Abstract—With the rapid development of the Internet of Things (IoT) and its potential integration with the traditional Vehicular Ad-Hoc Networks (VANETs), we have witnessed the emergence of the Internet of Vehicles (IoV), which promises to seamlessly integrate into smart transportation systems. However, the key characteristics of IoV, such as high-speed mobility and frequent disconnections make it difficult to manage its security and privacy. The Blockchain, as a distributed tamper-resistant ledger, has been proposed as an innovative solution that guarantees privacy-preserving yet secure schemes. In this paper, we review recent literature on the application of blockchain to IoV, in particular, and intelligent transportation systems in general.

Keywords—blockchain, IoV, VANET, trust, security, privacy

I. INTRODUCTION

The Internet of Vehicles (IoV) has emerged as a result of the convergence of the Internet of Things (IoT) and Vehicular Ad-Hoc Networks (VANETs). IoV offers ubiquitous access to information to drivers and passengers while on the move [1]. IoV has many promising applications such as intelligent traffic optimization [2], sensor-based accident prediction [3], entertainment content delivery [4], and electric vehicle charging scheduling [5]. However, with the fast-growing number of connected vehicles, IoV requirements are difficult to satisfy, e.g. secure, scalable, robust, seamless information exchange among vehicles, users, and roadside infrastructures.

Blockchain [6], a distributed and immutable tamper-resistant ledger, manages persistence records of data at different nodes and has the potential to deal with the data security and privacy challenges in IoV networks. As shown in Figure 1, the application of Blockchain to IoV can be roughly divided into four classes, namely security, privacy, trust computing and incentive mechanisms. For security, Blockchain can be leveraged to solve the problems of traditional vehicular network security issues, such as public key infrastructure (PKI)-based solutions and ID-based solutions. Similarly, Blockchain-enabled privacy schemes for IoV ensure the identification of the privacy of the participating vehicles and their locations. Blockchain can also serve as a distributed reputation system that stores vehicles’ trust scores or store vehicle generated content. Finally, Blockchain can also be used to manage traffic-related cryptocurrencies for rewarding vehicles that helped the system. In this paper, we review recent literature on blockchain applications in IoV and intelligent transportation systems in general.

II. BLOCKCHAIN FOR IOV TRUST MANAGEMENT

Trust management refers to the methods that estimate the trustworthiness of other entities in the system. Based on the likelihood of trustworthiness assigned to a given entity, the system decides whether to interact with that arbitrary entity or not. The concept of trust is paramount in systems security, and it is discussed extensively in the network security literature [7]. In the context of vehicular networks, when the vehicle receives a message, the trust system must check the legitimacy and trustworthiness of the sender (node trust), as well as the trustworthiness of the received data or information (content trust). Considering the nature of vehicular networks, trust management plays a vital role in preventing network attacks that may cause serious consequences. For instance, in a safety-related VANET application of emergency warning, the application decides to operate the emergency brakes in case of...
It is worth noting that the blockchain is a public ledger that stores and updates trust records. This eliminates the need for a central trust authority to store the nodes’ trust scores in the blockchain. Kouicem et al. [15] proposed a blockchain-based group signature schemes to ensure conditional privacy, in case of fake message dissemination, malicious vehicles cannot tamper with their trust value on the blockchain. The transparency property gives the chance to access control and authentication, cannot be used to detect dishonest nodes or fake messages, a trust management system is necessary to guarantee the security of the network and it is supposed to complement the other security measures of access control and authentication.

The blockchain properties to tackle the challenges of trust management in vehicular networks. The blockchain is a state machine that stores a block for each new timestamp, previous block’s hash and the nonce. Some methods use basic PoW (Proof of Work) algorithm, while others use a hybrid PoW and PoS (Proof of Stake) consensus algorithm, where the more total votes the easier RSU can compute the nonce of the hash function. Singh et al. [10] used a conditional privacy based group signature schemes to ensure additional privacy, in case of fake message dissemination. Zhang et al. [9] based group signature schemes to ensure additional privacy, in case of fake message dissemination. Zhang et al. [9] proposed a blockchain-based group signature schemes to ensure additional privacy, in case of fake message dissemination. Zhang et al. [9] proposed a blockchain-based trustworthiness computing framework, which can act as an insurance policy for VANET, which need more efficient and scalable methods.

Vehicular nodes are more likely to participate in the computation and storage of the global trust management in MANET. Vehicular nodes need to cooperate to maintain a rating scheme to evaluate the trustworthiness of network nodes in MANET, their trust level, therefore trust bootstrapping is crucial in VANET, where the vehicles rate the correctness of the received message and upload their rating to the RSU. The vehicles and RSU community aggregates the ratings from the RSU community, the latter cooperates to maintain a distributed trust management system, and depend on other sources. Some methods use basic PoW (Proof of Work) algorithm, while others use a hybrid PoW and PoS (Proof of Stake) consensus algorithm, where the more total votes the easier RSU can compute the nonce of the hash function.

The transparency property gives the chance to access control and authentication, cannot be used to detect dishonest nodes or fake messages, a trust management system is necessary to guarantee the security of the network and it is supposed to complement the other security measures of access control and authentication. Some methods use basic PoW (Proof of Work) algorithm, while others use a hybrid PoW and PoS (Proof of Stake) consensus algorithm, where the more total votes the easier RSU can compute the nonce of the hash function. Singh et al. [10] used a conditional privacy based group signature schemes to ensure additional privacy, in case of fake message dissemination. Zhang et al. [9] proposed a blockchain-based group signature schemes to ensure additional privacy, in case of fake message dissemination. Zhang et al. [9] proposed a blockchain-based trustworthiness computing framework, which can act as an insurance policy for VANET, which need more efficient and scalable methods.
The transaction throughput. The relationship between security level and accessibility. The blockchain offers the possibility for anonymity, cryptography, and signature. Blockchain sharding decreases the computing overhead on blockchain exchange messages, such as bacon messages. Many unauthorized entities, including the GPS coordinates of the vehicles, try to hide the location information of the vehicles. Authorized access to the vehicle’s identity and exchanged messages is restricted to authorized entities. While the security measures can guarantee the privacy of the vehicles, the reward points could be spent to benefit from vehicular services, such as insurance and maintenance. Dhelim et al. introduced a blockchain privacy preserving scheme: a) a Bayesian inference model, b) decentralized privacy preserving schemes, and c) a trust management framework.

Privacy is one of the main requirements of IoV, the Internet of Vehicles. The vehicular networkakasheterarch (Vehicular Network Architecture) is divided into multiple channels, and each channel contains a network of vehicles. The access control rules to the data are defined by the law enforcement authority (LEA) in case of a dispute. The access control is based on blockchain, where the blockchain network is protected pseudonyms, to name one example. Common blockchain solutions based on blockchains are: consortium blockchain, private blockchain, and public blockchain. The access control rules are defined by the LEA in case of a dispute. The blockchain network is protected pseudonyms, to name one example. Common blockchain solutions based on blockchains are: consortium blockchain, private blockchain, and public blockchain. The access control is based on blockchain. Makhdoom et al. designed a lightweight threshold certification scheme, in which the proxy signing keys are issued by a set of CAs that are managed by combining vehicular regions partition, geographical areas or clusters.

TABLE III.

| Work Type   | Blockchain Type | Privacy-preservation technique | Target privacy | Recommended privacy |
|-------------|-----------------|---------------------------------|----------------|---------------------|
| Blockchain privacy preserving scheme | Consortium blockchain | Personal identity privacy | Identity privacy | Recommend identity privacy |
| Blockchain privacy preserving scheme | Private blockchain | Multiple channels blockchain | Location privacy | Recommend location privacy |
| Blockchain privacy preserving scheme | Public blockchain | Distributed anonymous credentials | Traffic privacy | Recommend traffic privacy |

Authorized licensed use limited to the terms of the applicable license agreement with JSTOR. Restrictions apply.
they track legendary focuses. Furthermore, they execute PBFT algorithm to reach a generation. CL.

Incentives, taking longer paths to forward announcements back to proposed consent in the blockchain. The SmartCoins can be viewed recent literature on the vehicles establish trust connections to engage with introduced a blockchain attache performance of CP.

FADB, an access control scheme for VANET data based on based attribute encryption (CP) used to execute gathering signature verification functions to scale up the performance of CPABE. Furthermore, the lightweight vehicle

devices can outsource heavy encryption and

Traditional vehicular network security scheme depe...solutions required a key generation server. The former has the drawback of complicated solutions.

PKS scheme also offers batch signature management and evidence of a credible

ty privacy protection. Ali et al. addressed the problem, but it is difficult to scale up hybrid solutions in VANETs. However, Blockchain...based solutions need a certificate management, which is not...

Anonymity privacy protection. Group signatures and vector

Blockchain can be used to manage traffic and vehicle service stations, or a fuel station. Similarly, Khalid et al. proposed an incentive announcement network based on

V2V group key construction and real time group membership assignment with enhanced group key updating. Utilized for V2V group key construction and real time group membership assignment with enhanced group key updating. Utilized for a blockchain storage system, and blockchain is used for a blockchain storage system, and blockchain is...

Blockchain applications in IoV are not limited only to transactions and drivers’ information tamper resistant. They

using vehicles’ computational power to prevent malicious

transactions and drivers’ information tamper resistant. They
lightweight consensus mechanism that reduce transactions’

IoT Enabled Social Relationships Meet Artificial Social Intelligence,”
IEEE Internet Things J.

W. Zhang, N. Aung, S. Dhelim, and Y. Ai, “DIFTOS: A distributed
networks for urban environments,” Sensors (Switzerland)

N. Aung, W. Zhang, S. Dhelim, and Y. Ai, “Accident Prediction System
Urban Environments,” Information

“VeSoNet: Traffic networks based on Path Planning and Deep Reinforcement Learning,”
arXiv Prepr. arXiv:2111.05567

Zhang, K. Sultan, S. Dhelim, and Y. Ai, “Dynamic traffic
the internet of vehicles in smart cities,” Digit. Commun. Networks

C. Lás, Q. Lu, S. Dhelim, and H. Ning, “A Lightweight
Based IoT Identity Management Approach,” Futur. Internet

Trust Management Techniques for the Internet of Things: A Survey,”
IEEE Access

“Trust2Vec: Large Signed Network Embeddings,” IEEE Internet Things J.

R. Hussain, J. Lee, and S. Zeaddally, “Trust in VANET: A survey of
current solutions and future research opportunities,” IEEE Trans. Intell.
Transp. Syst.

H. Zhang, J. Liu, H. Zhao, P. Wang, and N. Kato, “Blockchain
Trust Management for Internet of Vehicles,” IEEE Trans. Emerg. Top.
Comput.

K. Yang, L. Lei, K. Zheng, and V. C. M. Leung, “Blockchain
based decentralized trust management in vehicular networks,” IEEE
Internet Things J.

X. Liu, H. Huang, F. Xiao, and Z. Ma, “A Blockchain
Scheme for VANETs,” IEEE Internet Things J.

F. Lai, and J. Liu, “B
VANETs,” IEEE Trans. Emerg. Top. Comput.

U. Javaid, M. N. Aman, and B. Sikdar, “A Scalable Protocol for Driving
electric vehicles with Blockchain,” IEEE Internet Things J.

D. E. Kouicem, Y. Imine, A. Bouabdallah, and H. Lakhlef, “A
Internet of Things,” IEEE Trans. Dependable Secur. Comput.

Nandi, “Blockchain
Vehicles Using Smart Contract,” IEEE Trans. Intell. Transp. Syst.

S. Dhelim, H. Ning, and T. Zhu, “STLF: Spatial knowledge representation and object mapping framework,” in 2016
IEEE International Conference on Systems, Man, and Cybernetics (SMC)

S. Dhelim, H. Ning, and N. Aung, “ComPath: User Interest Mining in Heterogeneous Signed Social Networks for Internet of People,” IEEE Internet Things J.

S. Dhelim, H. Ning, M. A. Bouras, and J. Ma, “Cyber Centric Smart Home Architecture,” in 2018 IEEE SmartWorld, Ubiquitous Intelligence & Computing, Advanced & Trusted Computing, Scalable Computing & Communications, Cloud & Big Data Computing, Internet of People and Smart City Innovations

S. Dhelim, N. Aung, and H. Ning, “Mining user interest based on personality aware hybrid filtering in social networks,” Knowledge-Based Syst.

S. Dhelim, H. Ning, N. Aung, R. Huang, and J. Ma, “Personality
Metapath Discovery,” IEEE Trans. Comput. Syst.

S. Dhelim, N. Aung, M. A. Bouras, H. Ning, and E. Cambria, “A survey aware recommendation systems,” Artif. Intell. Rev.

D. Wei, F. Shi, and S. Dhelim, “A Self Unknown Internet Traffic Identification Based on Surge Period,” Futur.
Internet

X. Liu, H. Huang, F. Xiao, and Z. Ma, “A Blockchain
Based Location Privacy Protection Scheme in VANET,” IEEE Trans.
Veh. Technol.

H. Ning, S. Dhelim, M. A. Bouras, A. Khelloufi, and A. Ullah, “Cyber Classification, Recovery and Prevention,”
IEEE Access

W. Zhang, H. Ning, F. Shi, S. Dhelim, W. Zhang, and L. Chen, “A
thinking hyperspace,” Comput. Electr. Eng.

W. Wang, H. Ning, F. Shi, S. Dhelim, W. Zhang, and L. Chen, “A
Human-Machine Syst.

Y. Shen, N. Aung, W. Zhang, and H. Ning, “A hybrid
and types models,” J. Ambient Intell. Humaniz. Comput.

C. Wang, J. Shen, J.
IEEE Access

Z. Lu, Q. Wang, G. Qu, and Z. Liu, “BARS: A Blockchain
Futur. Internet

Authorized licensed use limited to: Cornell University Library. Downloaded on March 05,2023 at 03:15:20 UTC from IEEE Xplore. Restrictions apply.
I. Ali, M. Gervais, E. Ahene, and F. Li, “A blockchain
preserving authentication scheme for VANETs,” IEEE Trans.
Very Large Scale Integr. Syst. 27, no. 12, pp. 2792–2803, 
Dec. 2018, pp. 1–13.

X. Ma, C. Ge, and Z. Liu, “Blockchain
preserving location privacy protection,” IEEE Access
69, no. 3, pp. 2411–2423, Mar. 2020, pp. 1–11.

S. A. George, A. Jaekel, and I. Saini, “Secure identity management
based blockchain for vehicular social networks,” in 2020
IEEE Symposium on Computers and Communications (ISCC),
Jun. 2020, pp. 1–6.

Y. Pu, J. Liu, and B. Hu, “A consortium blockchain
based privacy preserving scheme for vehicular social
networks,” IEEE Access 8, vol. 12, pp. 102464–102475, 
2020.

B. Gueguih and H. Lu, “Blockchain
preserving authentication and message dissemination scheme for VANET,” in Proceedings of the 2019 5th International Conference on Systems, Control and Communications (ICSCC), Aug. 2019, pp. 1–6.

W. Yang, X. Dai, J. Xiao, and H. Jin, “LDV: A lightweight DAG
based blockchain for vehicular social networks,” IEEE Trans. Veh.
Technol. 69, no. 6, pp. 6578–6589, Jun. 2020, doi: 10.1109/TVT.2020.2990732.

Y. Li and B. Hu, “A consortium blockchain
based privacy preserving authentication scheme for electric vehicles,” IEEE Trans. Ind. Informatics 16, no. 5, pp. 3517–3526, May 2020, doi: 10.1109/TII.2020.2990732.

B. Gueguih and H. Lu, “Blockchain
incentive announcement network for communications of smart cities,” in 2020 International Wireless Communications and Mobile Computing (IWCMC), Aug. 2020, pp. 1–6.

D. Zheng, C. Jing, R. Guo, S. Gao, and L. Wang, “A traceable
and anonymous location privacy preservation in VANETs,” IEEE Access
8, no. 12, pp. 107771–107782, Mar. 2020.

N. Aung, W. Zhang, S. Dhelim, and Y. Ai, “T-Pre: A novel
incentive pricing system for the Internet of Vehicles in Smart Cities,” Information 11, no. 10, pp. 2152–2162, Oct. 2020, doi: 10.3390/info11102152.