Trustful Blockchain-Enabled Identity Management for VANET with Short-Latency Authentication

Jiayue Zhou*, Jianan Hong†, Chengchen Zhu†, Futai Zou† and Cunqing Hua†
*SJTU-Paris Institute of Technology, Shanghai Jiao Tong University, China
†School of Cyber Science and Engineering, Shanghai Jiao Tong University, China

***Abstract*—Blockchain technology has emerged as a popular research topic, particularly in the area of identity management, which provides with a decentralized ID system due to its inherent distributed architecture. This paper focuses on the security issues for vehicular ad-hoc networks (VANETs), where there exists significant obstacles to deploy blockchain-based identity management system. The idea of lightweight node seems to address such issues, as it provides a local transaction query method. However, it cannot directly suit the complex identity management scenario, as malicious revoked users can successfully exploit spoofing attacks to mislead the lightweight nodes. This paper therefore proposes a new blockchain-enabled identity management scheme for VANET system, which realizes extremely short-latency identity verification with the idea lightweight node. Especially, to achieve trustful revocation for lightweight node, we leverage the mechanism of redactable blockchain with chameleon hash, as well our tailored security protocols. The proposed scheme offers a highly secure, distributed and low-cost identity management system. The experimental result shows our advantage in terms of functionality and efficiency.**

***Index Terms*—Redactable blockchain, VANET, chameleon hash, revocation, lightweight node.**

I. Introduction

The technique of Vehicular Ad-Hoc Networks (VANETs) leads to the development of V2X communications, which is formed as a combination of Vehicle-to-Vehicle (V2V), Vehicle-to-Infrastructure (V2I), and Vehicle-to-Pedestrian (V2P) communications [1]. Such technology makes the future transportation system smart and safe. However, due to the importance of messages transmitted in VANET (e.g., for navigation, accident avoidance), the false message will bring in inestimable safety problems, such as traffic jams and even severe incidents. Thus, the identity validity and reliability check should be taken into account during the system deployment [2]. Whereas, it is challenging to deploy identity management, since the entities are authorized by various providers. For instance, vehicles are identified by different car manufacturers,

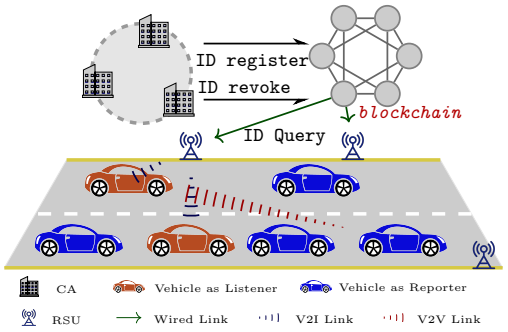

Fig. 1. A Scenario of Blockchain-enabled VANETs System

or network service providers, and the roadside units (RSU) are provided by governments, or other organizations. As a result, the centralized Public Key Infrastructure (PKI) method no longer works. With the decentralization and immutable property, blockchain is a natural carrier of secure and reliable identity management mechanism and is applied to many network scenarios [3, 4]. This attractive property increases functionality for identity management and authentication in terms of distributed deployment, trust level, robustness.

A blockchain-enabled communication and identity system is as shown in Fig. 1. The vehicles will report safety or informative messages to neighbor vehicles via wireless channels, and the RSU can also help transmit messages, as they can access the Internet via wired channels. There are multiple certificate authorities (CAs) to issue identity certificates, identify trust levels and even revoke privileges for RSUs and vehicles. For the report listeners, they rely on the blockchain to verify the identity of message sources. Nonetheless, due to the high dynamics of vehicular networks, maintaining rapid connectivity is difficult. Also, V2X network applications heavily rely on real-time communication [5], such as cooperative collision warning and remote vehicle diagnostics. For these

979-8-3503-7099-7/24/$31.00 ©2024 IEEE

restrictions, such authentication process of the DPKI model [6] is challenging: when a vehicle needs to authenticate its identity to another entity, an unstable link may cause a severe latency problem, as the verification needs information from the remote blockchain peers.

To address these challenging problems, this paper proposes a lightweight node-based VANET identity management architecture, allowing the vehicles act as lightweight nodes. A lightweight node in blockchain only stores the header information (as depicted in Fig. 2) of each block. A lightweight-node vehicle verifies a transaction locally, rather than remote peers, thus suits the latency-constrained VANETs. Whereas, such architecture cannot directly be used in identity management due to the revocation event. An instance is shown in Fig. 3: a vehicle's identity is revoked in block j. However, when it wants to prove the "validity" of the identity, since the lightweight node cannot be informed of the revocation from the block header information, it still can forge the validity of identity through the simplified payment verification (SPV) [7] method with the registered block i.

Moreover, to achieve the trust revocation function for lightweight node in the context of Blockchain-Enabled identity management for VANET system, this paper additionally presents a new authentication scheme. In the proposed scheme, the lightweight node can detect whether an identity is valid currently, with local blockchain query, thus realizing trusted and efficient authentication. Especially, unlike existing schemes, we realize the trustful revocation for lightweight-node verifiers by using the chameleon hash algorithm. The main contributions of our paper can be summarized as follows:

- We propose a Blockchain-Enabled Identity Management system for VANET, that leverages lightweight nodes. Thus, the authentication process relies on local certificate verification, which significantly increases the efficiency and security of authentication in VANET.
- We design a revocation protocol by implementing redactable blockchain with chameleon hash. This protocol enables lightweight nodes to be aware of historic block-redaction information, which to our best knowledge, has not been addressed by existing schemes.

II. Related work

Blockchain is an ideal technology to devise reliable and decentralized authentication solutions. Fromknecht *et al*. [8] proposed CertCoin, which ensures identity retention with the help of cryptocurrencies such as Bitcoin and Namecoin. Chen *et al*. [9] proposed a dependability-rank based consensus protocol in our blockchain system and a new data structure to support certificate forward traceability. Liu *et al*. [10] proposed a decentralized and traceable collaborative authentication mechanism by introducing the mechanism of secret sharing and dynamic proxy technology to blockchain. Zhuo *et al*. realized efficient and decentralized key management for VANETs, with an additional mechanism of public key registration, update and revocation in [11]. Xu *et al*. [12] leveraged the redactable blockchain to revoke illegal users without the CRL (certificate revocation list) method. Can *et al*. [13] presented BPAF, a blockchain-based authentication for vehicular fog devices, which achieves reliable and privacy-preserving authentication.

The idea of redactable blockchain solves the problem in blockchain that the illegal or invalid information (e.g., malicious user's identity registration) may be uploaded to the immutable ledger. In [14], Deuber *et al*. proposed a voting mechanism, where the redaction proposal reaches a consensus after generating threshold blocks for voting. In [15], Jia *et al*. proposed an online privacy-preserving on-chain certificate status query service, by using chameleon hash [16] to record the changes of blockchain. Luo *et al*. [17] utilized the redactable blockchain to record revocation information directly on the original certificate and removed additional data structures.

As can be seen, existing schemes cannot realize a lightweight node aware revocation mechanism, thus do not suit the VANET environment.

III. System Model

A. Architecture

As shown in Fig. 4, our system consists of 4 entities: consensus nodes, On Board Units (OBUs), Road Side Units (RSUs) and Certification Authorities (CA).

Blockchain Consensus nodes: They are full nodes from the perspective of blockchain data storage, and taking part in every-round consensus.

OBUs: refer to dynamically moving vehicles with limited storage capacity and real-time data interaction requirements, which need to verify each others' privilege or trust in communication. Especially, when the OBU is a verifier in authentication, it is a lightweight blockchain node.

RSUs: are fixed infrastructure components on roads for Internet connection by vehicles or data exchange. The RSUs in general are base stations placed at intersections of roads on places like petrol pumps and bus stops.

Certificate Authorities (CA):There are two types of CAs. iCA for cthe registration of the vehicle's and the RSU's

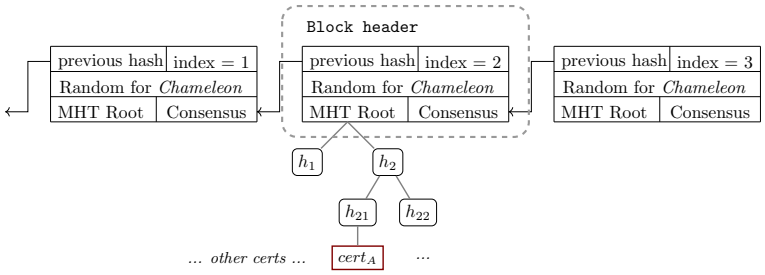

Fig. 2. Data Structure of Blockchain and Each Block Header in Proposed Scheme

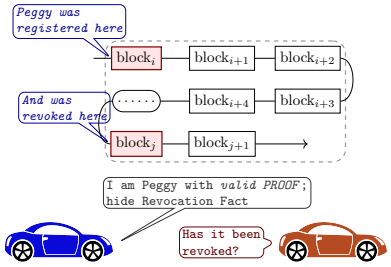

Fig. 3. Revocation Problem for Lightweight Node

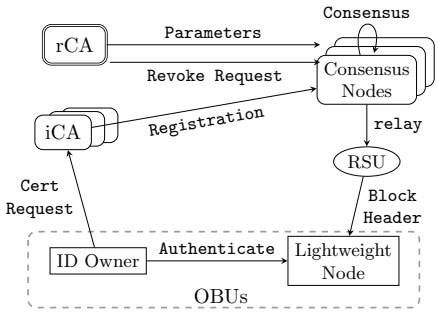

Fig. 4. Architecture

identity and rCA, a central root trusted authority, which is responsible for managing the whole system, providing the revocation privileges for other entities. In our model, there are multiple iCAs and one rCA.

B. Security Assumption and Requirements

In VANET system, the rCA is fully trusted. It securely preserves the secrecy of its secret parameters and honestly triggers the revocation process. The iCAs are also trusted if it has been registered to the system. The RSUs can be trusted if they are authorized by trusted iCAs. As deployed in public environment, they are likely to be compromised. But it is feasible to assume that: 1) if an RSU is verified, it will honestly deliver blockchain-related messages timely; 2) if a RSU is compromised, the CA should revoke its privilege in time.

IV. Proposed Scheme

A. Overview

The data structure of our scheme is shown as Fig. 2, in order to realize lightweight node-aware identity management. A blockchain is composed of a sequence of blocks, each of which consists of 5 necessary parameters:

- The index of a block increases one by one from the genesis block;
- $prev\_hash$ is the digest of the previous Block Header via the chameleon hash;
- Random field contains the random variable;
- MHT Root (denoted as R) is the hash of the Merkle tree root node, followed with a number of transactions;
- Consensus field differs according to the chosen consensus method.

Especially, let the pre-image of the hash of this block be

$$m = (index|pref\_hash|R), \tag{1}$$

B. Details of Our Proposed Scheme

1) Initialization phase: The rCA generates a cyclic group $\mathbb{G} =< g >$ of a large prime order p and a secure hash function $H : \{0,1\}^* \rightarrow \mathbb{Z}_p$. It selects a random trapdoor key $x \in \mathbb{Z}_p^*$ and publishes the public key $y = g^x$.

The Consensus nodes enter the system like general blockchain systems. After the blockchain system is set up, it begins to register the iCAs' identities with their attributes (e.g., government, car manufacturer, or other kinds of organizations) as transactions of the blockchain. The iCAs belonging to certain kinds have the right to register RSU's certificates to the blockchain.

2) Registration Phase: Each identity registration transaction is a certificate. A certificate is registered between the OBU (as a user), iCA and consensus nodes as follows.

Step 1. The user (denoted as U_j) locally generates a public-private key pair (pk_j, sk_j) locally and sends its ID and pk_j to the selected iCA as his/her identity registration request.

Step 2. If the request is not allowed, the iCA aborts the phase; otherwise, it packages registered identity and sends it to the blockchain system as a certificate transaction.

Step 3. The consensus nodes collect all registered certificates in the form of a Merkle tree, with the root value R_k, where k is the index of current block. A blockchain-wide consensus protocol is performed to determine random numbers

$r, s \in \mathbb{Z}_p$ in random field, and calculates a chameleon hash

$$h_k = CH.Hash(y, m_k; (r, s)) = r - H(y^{H(m_k,r)} g^s), \quad (2)$$

where $m_k = (k|h_{k-1}|R_k)$.

Step 4. When the new block is repackaged, the iCA returns a registration completion response to every user U_j, which contains the SPV auxiliary infromation AUX_j. At the same time, the RSUs will get the kth block and broadcast the header to all OBUs via their protected V2I channel.

3) Authentication Phase: An OBU U_j wants to authenticate to other OBU (denoted as U_r) as follows.

Step 1. delivers a message m_j to U_r. Followed by its certificate (refer to as $cert_j$, containing pk_j, U_j), block height k where the transaction is located, AUX_j, and a signature on m_j as $\sigma_j = Sig(m_j, sk_j)$.

Step 2. Upon the reception of the above delivery, U_r executes the following mechanism to check the validity of the source. It queries its local storage to retrieve R_k, and performs SPV with R_k, $cert_j$ and AUX_j. If so, verifies if σ_j is a valid signature of m_j with pk_j.

Especially, the RSUs periodically broadcast their validity of certificates as well as the public key in the blockchain.

4) Revocation Phase: **Step 1.** rCA locates the block index k containing the registration of $cert_j$, and returns h_k, deletes $cert_j$ from the tree, and recalculate new root R'_k, and of course a new m'_k. It runs $CH.Col$ by selecting random $k \in \mathbb{Z}_p$ and

$$\begin{aligned} r' &= h_k + H(g^k) \\ s' &= k - xH(m'_k, r') \end{aligned} \quad (3)$$

It informs the consensus nodes to redact the kth block with the revoked $cert_j$ and r', s'.

Step 2. Each consensus node checks the redaction information individually by running verify algorithm $CH.Ver$ as

$$h_k \stackrel{?}{=} r' - H(y^{H(m'_k,r')} g^{s'}), \quad (4)$$

where m'_k is generated as Step 1. If returns true, it notifies other consensus nodes an RSUs the new-version block k.

Step 3. After the RSU receives the redaction information, it checks the validity and broadcasts the header to the OBUs.

Step 4. The OBUs check the validity of redacted block header and replace the original kth header. If the OBU (denoted as U_i) is also registered in block k, it requests via RSU to retrieve its current auxiliary information AUX_i.

TABLE I
COMPARISON OF IDENTITY MANAGEMENT SCHEMES

Scheme	Revocable	Lightweight Node *Supp.*	Revocation Method
Fromknecht *et al.* [8]	✔	✗	Accumulator
Chen *et al.* [9]	✔	✗	Bloom Filter
Liu *et al.* [10]	✗	✔	\
Ma *et al.* [11]	✔	✗	Smart contract
Xu *et al.* [12]	✔	✗	Chameleon hash
Zhang *et al.* [13]	✔	✗	CRL
Our Scheme	✔	✔	Chameleon hash

V. SECURITY ANALYSIS

A. Trustful Revocation

Lightweight node is not convinced by the authentication from a revoked user in our scheme. Once a user is revoked, the MHT root value of its registered block is modified. Due to the semantic security of chameleon hash algorithm, only rCA (with trapdoor key x) can complete this modification to update the random variable of the relevant block header. The revoked user, whose certificate is no longer in the new-version block, cannot forge the supporting information for his/her illegal authentication. The redaction events can be notified to the OBUs trustfully via the RSUs' broadcast.

B. User Authentication Completeness

Legal OBUs can complete its authentication anytime and anywhere, even the relevant certificate is registered in a redacted block. As it is connected to a trust RSU during the relevant block header redaction broadcast, it can be notified immediately that it should update its auxiliary information. The supporting information update phase can be easily enforced by querying the connected RSU. Compared with the universe identity set of OBUs, the identities registered in one block is quite small .

C. DoS and Eclipse Attack Resist

Our identity management scheme for VANETs is robust against DoS and Eclipse attacks. Since the blockchain ledger is cached in the verification OBUs locally as a lightweight node. It cannot disable the verification capability of an OBU by isolating the OBU from honest consensus nodes.

VI. IMPLEMENTATION

We develop experiments in Python3.9 and measured on Raspberry Pi platforms. The cryptographic algorithm is implemented using with Charm-Crypto framework (with 192primev1 of eccurve). We compare our scheme with the following blockchain-based authentication schemes [8–13].

Table I shows the theoretical comparisons. We can find lightweight node-supporting is of great importance for highly dynamic VANET system, but it is a technical challenge to realize both revocation and lightweight node. As the lightweight node does not contain any transactions, it cannot check any kind of revocation notification, including CRL, smart contract processing. Even some schemes used chameleon hash, this challenge was not conquered, as the old-version SPV still work for revoked users. Luckily, our mechanism achieves lightweight node-aware revocation. This important property brings us significant advantage in authentication efficiency due to local certificate validity check. As shown in Table II, a lightweight node with 1GB storage capacity can store at most 8.7×10^6 blocks, which is a 250-year ledger.

TABLE II
OVERHEAD MEASUREMENTS ON OBU TESTED

Item	Measurement
Storage per block	0.12 kB
Storage for AUX	0.19 kB (256 IDs limit in block)
Throughput of Revocation	0.19 kB per user

We compare the revocation and verification time of our scheme with Certchain [9] and BPAF [13]. Fig. 5 shows the average time costs. Due to the fact that the compared schemes should access consensus nodes to retrieve locating and retrieving the revocation operation, their schemes should cost over 200 ms to verify an OBU's identity. As a comparison, the proposed scheme needs less than 8ms, which well satisfies the strict latency requirement for VANET.

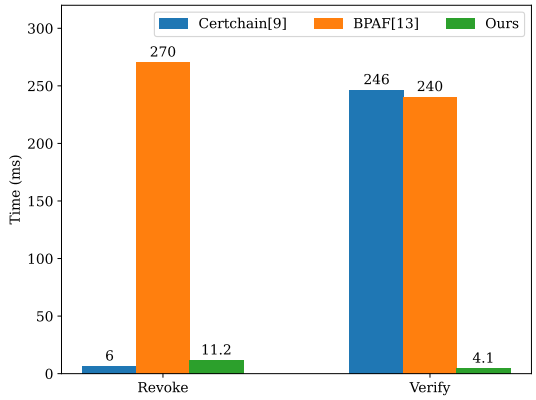

Fig. 5. Experimental Result of Executing Time

VII. CONCLUSION

This paper investigated problems of trustful revocation and low-latency blockchain query in VANET authentication, and proposed a novel blockchain-based efficient authentication scheme for such scenario. To satisfy the severe low latency requirement, lightweight node-based architecture is leveraged to let OBUs verify opponents' certificates locally. To deal with the challenge of trustful revocation for lightweight node verification, redactable blockchain-based revocation mechanism and the tailored network security protocol was proposed.

ACKNOWLEDGEMENT

This work was supported by National Key Research and Development Program of China (2022YFB2702300, 2023YFB2704903) and Natural Science Foundation of China (62202290).

REFERENCES

[1] A. Ghosal and M. Conti, "Security issues and challenges in V2X: A Survey," *Computer Networks*, vol. 169, p. 107093, Mar. 2020.
[2] R. Van Der Heijden, "Security architectures in V2V and V2I communication," in *Proc. 20th Student Conf. IT*, 2010, pp. 1–10.
[3] T.-T. Kuo, H.-E. Kim, and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications," *Journal of the American Medical Informatics Association*, vol. 24, no. 6, pp. 1211–1220, Nov. 2017.
[4] Y. Inedjaren, M. Maachaoui, B. Zeddini, and J.-P. Barbot, "Blockchain-based distributed management system for trust in VANET," *Vehicular Communications*, vol. 30, p. 100350, Aug. 2021.
[5] H. T. Cheng, H. Shan, and W. Zhuang, "Infotainment and road safety service support in vehicular networking: From a communication perspective," *Mechanical systems and signal processing*, vol. 25, no. 6, pp. 2020–2038, 2011.
[6] M. Y. Kubilay, M. S. Kiraz, and H. A. Mantar, "CertLedger: A new PKI model with Certificate Transparency based on blockchain," *Computers & Security*, vol. 85, pp. 333–352, 2019.
[7] "Bitcoinj," https://bitcoinj.org/.
[8] C. Fromknecht, D. Velicanu, and S. Yakoubov, "A decentralized public key infrastructure with identity retention," Cryptology ePrint Archive, Paper 2014/803, 2014.
[9] J. Chen, S. Yao, Q. Yuan, K. He, S. Ji, and R. Du, "Certchain: Public and efficient certificate audit based on blockchain for tls connections," in *Proceedings of the 2018-IEEE Conference on Computer Communications*. IEEE, 2018, pp. 2060–2068.
[10] H. Liu, P. Zhang, G. Pu, T. Yang, S. Maharjan, and Y. Zhang, "Blockchain Empowered Cooperative Authentication With Data Traceability in Vehicular Edge Computing," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 4, pp. 4221–4232, Apr. 2020.
[11] Z. Ma, J. Zhang, Y. Guo, Y. Liu, X. Liu, and W. He, "An Efficient Decentralized Key Management Mechanism for VANET With Blockchain," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 5836–5849, Jun. 2020.
[12] J. Xu, K. Xue, H. Tian, J. Hong, D. S. L. Wei, and P. Hong, "An Identity Management and Authentication Scheme Based on Redactable Blockchain for Mobile Networks," *IEEE Transactions on Vehicular Technology*, vol. 69, no. 6, pp. 6688–6698, Jun. 2020.
[13] C. Zhang, L. Zhu, and C. Xu, "BPAF: Blockchain-Enabled Reliable and Privacy-Preserving Authentication for Fog-Based IoT Devices," *IEEE Consumer Electronics Magazine*, vol. 11, no. 2, pp. 88–96, Mar. 2022.
[14] D. Deuber, B. Magri, and S. A. K. Thyagarajan, "Redactable Blockchain in the Permissionless Setting," in *Proceedings of the 2019 IEEE Symposium on Security and Privacy*, 2019, pp. 124–138.
[15] M. Jia, K. He, J. Chen, R. Du, W. Chen, Z. Tian, and S. Ji, "PROCESS: Privacy-Preserving On-Chain Certificate Status Service," in *Proceedings of the IEEE Conference on Computer Communications*, 2021, pp. 1–10.
[16] H. Krawczyk and T. Rabin, "Chameleon hashing and signatures," 1998.
[17] X. Luo, Z. Xu, K. Xue, Q. Jiang, R. Li, and D. Wei, "ScalaCert: Scalability-Oriented PKI with Redactable Consortium Blockchain Enabled "On-Cert" Certificate Revocation," in *Proceedings of the 42nd IEEE International Conference on Distributed Computing Systems (ICDCS)*, Jul. 2022, pp. 1236–1246.