Nepal, 2022, pp. 722-727, doi: 10.1109/I-SMAC55078.2022.9987282.

[5] Wang, C., Cheng, X., Li, J. et al. A survey: applications of blockchain in the Internet of Vehicles. J Wireless Com Network 2021, 77 (2021). https://doi.org/10.1186/s13638-021-01958-8.

[6] R. Jabbar et al., "Blockchain Technology for Intelligent Transportation Systems: A System- atic Literature Review," in IEEE Access, vol. 10, pp. 20995-21031, 2022, doi: 10.1109/ACCESS.2022.3149958.

[7] A. Dorri, M. Steger, S.S. Kanhere, R. Jurdak, Blockchain: a distributed solution to automo- tive security and privacy. IEEE Commun. Mag. 55(12), 119–125 (2017).

[8] A. Dorri, S.S. Kanhere, R. Jurdak, Blockchain in internet of things: challenges and Solutions (2016). arXiv:1608.05187.

[9] M.A. Ferrag, M. Derdour, M. Mukherjee, A. Derhab, L. Maglaras, H. Janicke, Blockchain technologies for the internet of things: research issues and challenges. IEEE Internet Things J. 6(2), 2188–2204 (2019).

[10] M.S. Ali, M. Vecchio, M. Pincheira, K. Dolui, F. Antonelli, M.H. Rehmani, Applications of blockchains in the internet of things: a comprehensive survey. IEEE Commun. Surv. Tutor. 21(2), 1676–1717 (2019) 10. R. Iqbal, T.A. Butt, M. Afzaal, K. Salah, Trust management in social internet of vehicles: factors, challenges, blockchain, and fog solutions. Int. J. Distrib. Sens. Netw. 15(1),

1550147719825820 (2019). https://doi.org/10.1177/1550147719 825820.

[11] L. Mendiboure, M.A. Chalouf, F. Krief, Survey on blockchain-based applications in internet of vehicles. Comput. Electr. Eng. 84, 106646 (2020). https://doi.org/10.1016/j.compele- ceng.2020.106646.

[12] F. Yang, S. Wang, J. Li, Z. Liu, Q. Sun, An overview of internet of vehicles. China Commun. 11(10), 1–15 (2014).

[13] L. Mendiboure, M.A. Chalouf, F. Krief, Towards a 5g vehicular architecture, in Communi- cation Technologies for Vehicles. ed. by B. Hilt, M. Berbineau, A. Vinel, M. Jonsson, A. Pirovano (Springer, Cham, 2019), pp. 3–15.

[14] S. Tanwar, J. Vora, S. Tyagi, N. Kumar, M.S. Obaidat, A systematic review on security issues in vehicular ad hoc network. Secur. Privacy 1(5), 39.

[15] S. Nakamoto, Bitcoin: a peer-to-peer electronic cash system. Technical report, Manubot (2019).

[16] A. Tiwari, V. Agarwal, Y. Aggarwal and U. Srivastava, "Server Security in Cloud Compu- ting Using Blockchain," 2022 8th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2022, pp. 963-966, doi: 10.1109/ICACCS54159.2022.9785060.

[17] N. Szabo, Formalizing and securing relationships on public networks. First Monday (1997).

[18] G. Wood et al., Ethereum: a secure decentralised generalised transaction ledger. Ethereum Proj. Yellow Pap. 151(2014), 1–32 (2014).

[19] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, et al., Hyperledger fabric: a distributed operating system for permissioned blockchains, in Proceedings of the Thirteenth EuroSys Conference (2018), pp. 1–15.

[20] M. Valenta, P. Sandner, Comparison of ethereum, hyperledger fabric and corda, no. June (2017), pp. 1–8.

[21] Chen, C.; Quan, S. RSU Cluster Deployment and Collaboration Storage of IoV Based Blockchain. Sustainability 2022, 14, 16152. https://doi.org/10.3390/su142316152.

[22] S. Majumder, A. Mathur, A. Javaid, A study on recent applications of blockchain technology in vehicular adhoc network (VANET) (2020), pp. 293–308.

[23] D. Das, S. Banerjee, W. Mansoor, U. Biswas, P. Chatterjee and U. Ghosh, "Design of a Secure Blockchain-Based Smart IoV Architecture," 2020 3rd International Conference on Signal Processing and Information Security (ICSPIS), DUBAI, United Arab Emirates, 2020, pp. 1-4, doi: 10.1109/ICSPIS51252.2020.9340142.

[24] S. M. Karim, A. Habbal, S. A. Chaudhry and A. Irshad, "BSDCE-IoV: Blockchain-Based Secure Data Collection and Exchange Scheme for IoV in 5G Environment," in IEEE Access, vol. 11, pp. 36158-36175, 2023, doi: 10.1109/ACCESS.2023.3265959.

[25] S. Yu, J. Lee, K. Park, A. K. Das and Y. Park, "IoV-SMAP: Secure and Efficient Message Authentication Protocol for IoV in Smart City Environment," in IEEE Access, vol. 8, pp. 167875-167886, 2020, doi: 10.1109/ACCESS.2020.3022778.

[26] V. Sharma, An energy-efcient transaction model for the blockchain-enabled internet of ve- hicles (IoV). IEEE Commun. Lett. 23(2), 246–249 (2019).

[27] A. Kchaou, R. Abassi, S.G. El Fatmi, Towards a secured clustering mechanism for messages exchange in VANET, in 2018 32nd International Conference on Advanced Information Net- working and Applications Workshops (WAINA) (2018), pp. 88–93.

[28] A. Kchaou, R. Abassi, S. Guemara, Toward a distributed trust management scheme for VANET, in Proceedings of the 13th International Conference on Availability, Reliability and Security (2018), pp. 1–6.

[29] Y.-T. Yang, L.-D. Chou, C.-W. Tseng, F.-H. Tseng, C.-C. Liu, Blockchain-based trafc event validation and trust verifcation for vanets. IEEE Access 7, 30868–30877 (2019).

[30] E. M. Cho and M. N. S. Perera, "Efficient Certificate Management in Blockchain based Internet of Vehicles," 2020 20th IEEE/ACM International Symposium on Cluster, Cloud and Internet Computing (CCGRID), Melbourne, VIC, Australia, 2020, pp. 794-797, doi: 10.1109/CCGrid49817.2020.000-8.

[31] D. Das, S. Banerjee, P. Chatterjee, U. Ghosh, W. Mansoor and U. Biswas, "Design of an Automated Blockchain-Enabled Vehicle Data Management System," 2022 5th International Conference on Signal Processing and Information Security (ICSPIS), Dubai, United Arab Emirates, 2022, pp. 22-25, doi: 10.1109/ICSPIS57063.2022.10002493.

[32] M. Yuan et al., "TRUCON: Blockchain-Based Trusted Data Sharing With Congestion Con- trol in Internet of Vehicles," in IEEE Transactions on Intelligent Transportation Systems, vol. 24, no. 3, pp. 3489-3500, March 2023, doi: 10.1109/TITS.2022.3226500.

[33] W. Jiang, M. Chen and J. Tao, "Federated learning with blockchain for privacy-preserving data sharing in Internet of vehicles," in China Communications, vol. 20, no. 3, pp. 69-85, March 2023, doi: 10.23919/JCC.2023.03.006.

[34] R. Kumar, P. Kumar, R. Tripathi, G. P. Gupta and N. Kumar, "P2SF-IoV: A Privacy-Preser- vation-Based Secured Framework for Internet of Vehicles," in IEEE Transactions on Intel- ligent Transportation Systems, vol. 23, no. 11, pp. 22571-22582, Nov. 2022, doi: 10.1109/TITS.2021.3102581.

[35] H. Chai, S. Leng, J. He, K. Zhang and B. Cheng, "CyberChain: Cybertwin Empowered Blockchain for Lightweight and Privacy-Preserving Authentication in Internet of Vehicles," in IEEE Transactions on Vehicular Technology, vol. 71, no. 5, pp. 4620-4631, May 2022, doi: 10.1109/TVT.2021.3132961.