CyberChain: Cybertwin Empowered Blockchain for Lightweight and Privacy-preserving Authentication in Internet of Vehicles

Haoye Chai, Supeng Leng*, Jianhua He, Ke Zhang, and Baoyi Cheng

***Abstract*—Internet of Vehicles (IoVs) presents promising opportunities for vehicle to everything (V2X) applications, wherein authentication acts as the cornerstone to realize trustworthy vehicular context and to support advanced applications. However, existing authentication schemes mainly depend on centralized servers with both security and privacy issues. In this paper, we propose a CyberTwin (CT) empowered blockchain framework for authentication, namely CyberChain, to reduce both the communication and storage cost while maintaining vehicular privacy. By designing a blockchain system in the cyberspace, we decouple the consensus process from the physical world, so that the operation cost of blockchain can be reduced. A Privacy-Preserving Parallel Pedersen Commitment (P4C) algorithm is designed to protect the privacy of vehicles and accelerate the authentication process. To further enhance the operation efficiency of CyberChain, we propose a Diffused Practical Byzantine Fault Tolerance (DPBFT) mechanism to reach consensus in the cyberspace that can reduce consensus latency. The proposed cyberchain framework and the associated mechanisms are evaluated by qualitative analysis and simulations. The evaluation results demonstrated that the proposed cyberchain based framework significantly improves the authentication performance in terms of authentication latency, privacy, communication overhead and storage cost.**

***Index Terms*—CyberTwin, Blockchain, Authentication, Internet of Vehicles, 6G.**

I. Introduction

With the development of Vehicle-to-Everything (V2X) technology, Internet-of-Vehicles (IoVs) shows great potentials for advanced vehicular applications among interconnected vehicles and traffic infrastructures, aiming to provide convenient and safe driving experiences. The advanced V2X applications require not only ultra reliability and low latency, but also extremely high security and trust to support communication and cooperation among vehicles. However, due to the openness of wireless communication, malicious entities can eavesdrop, intercept and even tamper the messages to steal private information or make chaotic traffic [1]. In this case, authentication is crucial for IoVs against potential attacks.

Existing research efforts have been dedicated to designing authentication schemes for IoVs, such as public key infrastructure (PKI) based schemes for digital signatures and certificate revocation list (CRL) [2]. However, existing schemes are mainly centralized and using third parties, such as certificate authority (CA) or key generation center (KGC). Threatened by distributed denial of service (DDoS) and single point of failure attacks, vehicles are unwilling to store their private information on the servers with privacy concerns. Recent interest has been dedicated to decentralized authentication [3], [4]. While the schemes require vehicles and traffic infrastructures to fully trust with each other and cooperate to obtain identity tokens that are impractical in large scale IoVs. Moreover, with the high mobility of vehicles, there can be frequent identity registration and re-authentication as well as the query of CRL across multiple traffic regions, which poses severe burden to communication links.

As a key enabling technology for 6G, blockchain holds great potentials for authentication in decentralized networks. Federal Communications Commission (FCC) has envisioned blockchain as the next revolution in 6G that facilitates flexible and trustworthy distributed management [5]. By integrating smart contract, cryptography and consensus technologies, blockchain serves as a reliable and trustworthy decentralized platform. Blockchain can authenticate a legal user with a hash function based account instead of identity tokens, so as to eliminate the CRL query and re-authentication processes. It enables users to autonomously manage their private data, meanwhile to trace and verify other behaviours with trust that can provide great advantages for identity authentication.

Nevertheless, the outstanding security performance and decentralization of blockchain come at the cost of excessive computing, communication and storage resources. On the one hand, existing blockchains applied in IoVs rely heavily on mutual communication among vehicles and traffic infrastructures (such as roadside units, RSUs), wherein the consensus requires multiple rounds of communication via Physical-to-Physical Communications (P2PC) [6], [7]. While in highly dynamic IoVs, authentication process should remain lightweight, so that vehicles can quickly access to the network and conduct time-sensitive applications [8]. On the other hand, because of the large-scale access and high mobility patterns, vehicles tend to have massive cross-region behaviours that introduce frequent identity handover and re-authentication processes. Since blockchain requires each node to cache a complete

This work was supported in part by the National Key Research and Development Program of China under Grant 2018YFE0117500, the National Natural Science Foundation of China under Grant 62071092, the Key Lab of Information Network Security, Ministry of Public Security under Grant C19603, and the European Union's Horizon 2020 research and innovation programme under the Marie Skłodowska-Curie grant agreement No. 101022280.

H. Chai, S. Leng, K. Zhang, and B. Cheng are with the School of Information and Communication Engineering, University of Electronic Science and Technology of China (UESTC), Chengdu, 611731, China, and the Shenzhen Institute for Advanced Study, UESTC, Shenzhen, 518000, China.

J. He is with the School of Computer Science and Electronic Engineering, University of Essex, Colchester, CO4 3SQ, UK (e-mail: j.he@essex.ac.uk).

* Corresponding author, email: spleng@uestc.edu.cn.

ledger, frequent handover of vehicles will exacerbate the synchronization overhead of ledger update, thereby hindering the scalability of blokchain and the efficiency of authentication.

To tackle the challenges faced by blockchain, another emerging technology, CyberTwin (CT), can be exploited for authentication in IoVs. By constructing digital replicas, CTs can map physical entities into the cyberspace in terms of status, features, and actions. In this case, the conventional P2PC can be simulated by the Virtual-to-Virtual Communications (V2VC) in the cyberspace that is jointly provided by the edge and core networks [9]. More importantly, the cyberspace stores mapping relationship that is not restricted by geographical locations. The relationship can be dynamically managed, which shows great potentials for mobility management in IoVs [10], [11]. However, the integration of cybertwin and blockchain is an unexplored problem. Especially in the large scale and highly dynamic IoVs, it should be urgently resolved for constructing and modeling CTs in blockchain as well as migrating CTs among different blockchain systems.

To address the issues above, we are motivated to combine both blockchain and CT technologies. In this article, we propose a cybertwin-empowered blockchain, namely, CyberChain (CC) for authentication in IoVs. The handover is taken place in the physical world, while the authentication process is conducted by consensus in the cyberspace. The CC not only utilizes blockchain to ensure security and privacy during the authentication process, but also exploits CT to reduce consensus latency and storage consumption. The main contributions of the paper are summarized as follows.

- A new CyberChain (CC) framework is proposed for authentication in highly dynamic IoVs. The CC constructs the blockchain system in the cyberspace, wherein the transaction, processing and consensus process can be migrated in the virtual world. The proposed framework enables decentralized and secure handover, meanwhile maintaining fast and lightweight with the aid of CT technology. To the best of our knowledge, it is the first time to construct a blockchain system in the cyberspace for vehicular authentication.
- In order to preserve vehicular privacy in the dynamic context, a Privacy-Preserving Parallel Pedersen Commitment (P4C) algorithm is developed for authentication without the secret opening procedure, so that verifiers achieve authentication via zero-knowledge proof. To cater for the high mobility of vehicles, we propose a lightweight cyber-consensus mechanism named Diffused Practical Byzantine Fault Tolerance (DPBFT), so as to accelerate authentication process. Facilitated by the reliable virtual communication of CT, the authentication of vehicles can be fast completed within a small range that is suitable for the time-sensitive IoVs.
- The communication and security performances are analyzed. Several potential attacks are discussed to verify the superior security performance of the proposed framework. It is the first time to explore the relationship between communication overhead and security performance of blockchain in the cyberspace. The analysis shows the proposed framework can make a good tradeoff between communication efficiency and security by integrating CT into blockchain, which can guide the design of the CT based blockchain systems.

The remainder of this paper is organized as follows. We review the related work of identity authentication schemes in IoVs. The cyberchain based vehicular authentication framework is presented in Section III. In Section IV, the P4C and the DPBFT algorithms are described in detail, followed by the communication and security analysis in Section V. In Section VI, the simulation results are presented. Finally, the paper is concluded in Section VII.

II. Related Work

The Authentication in IoVs has been widely studied. Typically, there are three types of authentication schemes: the certification based schemes, the password pair based schemes and the biosignature based schemes [12]-[15].

For the certification based authentication, Lv *et al* propose a homomorphic encryption based V2I authentication scheme with the help of the certification authority, aiming to realize fast and privacy-preserving authentication in highly IoVs [12]. A fog-based identity authentication scheme is proposed, wherein a PKI server and proxy vehicles authenticate the new vehicle members [13]. For the password pair based scheme, a group-key generation and a password based protocol is presented for VANETs [14]. For biosignature based scheme, the fingerprint and behavioral biometrics of drivers are designed for authentication[15]. While the above work depends on a centralized trusted authority (PKI or CA), due to the large scale of IoVs, the centralized authentication will aggravate the burden of core network. Moreover, there exists the risk of privacy leakage due to the single point of failure.

Emerging as a decentralized, trust, and privacy-preserving technology, blockchain has attracted widespread attention for authentication in IoVs. Wang *et al* propose a blockchain assisted authentication framework to achieve fast re-authentication of vehicles between infrastructures [16]. A smart contract is designed to realize the automatic authentication and conditional privacy in VANETs, without any online registration center [17]. The blockchain is designed as a decentralized and tamper-proof server to achieve automatic key management, realizing mutual authentication, key agreement, update and revocation [18]. However, most of existing work cannot resolve the severe communication overhead and storage cost introduced by consensus and ledger synchronization of blockchain. In the highly dynamic and large scale vehicular scenarios, it will greatly degrade the authentication efficiency.

As a promising technology of virtualization, CT constructs digital replicas for vehicles in the cyberspace. A cybertwin based approach that utilizes vehicle-to-cloud communication is proposed to realize cooperative ramp merging [19]. By monitoring the operation state of physical vehicles, several cybertwin-assisted schemes are proposed by combining computation capability and traffic data, so as to realize service offloading and traffic prediction [20], [21]. Utilizing the virtual communication, CT can simulate the communication behaviours of vehicles, and give real-time feedback to the physical world. In this case, we are motivated to integrate CT with blockchain for vehicular authentication. However,

due to the highly dynamic and large scale of IoVs, frequent association and mapping of CT exacerbate the maintenance cost of both conventional public-chain and consortium-chain. To guarantee the efficiency of CT based blockchain, a new framework should be developed that facilitates the handover of vehicles and the migration of blockchain in IoVs.

III. CyberChain Based Vehicular Authentication Framework

Facilitated by the ubiquitous V2X communication and AI on-board modules, IoV is envisioned to fully support the advanced vehicular applications and intelligent traffic services among smart vehicles and traffic infrastructures. Due to their high mobility, vehicles will have frequent cross-region behaviours, and migrate from one traffic region to another. In this case, vehicles should have legal identities in each new region, so that they can interact with others with trustworthy.

In this section, the CyberChain based framework for authentication in IoV is proposed. We leverage both the cybertwin and blockchain technologies to build a secure and lightweight authentication framework for IoV.

A. System Overview

The proposed CC based framework is illustrated in Fig. 1. The framework is logically divided into two spaces: physical world and virtual world.

Physical World: The space comprises of all the physical entities including vehicles and edge servers (ESs). According to the geographical location of the traffic network, the whole traffic network can be divided into multiple regions (like region A and B in the figure). Within one traffic region, there are multiple ESs that operate several CTs for vehicles. Moreover, the ESs in each traffic region also maintains an exclusive private CC, responsible for authenticating and managing vehicular identities within their communication range.

Virtual World: The virtual world refers to the digital replicas of all the entities in physical world. The basic unit of the virtual world is cybertwin (CT), including the CTs of vehicles and the CTs of ESs. Based on the basic unit, there are three digital objects in the virtual world:

1). Sub-CyberSpace (SCS): The SCS refers to the virtual space that is constructed by one ES. Since one ES can simultaneously operate multiple CTs for vehicles, one SCS is composed of: a). the CTs of vehicles located within the ES communication range; b). the CT of the ES itself.

2). CyberSpace (CS): Recalling the whole traffic network is divided into multiple regions, there will be several ESs within each region. In this case, the CS is an integrated space with multiple SCSs, that is to say, the CS is the virtual space that is constructed by all the ESs within one region (as CS A of region A and CS B of region B in Fig. 1).

3). CyberChain (CC) The CC is a digital blockchain defined in the virtual space. The nodes of CC are the CTs of vehicles and ESs. In our proposed framework, we develop a private-consortium structure for CC. Specifically, there is one private CC in each CS, wherein the CC maintains an exclusive ledger that records the identity information and interaction processes (such as data sharing and cooperative computing). Within one CC, the nodes in each SCS constitute a small-scale consortium. Compared with conventional blockchain, the proposed private-consortium structure shows advantages on the identity handover and lightweight consensus that will be elaborate in section. IV. B. In general, one CC only needs to record the information within its region, and it does not need to interact with CCs in other regions. Only when the vehicle requests the identity handover process, the CC needs to provide the information with the CCs in other regions.

In the proposed CC based framework, there is a two-way interaction between the physical world and the virtual world. As illustrated in Fig. 1, vehicles upload the modeling of CTs to the virtual world, then the cyberchain updates its operation state and feedback the update to the physical world.

(a). Modeling of Cybertwin: vehicles send their identity information and interaction records to corresponding CTs in the form of cybertwin modeling, which can be expressed as

$$CT = \{Atr, Act, sig\}, \tag{1}$$

where Atr represents the private attributes during the vehicular interactions, such as reputation or assets. Act is the interaction type, and sig is the digital signature of vehicles. Then, the CTs will encapsulate the updating logs to cyber-transactions, and broadcast the transactions for consensus. The general format of cyber-transaction is

$$Ctx = \{CT, Adr, sig, t_s\}, \tag{2}$$

where Adr represents the set of address that includes the addresses of both senders and receivers. t_s is the timestamp of the transaction, proving the unique existence of the transaction at the current moment.

(b). Update of Cyberchain state: After the consensus process in the cyberspace, the operation state of CC is changed, including the ledger state (such as block height, number of CC users, etc.) and account asset of CTs (such as the updated reputation value and current account balance). Afterwards, the update is sent back to the physical world. Vehicle can utilize the updated information to perform different operations. Take the authentication scenario as an example, when one vehicle tends to migrate from one region to another, the interaction history in the old CC ledger can be referred to by the new region as the criterion of the authentication process.

Linking Physical and Virtual World: In our proposed framework, the edge servers (ESs) are designed as the link bridge between the physical world and virtual world:

1). Vehicle in the physical world will first choose one ES within its communication range and construct its CT in the virtual world. The CTs are operated and located on the ESs.

2). Due to the strong computation capability, one ES can simultaneously operate CTs for multiple vehicles. In other words, ESs are the physical carriers of SCSs that are the main advantages of the proposed CC. Compared with traditional blockchain depending on the physical communication, the communication within SCS mainly relies on virtual communication between CTs and is not restricted by physical channel constraint. For example, one ES can creates multiple threads for the CTs, and the communication among the CTs can be accomplished by the interprocess communication (IPC) process, thus greatly reducing the communication delay.

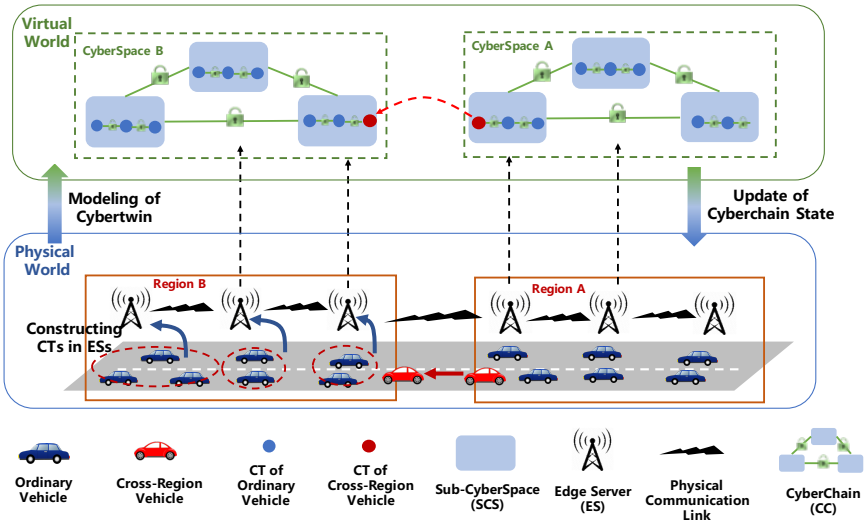


Fig. 1: CyberChain Based Authentication Framework

3). By utilizing the storage capability of ESs, the CC ledger is cached on the ESs in the virtual world. Vehicles in the physical world have no need to cache the ledger.

Identity Handover of Vehicles: Due to the high mobility of vehicles, there exists frequent identity handover processes. Typically, there are two types of identity handover processes in our framework: ***1). Identity handover between two SCSs*** and ***2). Identity handover between two CSs***.

For the first type of handover, since the handover process between different SCSs takes place inside the same CS, the corresponding blockchain identity of the vehicle in the CC will keep unchanged before and after the handover (as the blockchain address will not change). In other words, the identity of the vehicle remains legal during the handover process. Essentially, the CTs of nodes are the addresses in our cyberchain system. All the logs of CTs are recorded in the blockchain ledger in the form of transactions. Therefore, within the same blockchain system, the process of rebuilding CT is to reactivate the blockchain account. Therefore, the handover node only needs to utilize its private key to authorize ES to reactivate the account, so as to rebuild its CT. Based on the local ledger, the ES can rebuild the account of handover node, rather than requesting ledger information from other ESs, thus reducing communication overhead. In the proposed framework, we utilize the cyber-transaction to resolve the handover between different SCSs. We define a special transaction TX_{csv} for the cross-SCS vehicles (CSVs), which can be expressed as

$$TX_{csv} = \{CT : (s_{adr}, Act = cs)||Adr = d_{adr}||sig||t_s\}, \quad (3)$$

where s_{adr} is the original SCS id of CSV and Act denotes the cross-SCS behaviour. Then, TX_{csv} will be sent to the new SCS for consensus. After the consensus, the transaction is valid within the CC, and the ES in original SCS will migrate the CT of CSV to the new ES, and the handover is completed.

However, for the second type of handover, the whole process involves the authentication of the identity information of the cross-region vehicles (CRVs) and the address conversion between two private CCs. In this case, the handover cannot be solved like the first type. Next, we focus on the second handover problem that will be elaborated in the next subsection.

B. Identity Handover Between Two CSs

The ultimate goal of the type of handover is to determine whether the cross-region vehicle (CRV) has a legal identity in the original region. After the CRV arrives in a new region, if the Atr it provides to the new region is consistent with the newest Atr recorded in the original region, the CRV can be deemed as honest and legal.

The proposed framework utilizes consensus to realize authentication without introducing extra identity-based token [22]. The consensus process requires every blockchain node to reach the same view of the entire network. Hence, the identity information of CRVs can also be spread and verified by the consensus, thereby completing the authentication process. Following the example depicted in Fig. 1, we will give the specific workflow of the cyberchain based authentication process.

(1). Invoking Handover Contract: When the CRV tends to leave region A and drive to B, it first sends a special transaction TX_{CRV} to the original cyberspace to invoke the smart contract $HandOver$. The $HandOver$ will generate a set of blind factors $\mathcal{B}$ for authentication that will be elaborated in section. V. The format of TX_{CRV} is expressed as

$$TX_{CRV} = \{CT : (s_{adr}, d_{adr}, Act = ho)||Adr = HO||sig||t_s\}, \quad (4)$$

where s_{adr} and d_{adr} is the region id of current region and the destination region, the Act represents the cross-region handover and the term HO indicates the CC address of smart contract $HandOver$.

(2). Sending Identity Commitment: After invoking $HandOver$, the CRV can drive to region B for authentication. The CRV first starts a session with one of the ESs ES_{new} in region B. Then, the CRV will send a special message identity commitment ic to ES_{new} to prove its legality, that is

$$ic = Encrypt(Atr), \quad (5)$$

where $Encrypt()$ function encrypts the private Atr into ciphertext to protect privacy. The message ic indicates that the CRV does have the declared Atr in region A.

(3). Sending Identity Proof: Meanwhile, the blind factors $\mathcal{B}$ generated by $HandOver$ are returned to ES_V. ES_V is where the CRV constructs its CT on in region A. ES_V generates the identity proof ip and sends it to the destination d_{adr}in region B, the general format of ip is

$$ip = Encrypt(Atr, \mathcal{B}). \tag{6}$$

Note that step (2) and (3) are implemented in parallel.

(4). Generating Identity Transaction: After receiving both ip and ic from CRV and ES_V respectively, ES_{new} acts as a temporary CC node to issue a special transactions, identity transaction TX_{it},which can be expressed as

$$TX_{it} = \{CT : (ip, ic, Act = authen)||Adr||sig||t_s\}, \tag{7}$$

where CT term indicates the transaction is issued by ES_{new}, and the Act represents the transaction is issued for authentication. It should be noted that ES_{new} can only temporarily issue TX_{it} when during the authentication process. It does not have the right to participate in the interaction process, nor the right to participate in the consensus process, thus the entire CC system is still a distributed system. The temporarily issuing mechanism is inspired by *milestone* in [23].

(5). Completing Authentication by Consensus: ES_{new} broadcast the TX_{it} for consensus. Each CT in CS B verify the TX_{it} by checking the value Atr of both ic and ip. If the two values are equal, the TX_{it} is regarded as valid, otherwise the verification failed. When more than half of the CTs in the cyberspace B have passed the verification of TX_{it}, the consensus is reached. At this moment, the authentication of the CRV is completed.

C. Advantages of the CyberChain in Authentication

By constructing replicas of physical nodes in the cyberspace (i.e. CTs), CTs can simulate the communication, calculation and processing behaviours of physical nodes, so that the CTs can obtain the same operating results as those of physical nodes. In this case, the publishing of transactions, verification and consensus processes in traditional blockchain can be carried out in the cyberspace, thereby reducing the number of interactions in the physical world and improving the efficiency of the blockchain system. There are three unique features of the proposed cyberchain compared with traditional blockchain.

1). Reduction of physical-to-physical communications. By introducing CTs in blockchain, both CRVs and OVs will upload their states and attributes to the corresponding CTs. Then, the generation and broadcast of transactions are executed by CTs in the cyberspace, instead of in the physical world. For the authentication process, both the invocation transaction TX_{CRV} and identity TX_{it} are not transmitted through the vehicle entities, but broadcast in cyberspace using CTs. Facilitated by the V2VC, such as inter-process communication that is not restricted by the actual physical channel, the corresponding CTs can realize fast and reliable communication with other CTs in cyberspace, thereby greatly reducing the authentication delay.

2). Decoupling consensus process from physical entities. In traditional blockchain based consensus, most of the packaging and block broadcast processes depend on computation power and communication capability of blockchain nodes, *i.e.*, vehicles. In the highly dynamic IoV, this will cause serious efficiency issues of the blockchain system. Due to the intermittent vehicular link and unstable connection, the consensus in traditional blockchain suffers from packet loss and high deliver delay, while in the proposed cyberchain, the consensus of transactions is based on V2VC, as discussed above, thus it can realize fast identity authentication.

3.) Distributed transactions but centralized storage. In the proposed CC, the CTs are responsible for generating transactions, while CTs are essentially virtual nodes and have no storage capacity, thus the ledger of CC is cached in the corresponding ESs. In this case, multiple CTs share the same ledger that is cached on the ESs. Meanwhile, the ledger can only be accessed through the private key of vehicles and ESs, as mentioned in Eq. (1), and the ESs cannot modify the ledger without consensus process. Therefore, the proposed cyberchain is still essentially a distributed system. This distributed transaction but centralized storage feature greatly reduces storage overhead while ensuring scalability of the proposed CC.

IV. Privacy-preserving Contract and Lightweight Cyber-Consensus for Vehicular Authentication

Though the proposed CC reduce the authentication delay through the virtual communication, there are still several privacy- and efficiency-related issues to be tackled in IoVs. On the one hand, due to the high mobility of vehicles, the members of one region often change [24]. Hence, the entire network environment is untrusted,and there exists the risk of privacy leakage. For example, the malicious vehicles can capture the ic and ip message and analyze the attribute of CRVs to obtain their privacy. On the other hand, the conventional consensus mechanisms such as proof-of-work and PBFT that depend on huge computation or frequently broadcast show inefficiency during the proposed authentication process.

Consequently, to address the issues above, we propose a Privacy-Preserving Parallel Pedersen Commitment (P4C) Algorithm for the $HandOver$ contract, combining both zero-knowledge proof and pedersen commitment. Then, to cater for the delay-sensitive IoVs, a diffused practical byzantine fault tolerance (DPBFT) is designed for realizing fast consensus in a small traffic range, afterwards reaching a gradual consensus on the whole network. For the convenience of readers, Table I presents the main variables adopted in this article.

A. Preliminaries

In order to better describe the proposed authentication scheme, some preliminaries are presented here.

1) Bilinear Pairing and Elliptic Curve Discrete Logarithm Problem (ECDLP): Let G_1 be the cyclic group with the prime order q and g is the generator of G_1, $g \in G_1$. The Bilinear Pairing is a mapping relationship $\Pi(G_1 \times G_1) \rightarrow G_2$ on G_1 and G_2. The mapping holds three unique features: *Bilinearity* where for all $h, g \in G_1$ and $a, b \in Z_q$, $\Pi(h^a, g^b) = \Pi(h, g)^{ab}$. *Non-degeneracy* where $\Pi(g, g)$ is a generator of G_2 if g is a

TABLE I: VARIABLE TABLE

Variable	Definition
CS, SCS	CyberSpace and Sub-CyberSpace
ES	Edge Server
M	Number of SCS
n_m	Number of CTs in SCS_m
ξ	Least number of CTs in one ES
f_1	Total number of Malicious CTs
f_2	Number of ESs that suffer from single-point of failure
G, H	Elliptic Curve Point with length σ_2
y, r, e, s	Blind Factors with length σ_1
m	Original Secret
C_p	Time Consumption of Generating G
C_h, C_c	Time Consumption of Generating a hash value and a random number
C_c	Time Consumption of Elliptic Curve Pairing
C_v	Time Consumption of Verification

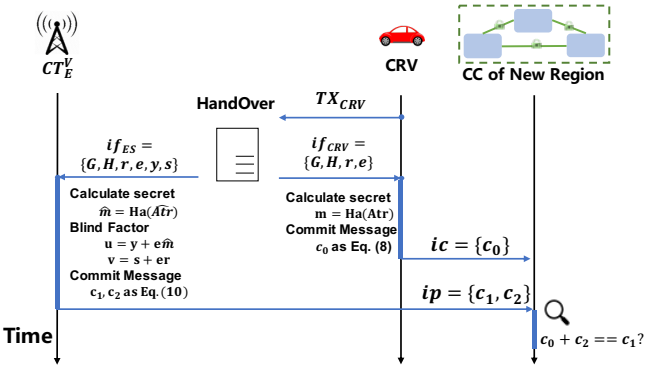


Fig. 2: Privacy-preserving Authentication Process

generator of G_1. *Computable* Π can be efficiently computed. Given the elliptic curve based multiplicative group $\mathcal{G}$, let two point G, H be in $\mathcal{G}$. The Elliptic Curve Discrete Logarithm Problem (ECDLP) is to find a number k that $Gk = H$.

2) Elliptic Curve Pederson Commitment (ECPC): Elliptic Curve Pedersen Commitment [25] is an unconditionally hiding and computationally binding scheme that uses secure Elliptic Curve Cryptography (ECC) technology and the intractability of ECDLP, showing perfect privacy-preserving capability. Typically, there are two types of ECPC: the one is non-privacy-preserving ECPC (NPPPC) [26], the other one is zero-knowledge proof ECPC (zkPC) [27]. The general workflow of the two schemes can be described as the three steps: (1). Setup stage. The stage generates the elliptic curve point G, H. (2). Commit Stage. The stage generate the encrypted message c with secret factor r. (3). Open Stage. In NPPPC, the open stage will reveal the r to the verifier to prove its commitment. In zkPC, the verifier will first send a challenge factor e to the prover, then the prover will recalculate a new encrypted message $c1$ with e, and send back to the verifier.

Motivation: However, it is inappropriate to directly utilizing the two schemes in our CC based authentication framework. First, the NPPPC directly exposes the security message (that is the private attribute Atr in our scenario) to the verifier. Under the untrusted vehicular scenario, it will introduce serious privacy issues. Secondly, the zkPC enforces the verifiers (the ES_{new} and CTs in the new region) to send the challenge factor e to the prover (the CRV), then it also requires the CRV to send a new commitment back to the verifiers. The whole process consists multiple round of communications between prover and verifiers, which is impractical in the blockchain based system. In this case, we are motivated to develop a privacy-preserving and communication-efficient scheme to realize the authentication process.

B. Privacy Preserving Parallel Pedersen Commitment (P4C) Algorithm for HandOver Contract

The core idea of the proposed P4C algorithm is to eliminate the open stage and to support parallel verification, so that the authentication achieves privacy-preserving and communication performance. The basic workflow is described as follows:

(1). Setup: Suppose the attribute of the CRV that The step is executed in the smart contract $HandOver$. Invoked by the TX_{CRV}, $HandOver$ randomly generates a group of elliptic curve points $\mathcal{G}_p$ with a large prime p, then the contract randomly choose two generator points $G, H \in \mathcal{G}_p$ and a randomly generated secret key q so that $H = qG$ that satisfies CDH condition. Besides, three blind factors r, y, s are also generated by the $HandOver$, together with a challenge factor e. After the generation process, the G, H, y, s, r, e is returned back to ES_V, and G, H, r, e is sent to the CRV.

(2). Parallel Commit: Upon receiving the output from $HandOver$, both the CRV and the ES_V start to calculate the commit message to prove the legality of the CRV. Specifically, for the CRV: it first utilize Hash function $Ha()$ to encrypt its Atr term as secret m, $i.e.$ $m = Ha(Atr)$,then the identity commit ic that integrates commit message c_0 is computed as

$$ic = \{c_0\} = (mG + rH)e. \tag{8}$$

For ES_V, it first computes $\hat{m} = Ha(\hat{A}tr)$. Compared with m sent by the CRV, $\hat{m}$ is the actual recorded attributes in the ledger, whereas m is the declared attributes by the CRV. When the CRV is honest, $m = \hat{m}$. Then the CT_E^V computes

$$u = y + em, \quad v = s + er. \tag{9}$$

Subsequently, the identity proof ip that contains blind commit messages c_1 and c_2 are calculated as

$$ip = \{c_1 = uG + vH, c_2 = yG + sH\} \tag{10}$$

(3). Non-opening Verification: After calculating c_0, c_1 and c_2, the CRV and ES_V send the messages to the destination d_{adr} in TX_{CRV} for consensus. The CTs in the new region only need to verify

$$c_0 + c_2 == c_1, \tag{11}$$

where " == " represents judgement operation. If the equation above holds, the CRV is deemed as honest, else the nodes in the new region have a reason to believe the CRV sends a faulty attribute and reject the authentication process.

During the authentication process, it can be observed that the attribute can be verified by c_0, c_1 and c_2, without the open process in conventional pedersen commitment schemes that reveals m and r, showing great privacy-performance. Moreover, compared with existing ZKP based pedersen commitment schemes, the proposed scheme enables the parallel sending of commit message. The attribute can be authenticated by performing only one round of communication, thus the pro-

Algorithm 1: Contract HandOver

Function HandOver(TX_{CRV}){
Check sig of TX_{CRV}
Obtain the destination d from TX_{CRV}
Generate G, H, y, r, s, e as the step of $Steup$
Generate Identity factors for the CRV
if_{CRV}={G, H, r, e}
Generate Identity factors for the ES_V
if_{ES_V}={G, H, r, e, y, s}
Return if_{CRV} and if_{ES_V} }

posed scheme is also communication-efficiency. The specific interaction is depicted in Fig. 2, and the detailed format of contract $HandOver$ is also concluded in Algorithm 1.

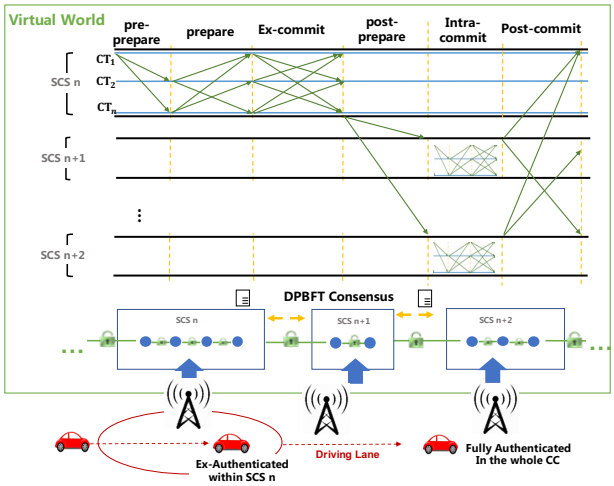


Fig. 3: The proposed Diffused PBFT Consensus

C. Diffused Practical Byzantine Fault Tolerance

Traditional consensus mechanisms such as PoS or PBFT regard the new transactions (or block) as valid only if the entire network achieves a unified ledger view, which will introduce an intolerable consensus delay under the large scale vehicular networks. In practical, due to the wide communication range of ESs, we notice that the CRV cannot drive across multiple ESs in a very short time period. Following this viewpoint, the consensus process can firstly be executed in a small range around the CRV, so that the CRV can be quickly authenticated within its current small range. Hence, we are motivated to develop a lightweight consensus mechanism, namely diffused Practical Byzantine Fault Tolerance (DPBFT), aiming to accelerate the authentication process. The DPBFT process contains six steps, as shown in Fig. 3.

Pre-prepare and Prepare: The two processes are similar with that of conventional PBFT. The CT of ES_{new} broadcast identity transaction TX_{it} with other CTs in all the SCSs. Upon receiving TX_{it}, the CTs in the SCS first check its integrity and validity. After verify the equation in Eq. (11), the CTs will broadcast the PREPARE message with other CTs in SCS_n.

Ex-commit: Unlike conventional PBFT, after receiving more than $2f_i + 1$ (f_i is the maximum number of fault-tolerant CTs in SCS_n) PREPARE messages from other CTs, the CTs will broadcast EX-COMMIT with others instead of commit. The EX-COMMIT indicates that TX_{it} is verified by the CTs in local SCS, that is to say, the consensus is achieved within a small range. After the EX-COMMIT process, the CRV is deemed as authenticated in the SCS_n, now it can interact with other CTs and issue the transactions within the SCS_n.

Post-prepare and Intra-commit By collecting $2f_i + 1$ EX-COMMIT messages from CTs in SCC_n, the local view of the ledger is updated. At this moment, the ES_n sent the "ex-authenticated" transaction TX_{it} to other SCCs for further consensus. Similar with the pre-prepare, prepare and ex-commit processes, all other SCCs implement the consensus in their own range to reach the ex-commit stage, then they broadcast the EXCOMMIT messages back to other SCCs.

Post-commit Upon collecting $2f' + 1$ (f' is the maximum number of fault-tolerant ESs) EXCOMMIT messages from the whole CS, TX_{it} is deemed as valid and legitimate, then the view of all the SCSs reach consensus. Until now the CRV is fully authenticated and it can interact with all the CTs in CS.

There are two main advantages of the proposed diffused PBFT (DPBFT) in comparison with the conventional PBFT based algorithms. Firstly, it can reduce the communication overhead. The proposed DPBFT decomposes traditional PBFT into multiple "sub-consensus areas", i.e., SCSs in our paper. Within each SCS, CTs will firstly reach a primary consensus in a relatively small range, then the primary consensus result is sent to the whole network for further consensus. Since the primary consensus can be implemented in parallel, large-scale communication process can be replaced by multiple small-scale communication processes, thus reducing the communication overhead. Secondly, by utilizing the DPBFT, the authentication process shows a trend of diffusion. In other words, the CRV is first authenticated in the region that is closest to it, then it is gradually authenticated by other regions. In this case, after the CRV has completed the consensus in a small region, it can directly interact with the surrounding CTs as a legal identity without waiting for the consensus result of other nodes in the entire network. Therefore, the proposed DPBFT can greatly shorten the authentication delay and improve the system efficiency.

V. Communication and Security Analysis

In this section, we analyze the proposed P4C algorithm and the DPBFT mechanism. Specifically, the communication and security performance of the proposed DPBFT are analyzed in terms of communication overhead and tolerant bound of single point of failure attack. Then, the authentication latency of the P4C algorithm is calculated, followed by the security analysis of potential malicious attacks.

A. Analysis of the DPBFT Consensus

Suppose the CTs constructed by vehicles distributively locate on total M SCS in the CC. Let $\mathcal{M} = \{1, ..., m, ...M\}$ denote the set of ESs, and n_m denotes the number of CTs in SCS_m that satisfies $\sum_m n_m = N$. In order to ensure the balance

of the CT construction, we assume that there must be at least ξ CTs within one ES, that yields

$$n_m \geq \xi, \quad \forall m \in \mathcal{M} \tag{12}$$

1) Communication Overhead: As indicated in Section IV. C, the consensus is implemented in parallel by CTs in different SCSs, hence, the total signaling cost can be computes as the sum of intra-interactions within each SCS and the interactions among the SCCs, that is

$$\begin{aligned} c &= \sum_{m=1}^{M}[(n_m-1)+(n_m-1)^2+n_m(n_m-1)] \\ &+ (M-1)+(M-1)^2 = 2\sum_{m=1}^{M} n_m(n_m-1)+M(M-1) \\ &\geq 2M\xi(\xi-1)+M(M-1). \end{aligned} \tag{13}$$

2) Security Analysis of Single-point of Failure: Considering a non-trust scenario where there are total f_1 malicious CTs among all CTs, and f_2 ESs that suffer from the single-point of failure (spf-ESs). Both the malicious CTs and spf-ESs will choose to disturb the consensus process and undermine the authentication of CRVs. Next, we will analyze the worst situation of the CC system under the DPBFT mechanism.

From the perspective of malicious CTs, the most harmful action to the consensus is to mislead as many SCSs as possible, so that the system cannot reach a consistent states. Given the fixed malicious CTs f_1, in the worst situaion, each SCS should only have the minimal number of CTs, *i.e.*, $n_1 = n_2 = ... = n_M = \xi$, so that the malicious CTs can destroy one sub-consensus with the least cost. In this case, the number of "occupied" SCSs ("occupied" SCS refers to the SCS that cannot broadcast the correct EXCOMMIT message in post-prepare stage) can be expressed as

$$N_{occ} = \lfloor f_1 / \lfloor \frac{\xi}{3} + 1 \rfloor \rfloor \tag{14}$$

The worst case during DPBFT is that malicious CTs and spf-ESs conspire to attack the system. By observing the attack of malicious CTs, the optimal attack strategy of spf-ES is to implement single-point of failure on those "non-occupied" SCSs, thus the total number of SCSs being attacked is

$$N_{att} = f_2 + N_{occ}. \tag{15}$$

Similarly, the post commit process in DPBFT ensures that it can tolerant at most $\lfloor M/3 \rfloor$ SCSs, that is

$$N_{att} < \lfloor M/3 \rfloor. \tag{16}$$

By rearranging the inequality above, the tolerant upper bound of spf-SCS can be obtained

$$f_2 < \lfloor M/3 \rfloor - \lfloor f_1 / \lfloor \frac{\xi}{3} + 1 \rfloor \rfloor \tag{17}$$

Based on the analysis above, the communication overhead can be approximately calculated as $O(M^2 + Mn_{max}^2)$ according to Eq. (13), where n_{max} is the maximum number in $\mathcal{M}$, instead of the $O(N^2)$ in PBFT (N is the total number of CTs). Since both M and n_{max} are far less than the large scale N, it can be deduced that the proposed DPBFT achieves a lower communication overhead compared with conventional PBFT. While the low communication overhead comes at the cost of certain security. As shown in Eq. (17), compared to conventional PBFT, the proposed DPBFT has a $\lfloor f_1 / \lfloor \frac{\xi}{3} + 1 \rfloor \rfloor$ reduction in terms of single-point of failure. Besides, the minimal number of CTs within each SCS ξ has a non-negligible impact on both communication and security. With the increase of ξ, the defensibility of single-point of failure can be enhanced as Eq. (17), meanwhile this will conversely aggregate the communication cost. In practical, the value of ξ is related with the ES ability of constructing CTs, and it should be well designed of the CC system, in order to make a good balance between the security and communication.

B. Analysis of the P4C Algorithm

In this subsection, the proposed P4C algorithm will be analyzed in terms of authentication delay and resistance against potential malicious attacks.

1) Authentication Latency of P4C Algorithm: The total authentication latency comprises three components: the setup. commit and verification processes. In order to quantify the overall latency, several variables are required defined.

First, the bit length of messages are given. There are total 6 types of messages during the P4C algorithm, including 4 random number r, e, y, s with bit length σ_1 and 2 random elliptic curve points G, H with the bit length σ_2. Moreover, we assume all the header of the sending messages have the equal length with $\triangle$. Denote C_p as the time consumption of generating the group of elliptic curve with a large prime p. To measure the computation consumption of the P4C algorithm and the comparison groups, we resort to the computation overhead that is defined as the time consumption of one certain operation [28]. There are four related operations during the simulation: the generation of hash value C_h, the generation of a random number C_r, the elliptic curve pairing that generates the commit C_c in Eq. (8), (10), and the verify function C_v. The latency during the setup process can be calculated as

$$\begin{aligned} l_{setup} &= (C_p + 2C_r) + (C_r + C_c) + 4C_r \\ &+ max(\frac{\triangle + 2\sigma_2 + 4\sigma_1}{R_{HO,CT}}, \frac{\triangle + 2\sigma_2 + 2\sigma_1}{R_{HO,CRV}}), \end{aligned} \tag{18}$$

where $R_{HO,CT}$ and $R_{HO,CRV}$ are the transmission rate between the smart contract $HandOver$ and the ES_E^V, CRV, respectively. Here $(C_r + C_c)$ represents the point generation process: $H = qG$. Then, the commit process includes the secret generation process, the calculation of blind factor and commit calculation process, wherein the latency can be expressed as

$$l_{commit}^{CT} = C_h + 2 * C_c, \quad l_{commit}^{CRV} = C_h + C_c. \tag{19}$$

At last, the sending verification process can be computed as

$$l_{sv}^{CRV} = \frac{\triangle + 2\sigma_2}{R_{CT,New}}, \; l_{sv}^{CT} = \frac{\triangle + 2\sigma_1}{R_{CRV,New}}, \tag{20}$$

where $R_{CRV,New}$ and $R_{CT,New}$ are the corresponding channel condition between the ES_{New} and CRV, ES_V^E. Consequently, the total latency of the authentication process can be calculated as

$$l_{aut} = l_{setup} + max(l_{commit}^{CRV} + l_{sv}^{CRV}, l_{commit}^{CT} + l_{sv}^{CT}) + C_v. \tag{21}$$

Based on the equations above, it can be deduced that the commit process and the sending verification process of both CRV and CTs can be operated in parallel, thus the overall authentication latency can be greatly reduced.

2) Conspiracy Attack: The attack refers to that the malicious CRV can conspire with other vehicles in a small range in order to access to the new region with an illegal identity, namely id_{att}, then to interact with other vehicles with malicious transactions,namely TX_{att}s. However, due to the diffusion feature of the identity transaction TX_{it}, the CTs in other regions can hereafter receive the TX_{it} and verify the correctness of ic and ip. Under the assumption that malicious CRV cannot control most of the vehicles in the new region, the final authentication will failed. In this case, the identity id_{att} will be deemed as invalid in the new region. The transactions related to TX_{att}s will also be regarded as invalid, and not be appended in the ledger. That is to say, though the conspiracy attack can cheat honest vehicles within a small range, the attack will be eliminated alongwith the diffusion of TX_{it}, and all the malicious transactions TX_{att}s that occurred during the attack will also be expired.

3) Man-in-the-Middle Attack: The type of the attack means that the attackers intercept and steal the message during the authentication process, so as to obtain the private information of the honest vehicles. In the proposed P4C algorithm, both the ic and ip are in the form of pedersen commitments, which conceal the secret attributes Atr, Besides, the P4C leverage the parallel verification scheme without the opening procedure. Even if the attackers obtains the public point of elliptic curve G, H, they cannot calculated the corresponding attributes Atr within polynomial time.

4) Replay Attack: The attack refers to the attackers that re-use their authenticated ic or collect others ic to realize re-authentication. In our proposed authentication framework, each transaction is marked by the timestamp. During the verification process of the consensus, all the CTs will verify the time current time with the timestamp encapsulated in TX_{id}. If the gap between the current time and timestamp locates within a certain time period, then the transaction TX_{id} is valid, otherwise it is refused. Moreover, since the ip is generated by referring to the latest Atr value on the ledger. In this case, the authentication process will be also denied if the malicious one CRV replays an previous ic to the new region.

VI. Performance Evaluation

In this section, we evaluate the proposed CyberChain based authentication framework. The proposed P4C algorithm is firstly simulated with respective to communication and computation overheads. Then, the DPBFT is evaluated in terms of signaling cost and authentication delay. Finally, the security performance and caching cost are investigated of the proposed CC based framework.

A. Simulation Setup

We measure the P4C algorithm on a PC with Inter Core i7-9750H 2.6GHz and 16G RAM. For the authentication part, we resort to the $SHA256$ and $int()$ function to transform the Atr to an integer value. Moreover, we generate elliptic curve point with the recommended elliptic curve parameters sec256k1 presented in [29] with 160 bit length. The corresponding generator key q with a 256 bit length ($i.e.$ $\sigma_1 = 256\ bit$), so that a generation elliptic curve point can be obtained by $H = qG$. Besides, the blind factor y, r, s and challenge factor e are generated randomly with the σ_1 bit length. Two existing authentication schemes are chosen as the comparison groups, $i.e.$, the NPPPC [26] and the zkPC [27] algorithms.

TABLE II: SIMULATION PARAMETERS

Parameters	Value
The Number of Vehicle	50
Channel Loss between Vehicles and ESs PL	$\alpha + 10\beta log(d) + X_\delta$
The distance between vehicles and ESs	uniform distribution within (20,100)
Authentication Block Header	80 KB
Data rate of CTs in cyberspace	12Mbps
Minimal Constructing Requirement of CT within one SCS ξ	[3, 15]
Blind Factors y, r, s, Challenge Factor e	σ_1=256-bit length
Elliptic Curve G, H	σ_2=160-bit length
Computation Overhead (ms)	C_h = 0.01215, C_c = 81.96496 C_r = 0.01478, C_v = 0.00309

For the simulation of CyberChain, a conventional physical blockchain with standard PBFT consensus is selected as comparison group. The communication link of vehicles is modeled as the mmWave transmission link with the path loss model $PL[dB] = \alpha + 10\beta log(d) + X_\delta$ [30], where α is the intercept in dB, β is the slope and X_δ follows the Gaussian distribution with zero mean and δ standard deviation. d is the distance between vehicles that is set as the uniform distribution within $(20, 100)$. To characterize the V2VC of CTs, we assume each CT is constructed in the corresponding ES as the Universal Serial Bus (USB) system, wherein the CTs are linked in series through hubs [31]. The communication rate between CTs can be approximately modeled as the data transfer through the downstream ports with the bitrate 12Mbps. We set the blocksize as 100, wherein the size of each TX_{id} is $3\sigma_2$, and the size of the block header equals 80KB. More specific simulation parameters are shown in Table II.

B. Numerical Results

We first evaluate the proposed P4C algorithm in Table III. There are two provers: the CRV and the ES_V. For the CRV, its computation consumption contains one hash operation C_h and one pairing operation C_c during the parallel commit stage, and its communication overhead comes from the sending of c_0 in Eq. (8) with the σ_2 length. For the ES_V, its computation consumption consist of one hash operation C_h and four pairing operations $4C_c$. The communication consumption includes the transmission of c_1 and c_2, with $2\sigma_2$ length. Similarly, we conclude the communication and computing consumption of NPPPC and zkPC algorithms in Table II. It can be figured that the proposed P4C algorithm efficiently reduce the communication and computation overhead of CRV. Though the computation overhead of ES_V has a $3C_c - C_r$ increment compared to NPPPC, the proposed algorithm realizes good privacy-preserving of the provers. Moreover, the proposed P4C algorithm enables the smart contract $HandOver$ to generate the the blind factors G, H, y, r, s, e in a decentralized manner. Although the contract will increase $4\sigma_1$ generation and

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2021.3132961, IEEE Transactions on Vehicular Technology

TABLE III: COMPUTATION & COMMUNICATION CONSUMPTION

Algorithm	NPPPC [26]	zkPC [27]	P4C
Computation Overhead of the Prover	$C_h + C_c + C_r$	$C_h + 4C_c + 3C_r$	CRV: $C_h + C_c$ ES_V:$C_h + 4C_c$
Communication Overhead of the Prover	$\sigma_2 + 2\sigma_1$	$\sigma_2 + 3\sigma_1$	CRV: σ_2 ES_V:$2\sigma_2$
Computation Overhead of the Verifier	$C_c + C_v$	$C_r + C_c + C_v$	C_v
Communication Overhead of the Verifier	0	σ_1	0
Public-parameter Generation	Third Party : (Centralized) $2\sigma_2$	Third Party: (Centralized) $2\sigma_2$	*HandOver* of CC: (Decentralized) $2\sigma_2 + 4\sigma_1$
Communication-Efficient	✓	–	✓
Privacy-Preserving	–	✓	✓

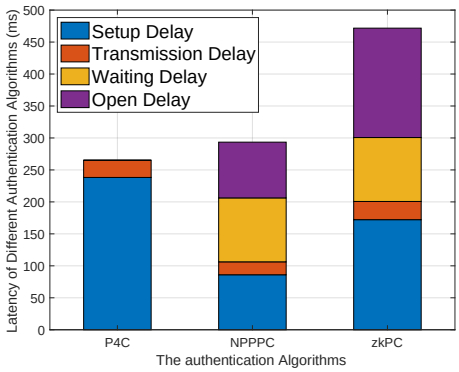


Fig. 4: The Authentication Latency of Different Algorithms

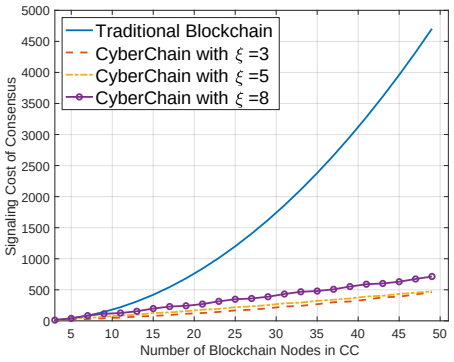


Fig. 5: The Signaling Overhead of the CPBFT Consensus

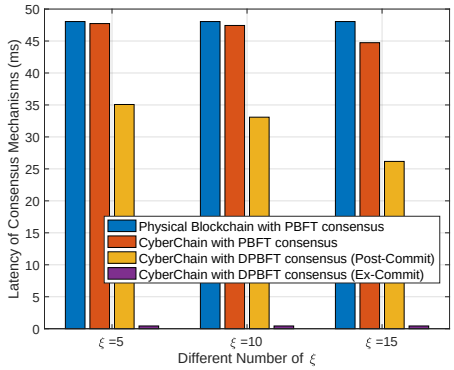


Fig. 6: The Consensus Latency with Different CT Requirement

transmission, it can eliminate the open stage and support the parallel commit stage, thus reducing the authentication latency.

The authentication delay are presented in Fig. 4. It can be figured that the proposed P4C algorithm achieves the fastest authentication than the comparison groups. During the setup stage, since the P4C requires the smart contract to calculate the public points G, H as well as blind factors y, r, e, s, while the comparison groups only need to calculate the G, H, the P4C has a relative long setup delay. However, the blind factors are generated by the *HandOver* that are accessible only for the legal CTs in the CC, and the factors can be simultaneously transmitted to the CRV and ES_V with immutability. In this case, the two provers (*i.e.* the CRV and ES_V) can send the identity proof in parallel, instead of waiting for certain time period as conventional Pedersen commitment schemes. Consequently, both the waiting stage and the open stage can be eliminated in the proposed P4C algorithm, thereby the overall authentication latency can be greatly reduced.

Then, the performance of the proposed CC is discussed. Two comparison groups are chosen: a physical private blockchain with the PBFT consensus, and a cyberchain with the PBFT consensus. It should be noted that we investigate the consensus latency within one hop range, that is to say, all the nodes in the blockchain can transmit the consensus related message (post-prepare and post commit) via one hop communication. We tend to utilize the simplified consensus latency to prove the lightweight and time-efficient features of the proposed DPBFT. As the V2VC is not restricted by the physical channel, if the consensus latency of the proposed CC within one hop shows superiority than physical blockchain, it will outperforms in the eventual consensus process.

As shown in Fig. 5, the signaling overhead is investigated. The signaling overhead is the total communication times during consensus process. It can be figured that the proposed DPBFT greatly reduces the communication overhead, realizing a maximum reduction of 80 %. The saved overhead increases with the increasing of the number of nodes within the CS (*i.e.* CTs). Compared with traditional physical blockchain with PBFT consensus,the proposed DPBFT takes the advantages of the division of CS, as expressed in Eq. (13). The total CS is divided into several SCSs, each of which consists ξ CTs. The CTs within one SCS firstly implement the intra-commit in a $O(\xi)$ complexity as illustrated in Fig. 3, then the local consensus result will sent to other SCSs to reach a post-commit process, thereby reducing the total communication overhead. In addition, it can be inferred that the overhead increases with the number of ξ that refers to the minimal constructing requirement of CTs within one SCS. given the fixed number of CTs N, the lower bound of communication overhead in Eq. (13) can be transformed as $c \geq 2N(\xi - 1) + \frac{N^2}{\xi^2} - \frac{N}{\xi}$. By calculating its first derivative, it yields $c' = N\frac{\xi + 2\xi^3 - 2N}{\xi^3}$. In this case, continuously increasing the value of ξ will make $c' > 0$, thus resulting in the increment of overhead.

The overall consensus latency is investigated in Fig. 6. The latency of cyberchain with PBFT consensus is slightly smaller than that of the physical chain, which is credit to the V2VC. Compared with physical transmission, the V2VC has a more stable and faster transmission rate, while the advantages of cyberchain is not fully demonstrated in one hop range.

This article has been accepted for publication in a future issue of this journal, but has not been fully edited. Content may change prior to final publication. Citation information: DOI 10.1109/TVT.2021.3132961, IEEE Transactions on Vehicular Technology

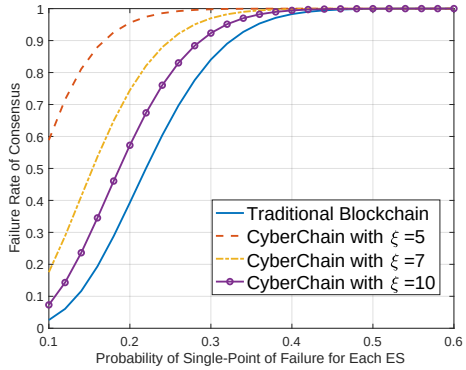


Fig. 7: The Defensibility of Single-Point of Failure

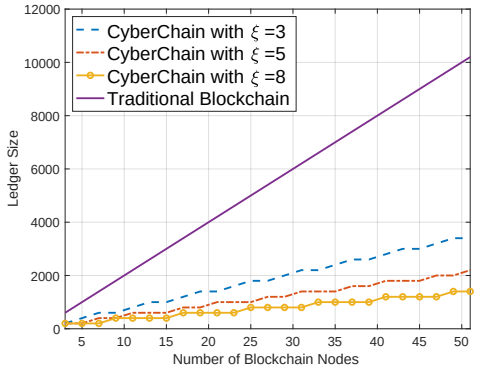


Fig. 8: The Storage Cost of the CyberChain

In this case, the proposed DPBFT shows great superiority compared to the other twos. Due to the ex-commit process of the DPBFT, the consensus is firstly achieved within one SCS in a short time. Then, the post-prepare process enables each SCS to broadcast one message, instead of broadcasting by every nodes, which shortens the latency of post-commit process. Combing the two process, the overall latency is reduced. Besides, it is noted that increasing ξ will further enhance the latency performance. This can be explained with the increasing of ξ, the inter-communication among SCSs will be replaced by the intra-communication among CTs. The intra-commit stage can be accelerated by means of V2VC in a parallel manner, thus realizing the lightweight and time-efficient.

Fig. 7 shows the defensibility of single-point of failure (spf) of the proposed CC. Compared with traditional blockchain, the proposed DPBFT shows weakness towards the malicious attack. However, according to Eq. (17), the defensibility of spf will be enhanced with the increment of ξ. Combing both Fig. 5, Fig. 6 and Fig. 7, it can be deduced that the proposed CC make a good tradeoff between the security and communication cost. In practical deployment, we can choose the a suitable ξ in CC, so that both the communication and the defensibility can reach a optimal value.

The storage cost of the proposed CC is finally investigated in Fig. 8. The cost of traditional blockchain is linearly increasing with the number of blockchain nodes. This is obvious since the total centralized physical blockchain enforces each node to cache a complete ledger. While the proposed CC shows good storage-saving power than than the physical blockchain. It can be figured that a larger ξ in CC will contribute to a lower storage cost. This benefits from the *distributed transactions but centralized storage* of the CC, as discussed in Section III. C. The ESs can provide their physical caching capability for the blockchain ledger, whereas they can only access to the ledge with their own CTs. Consequently, the CTs can transact with other CTs in cyberspace, without being restricted by physical storage, proving the scalability of the proposed CC.

VII. Conclusion

In this paper, a CyberChain based framework is proposed for authentication in highly dynamic IoVs. Integrating both blockchain and cybertwin technology, we build a blockchain in the cyberspace to enhance the authentication efficiency. Based on the framework, a P4C algorithm is proposed to realize privacy-preserving and communication-efficient authentication. We further design a DPBFT consensus mechanism for the cyberchain to reduce the authentication delay. Simulation results demonstrate the superiorities of the proposed CyberChain, wherein the caching cost can be reduced by 50 % compared with traditional blockchain while ensuring almost equal security. Moreover, compared with traditional schemes, the P4C algorithm reduces the authentication latency by the parallel design, meanwhile saving the communication and computation overhead of CRVs and ESs. The proposed DPBFT has an 80 % reduction of the signaling cost, and the overall consensus latency is also reduced facilitated by the virtual communication of CTs. Future work will focus on analyzing the optimal construction and migration strategies of CTs based on the proposed cyberchain framework.

References

[1] Q. Feng, *et al*, "BPAS: Blockchain-Assisted Privacy-Preserving Authentication System for Vehicular Ad Hoc Networks," in IEEE Transactions on Industrial Informatics, vol. 16, no. 6, pp. 4146-4155, June 2020, doi: 10.1109/TII.2019.2948053.

[2] J. Zhang, *et al*, "An Extensible and Effective Anonymous Batch Authentication Scheme for Smart Vehicular Networks," in IEEE Internet of Things Journal, vol. 7, no. 4, pp. 3462-3473, April 2020, doi: 10.1109/JIOT.2020.2970092.

[3] H. Zhou, N. Cheng, J. Wang, J. Chen, Q. Yu and X. Shen, "Toward Dynamic Link Utilization for Efficient Vehicular Edge Content Distribution," in IEEE Transactions on Vehicular Technology, vol. 68, no. 9, pp. 8301-8313, Sept. 2019, doi: 10.1109/TVT.2019.2921444.

[4] X. Zha, W. Ni, K. Zheng, R. P. Liu and X. Niu, "Collaborative Authentication in Decentralized Dense Mobile Networks With Key Predistribution," in IEEE Transactions on Information Forensics and Security, vol. 12, no. 10, pp. 2261-2275, Oct. 2017, doi: 10.1109/TIFS.2017.2705584.

[5] Xu, Hao, et al. "Blockchain-enabled resource management and sharing for 6G communications." Digital Communications and Networks 6.3 (2020): 261-269.

[6] Y. Wu, K. Zhang and Y. Zhang, "Digital Twin Networks: a Survey," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2021.3079510.

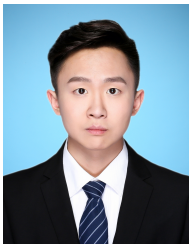
[7] K. Xiong, S. Leng, C. Huang, C. Yuen and Y. L. Guan, "Intelligent Task Offloading for Heterogeneous V2X Communications," in IEEE Transactions on Intelligent Transportation Systems, vol. 22, no. 4, pp. 2226-2238, April 2021, doi: 10.1109/TITS.2020.3015210.

[8] H. Zhou et al., "TV White Space Enabled Connected Vehicle Networks: Challenges and Solutions," in IEEE Network, vol. 31, no. 3, pp. 6-13, May/June 2017, doi: 10.1109/MNET.2017.1600049NM.

[9] P. Jia, X. Wang and X. Shen, "Digital-Twin-Enabled Intelligent Distributed Clock Synchronization in Industrial IoT Systems," in IEEE Internet of Things Journal, vol. 8, no. 6, pp. 4548-4559, 15 March15, 2021, doi: 10.1109/JIOT.2020.3029131.

[10] Q. Yu, J. Ren, Y. Fu, Y. Li and W. Zhang, "Cybertwin: An Origin of Next Generation Network Architecture," in IEEE Wireless Communications, vol. 26, no. 6, pp. 111-117, December 2019, doi: 10.1109/MWC.001.1900184.

[11] H. Zhou, W. Xu, J. Chen and W. Wang, "Evolutionary V2X Technologies Toward the Internet of Vehicles: Challenges and Opportunities," in Proceedings of the IEEE, vol. 108, no. 2, pp. 308-323, Feb. 2020, doi: 10.1109/JPROC.2019.2961937.
[12] S. Lv and Y. Liu, "PLVA: Privacy-Preserving and Lightweight V2I Authentication Protocol," in IEEE Transactions on Intelligent Transportation Systems, doi: 10.1109/TITS.2021.3059638.
[13] L. Song, G. Sun, H. Yu, X. Du and M. Guizani, "FBIA: A Fog-Based Identity Authentication Scheme for Privacy Preservation in Internet of Vehicles," in IEEE Transactions on Vehicular Technology, vol. 69, no. 5, pp. 5403-5415, May 2020, doi: 10.1109/TVT.2020.2977829.
[14] Islam,*et al*(2018). A robust and efficient password-based conditional privacy preserving authentication and group-key agreement protocol for VANETs. Future Generation Computer Systems, 84, 216-227.
[15] Y. Xun, J. Liu, N. Kato, Y. Fang and Y. Zhang, "Automobile Driver Fingerprinting: A New Machine Learning Based Authentication Scheme," in IEEE Transactions on Industrial Informatics, vol. 16, no. 2, pp. 1417-1426, Feb. 2020, doi: 10.1109/TII.2019.2946626.
[16] C. Wang, *et al*, "B-TSCA: Blockchain assisted Trustworthiness Scalable Computation for V2I Authentication in VANETs," in IEEE Transactions on Emerging Topics in Computing, doi: 10.1109/TETC.2020.2978866.
[17] D. Gabay, K. Akkaya and M. Cebe, "Privacy-Preserving Authentication Scheme for Connected Electric Vehicles Using Blockchain and Zero Knowledge Proofs," in IEEE Transactions on Vehicular Technology, vol. 69, no. 6, pp. 5760-5772, June 2020, doi: 10.1109/TVT.2020.2977361.
[18] Z. Ma, J. Zhang, Y. Guo, Y. Liu, X. Liu and W. He, "An Efficient Decentralized Key Management Mechanism for VANET With Blockchain," in IEEE Transactions on Vehicular Technology, vol. 69, no. 6, pp. 5836-5849, June 2020, doi: 10.1109/TVT.2020.2972923.
[19] X. Liao et al., "Cooperative Ramp Merging Design and Field Implementation: A Digital Twin Approach Based on Vehicle-to-Cloud Communication," in IEEE Transactions on Intelligent Transportation Systems, doi: 10.1109/TITS.2020.3045123.
[20] X. Xu et al., "Service Offloading with Deep Q-Network for Digital Twinning Empowered Internet of Vehicles in Edge Computing," in IEEE Transactions on Industrial Informatics, doi: 10.1109/TII.2020.3040180.
[21] C. Hu et al., "A Digital Twin-Assisted Real-time Traffic Data Prediction Method for 5G-enabled Internet of Vehicles," in IEEE Transactions on Industrial Informatics, doi: 10.1109/TII.2021.3083596.
[22] Y. Liao, et al. "Cross-regional driver–vehicle interaction design: an interview study on driving risk perceptions, decisions, and ADAS function preferences." Iet Intelligent Transport Systems (2018).
[23] S. Popov. (2018). "The tangle.", [Online]. Available: https://www.iota.org/foundation/research-papers.
[24] G. Qiao, S. Leng, S. Maharjan, Y. Zhang and N. Ansari, "Deep Reinforcement Learning for Cooperative Content Caching in Vehicular Edge Computing and Networks," in IEEE Internet of Things Journal, vol. 7, no. 1, pp. 247-257, Jan. 2020, doi: 10.1109/JIOT.2019.2945640.
[25] Wang, *et al*. "Blockchain-based multi-party proof of assets with privacy preservation." Information Sciences 547 (2021): 609-621.
[26] Romdhane, Rihem Ben, et al. "An Efficient and Privacy-Preserving Billing Protocol for Smart Metering." AINA (2). 2021.
[27] Zhang, Liang-Ao, et al. "ABE based Access Control with Authenticated Dynamic Policy Updating in Clouds." International Journal of Security and Its Applications 9.8 (2015): 95-110.
[28] Y. Yao, X. Chang, J. Mišić and V. B. Mišić, "Lightweight and Privacy-Preserving ID-as-a-Service Provisioning in Vehicular Cloud Computing," in IEEE Transactions on Vehicular Technology, vol. 69, no. 2, pp. 2185-2194, Feb. 2020, doi: 10.1109/TVT.2019.2960831.
[29] "Standards for Efficient Cryptography Group",[Online]. Available: https://www.secg.org/.
[30] X. Chen, *et al*, "Deep Learning Based Intelligent Inter-Vehicle Distance Control for 6G-Enabled Cooperative Autonomous Driving," in IEEE Internet of Things Journal, doi: 10.1109/JIOT.2020.3048050.
[31] M. F. *et al*, "A Provably Secure Two-Factor Authentication Scheme for USB Storage Devices," in IEEE Transactions on Consumer Electronics, vol. 66, no. 4, pp. 396-405, Nov. 2020, doi: 10.1109/TCE.2020.3035566.



Haoye Chai received the B.Sc. degree in information and communication engineering from University of Electronic Science and Technology of China, Chengdu, China, in 2016. He is currently working toward the Ph.D. degree in University of Electronic Science and Technology of China. His research interests include Mobile Edge Computing, Internet of Vehicles and blockchain in wireless networks.

Supeng Leng is a Full Professor and a Vice Dean in the School of Information & Communication Engineering, University of Electronic Science and Technology of China (UESTC). He is also the leader of the research group of Ubiquitous Wireless Networks. He received his Ph.D. degree from Nanyang Technological University (NTU), Singapore. He has been working as a Research Fellow in the Network Technology Research Center, NTU. His research focuses on resource, spectrum, energy, routing and networking in Internet of Things, Internet of Vehicles, broadband wireless access networks, and the next generation mobile networks. He published over 200 research papers in recent years. He serves as an organizing committee chair and TPC member for many international conferences, as well as a reviewer for over 10 international research journals.

Jianhua He received the Ph.D. degree from Nanyang Technological University, Singapore, in 2002. He is currently a Reader with University of Essex, UK. His main research interests include wireless communications and networks, connected vehicles, autonomous driving, Internet of Things, mobile edge computing, data analytics, AI and machine learning. Dr He published more than 150 research papers in international journals and conferences in these research areas. He is the workshop chair of MobiArch'20 and ICAV'21, a steering committee member of MobiArch'21 and a member of editorial board for several international journals. He is the Coordinator of EU Horizon2020 projects COSAFE and VESAFE on cooperative connected autonomous vehicles.

Ke Zhang received his Ph.D. degree in University of Electronic Science and Technology of China, 2017. He is currently an associate professor in the School of Information and Communication Engineering, University of Electronic Science and Technology of China. His research interests include scheduling of mobile edge computing, design and optimization of next-generation wireless networks, and the Internet of Things.

Baoyi Cheng received the B.S. degree in 2020 from the University of Electronic Science and Technology of China, Chengdu, China, where he is currently working toward the M.S. degree with the School of Information and Communication Engineering. His research interests include the vehicular networks, mobile edge caching, and blockchain in wireless networks.