Decentralized Public-Key Infrastructure With Blockchain in V2X Communications

Promising or Only Euphoria?

Edy Kristianto, Van-Linh Nguyen, and Po-Ching Lin | National Chung Cheng University

A centralized public-key infrastructure (PKI) has revealed disadvantages to enterprise applications. This work presents a taxonomy of blockchain-based decentralized PKI schemes along with the prospective technologies for developing a robust PKI for vehicle-to-everything communications.

In the coming years, vehicle-to-everything (V2X) communications will be viewed as crucial technologies for expanding the sensing coverage for connected vehicles. Most often, V2X communications cover multiple types, such as vehicle to infrastructure (V2I), vehicle to network, vehicle to vehicle (V2V), and vehicle to pedestrian. In typical vehicular communications, a V2X-enabled vehicle has to be authenticated before joining V2X communications. Authentication is required to protect such communications against unauthorized users and thus further enhance the reliability of sharing information. Given the premise of millions of connected vehicles, V2X authentication faces two key issues: scalability and availability.

The development of V2X security systems tends to implement large-scale public-key infrastructure (PKI) systems to support authentication in V2X communications. The PKI-based V2X ecosystem needs trusted entities, such as the certificate authority (CA), to provide a bunch of pseudonym keys. The pseudonym keys are used to tackle privacy issues and need to change frequently. The PKI implementation can be intrinsically centralized (C-PKI) or decentralized (D-PKI). The centralized architecture often faces bottleneck issues from the heavy authorization, registration, or verification requests traffic. Meanwhile, decentralizing the authentication functions is a potential solution for avoiding bottleneck performance and misbehaving CA issues. For example, the European Union (EU) prefers to use multiple root CAs in the PKI to provide redundancy and interoperability in expanding and decentralizing operations.

Several recent studies[1,2] and industrial solutions (such as Remme) have shown that a D-PKI has the potential of being an alternative to a C-PKI. One of the most popular decentralized technologies is blockchain. By leveraging the strength of verifiable peer-to-peer blockchain networks, a blockchain-based D-PKI model (termed a *B-PKI*) can effectively enhance vehicle authentication capabilities (scalability/availability) and privacy. By contrast, the C-PKI must accomplish the enhancement via a complicated pseudonym certificate generation and revocation model. However, decentralized solutions are not entirely straightforward for tackling PKI management. The existence of a CA is still required as the legal authority that issues certificates. CAs store the credentials in hardware security modules at data centers and are kept offline.[3] B-PKIs are in the research phase for a consortium of governments and automotive industries, such as the Mobility Open Blockchain Initiative.

Considering the potential of such a decentralized technology, this work extensively reviews the latest achievements in using blockchain for building scalable V2X authentication and privacy preservation and answers some key questions.

Digital Object Identifier 10.1109/MSEC.2022.3141727
Date of current version: 31 January 2022

1. How can blockchain technology compensate for the inadequacies in the conventional PKI and help to enhance the scalability and availability of V2X authentication?
2. How is B-PKI architecture different from that of a conventional C-PKI?
3. How can both security and privacy in a united PKI platform be guaranteed?
4. In what way is B-PKI architecture robust enough to withstand attacks that the C-PKI is struggling to deal with?
5. How can one improve the efficiency of the B-PKI and integrate it into well-established standards such as ETSI TS 103 415[3] to best support V2X authentication?
6. From the viewpoint of vehicles and service providers, how will such a B-PKI model impact their deployment capability, particularly backward compatibility?

Unlike earlier reviews, such as that of Mollah et al.,[2] this study focuses on the issues of blockchain technology for D-PKI models in V2X communications. Figure 1 shows the taxonomy of key technologies, vulnerabilities, defense methods, and future research directions that enhance the B-PKI model. These topics are then detailed in the following sections.

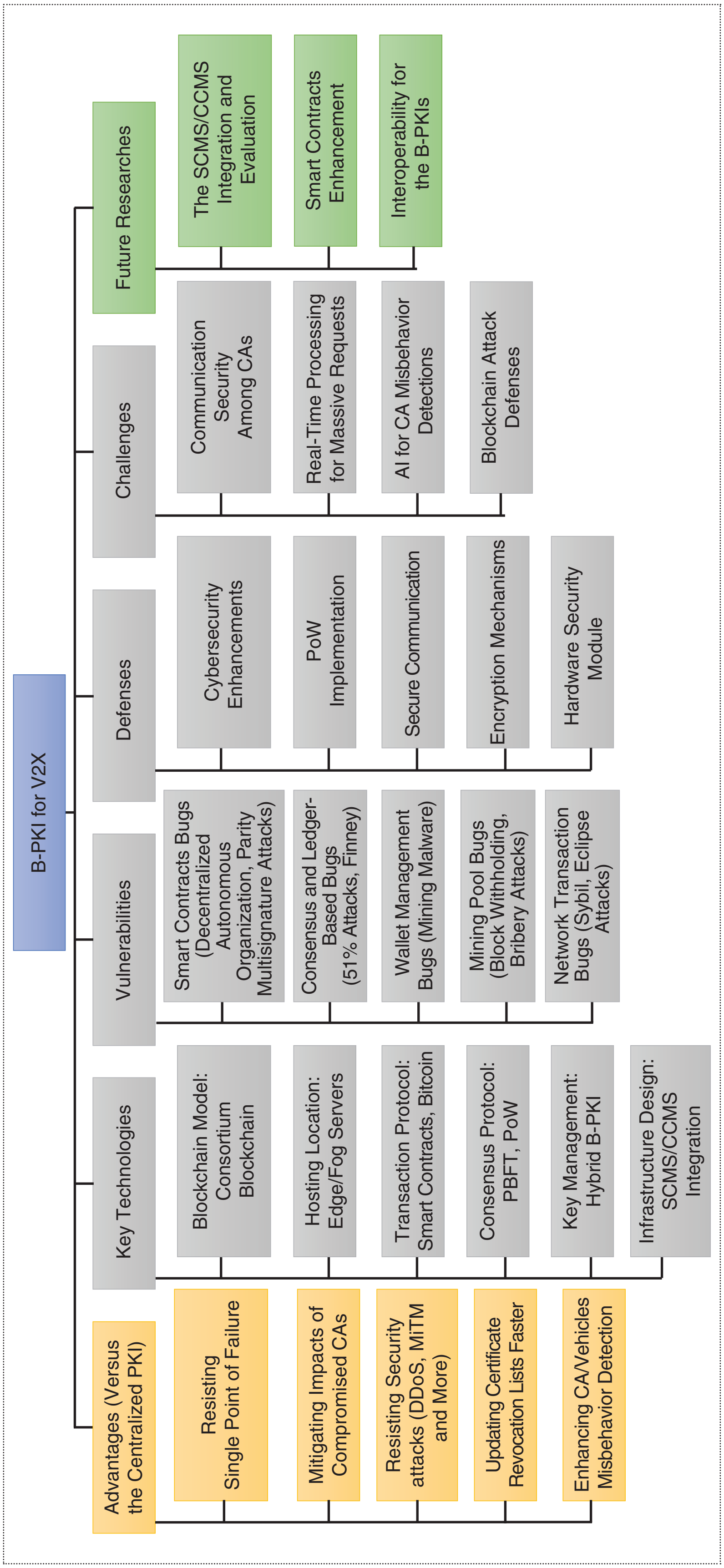
B-PKI for V2X
Advantages (Versus the Centralized PKI)
Resisting Single Point of Failure
Mitigating Impacts of Compromised CAs
Resisting Security attacks (DDoS, MiTM and More)
Updating Certificate Revocation Lists Faster
Enhancing CA/Vehicles Misbehavior Detection
Key Technologies
Blockchain Model: Consortium Blockchain
Hosting Location: Edge/Fog Servers
Transaction Protocol: Smart Contracts, Bitcoin
Consensus Protocol: PBFT, PoW
Key Management: Hybrid B-PKI
Infrastructure Design: SCMS/CCMS Integration
Vulnerabilities
Smart Contracts Bugs (Decentralized Autonomous Organization, Parity Multisignature Attacks)
Consensus and Ledger-Based Bugs (51% Attacks, Finney)
Wallet Management Bugs (Mining Malware)
Mining Pool Bugs (Block Withholding, Bribery Attacks)
Network Transaction Bugs (Sybil, Eclipse Attacks)
Defenses
Cybersecurity Enhancements
PoW Implementation
Secure Communication
Encryption Mechanisms
Hardware Security Module
Challenges
Communication Security Among CAs
Real-Time Processing for Massive Requests
AI for CA Misbehavior Detections
Blockchain Attack Defenses
Future Researches
The SCMS/CCMS Integration and Evaluation
Smart Contracts Enhancement
Interoperability for the B-PKIs

Figure 1. The taxonomy of key technologies, vulnerabilities, defense methods, and future research directions to enhance the B-PKI model. DDoS: distributed denial-of-service; MiTM: man in the middle; AI: artificial intelligence; PBFT: Practical Byzantine Fault Tolerance; PoW: proof of work; SCMS: Security Credential Management System; CCMS: Cooperative ITS Credentials Management System.

Background

Countries worldwide have different views on the shape of V2X authentication architecture as a result of different requirements on the features and local laws. The EU and the United States have a mature process in V2X development and have become a reference for other countries. In the EU, the PKI system for V2X is called the *Cooperative ITS Credentials Management System* (*CCMS*) and is maintained by the ETSI Intelligent Transport System (ITS). In the United States, it is called the *Security Credential Management System* (*SCMS*).[5] Indeed, at the time of this writing, there is still a gap to form a unified standard and clear specification of what a fully commercial PKI for vehicular communications looks like.

The SCMS mentioned in this article is a proof-of-concept reference from the United States. Future commercial products may have many changes. The key differences between the SCMS and CCMS are the architecture and standard references. For example, the CA management model in the SCMS is designed with high-level electors and a root CA to issue certificates for vehicles. This SCMS model works as a single control point where a national agency like the U.S. Department of Transportation will be the SCMS Manager.

In the EU, since it consists of many member state authorities, the CCMS architecture is tweaked to allow the EU members/commercial entities to run their own root CAs. The CAs are under central coordination of the Central Point of Contact (CPOC) and Trust List Manager (TLM) through the European Certificate Trust List. The CPOC and TLM are managed by the European Commission. This "multiple credential-management-systems" model is meant to preserve the autonomy of the stakeholders, where member states, vehicle manufacturers, and probably other entities can run their own version. Besides, the SCMS was originally designed for U.S.-based V2X standards, for example, dedicated short-range communications (DSRC), and it used the Wireless Access in Vehicular Environment Security IEEE 1609.2 protocol stack. The state-of-the-art standard reference for the SCMS in the United States is SAE J3161/1, after the U.S. Federal Communications Commission approved eliminating DSRC.

By contrast, the CCMS is designed to work with Cooperative ITS architecture in Europe and is based on ETSI TS 103 097 and TS 102 941. Because of the assumption of intermittent connectivity between the vehicles and the back-end infrastructure, the SCMS can issue a large number of pseudonym certificates, enough to use over the years with 20 per week. On the other hand, the CCMS was designed to operate with the assumption of frequent connectivity of vehicles to the back end; thus, this system prefers to issue a limited number of pseudonym certificates and mandate the valid time to a maximum of three months only.

Although there are differences in the architecture and standard references, both systems share many similarities in the component functionality, such as misbehavior authority (MA), pseudonym generation/management, or certificate revocation list (CRL) maintenance. Both systems can issue up to hundreds of billions of certificates per year—enough to support up to millions of vehicles in their countries. According to Statista, in 2018–2019, there were some 276 million vehicles registered in the United States and roughly 292 million units in Europe. Note that each vehicle can own dozens of pseudonyms keys for usage per year.

Since the U.S. and EU design philosophies on the credentials management system (CMS) have pursued different paths, other countries may side with their requirements. For example, Australia, China, Japan, and Korea will likely adopt a modified SCMS model where a national agency will manage their own root CAs and translate local policy requirements into corresponding technical and operational processes (such as a pseudonym certificate lifecycle). Because of the lack of available public documents on the selection decision in other countries, we believe that the dominant model for them will be the one that is widely used and proved with an affordable deployment cost.

> **"Given the premise of millions of connected vehicles, V2X authentication faces two key issues: scalability and availability."**

However, both the CCMS and SCMS are a form of C-PKI, which maintains a power for a central authority (a CA) in creating, validating, storing, and revoking user certificates. The C-PKI architecture has been proven to work with many Internet applications, but it has shortcomings in several areas: 1) trust maintenance among the PKI entities, 2) scalability to serve a massive number of vehicles, and 3) an efficient mechanism for pseudonym revocation in terms of cost and security. These drawbacks are becoming more challenging to overcome, particularly at the rapidly expanding Internet size. First, all vehicles in the C-PKI need to trust that the CAs are honest and uncompromised, but this strong assumption is somewhat self-confident. In practice, security breaches or insider attackers to issue rogue pseudonym certificates (misbehaving CAs) can potentially cause devastating damage to safety communication, personal privacy, and even the certificate providers. For instance, the certificate authority DigiNotar went bankrupt as a result of being the victim of theft of 500+ certificates.

Second, the C-PKI relies on a central authority to create, validate, store, and revoke the certificates. On such a central system, it will be challenging to maintain hundreds of billions of pseudonym keys in storage and distribution, let alone extensive verification/revocation. This raises scalability concerns for the C-PKI, that is, the single-point-of-failure issue in the centralized model. Finally, renewing CRLs or revoking certificates of a misbehaving vehicle in a timely manner is not an easy task because of the complexity of balancing the need for pseudonym revocation and bandwidth constraints of vehicular networks.

In the literature, there are several approaches to address these three issues. For example, Giannetsos and Krontiris[6] proposed direct anonymous attestation to shift the trust from the CA's infrastructures to a decentralized architecture. The pretty good privacy (PGP) is also a form of D-PKI-like architecture (used for email security); it indicates that a PGP user can be trusted if its messages have been signed by one or more other trustworthy PGP users. This web-of-trust model practically eliminates the single-point-of-failure problem, but it cannot deal with the key revocation. On the other hand, the blockchain-based PKI is expected to be the most promising technology to address the problems of trust maintenance, scalability, and efficient privacy preservation.

Blockchain-based PKI is the expected technology to deal with these shortcomings, which are a challenge to afford in the C-PKI. For privacy preservation, the hash function methods in the blockchain are the enablers. User transactions stay anonymous and secure since there is no link between user certificates (that is, the blockchain wallet address) and the owner's identity (using one-way hash functions). Any party can read content and history activities in a blockchain, but it does not know the real identity. Such transparency eliminates the trust problem on the third-party CA's actions. Besides, altering the records becomes impossible since an attacker needs to change every record in the blockchain. All the participating entities can notice any modification to the content. This feature significantly mitigates the threats of internal attackers.

Also, with the distributed architecture and fast consensus algorithms, the B-PKI can resist outsider attackers, such as distributed denial-of-service (DDoS) and double registration attacks, while supporting efficient CRL revocation (fast synchronization). From a design perspective, the B-PKI reduces the dependence on a powerful, centralized CA in a conventional PKI by shifting the power of proof for data authentication to third-party stakeholders in a fully decentralized network. By decentralizing the authentication components (for example, the CA) and supporting a strict peer-reviewed process, the B-PKI avoids the single point of failure and risks of compromised or misbehaving CAs. For compatibility, the B-PKI reuses some components of the C-PKI. Figure 2 illustrates the typical structure and general workflows of both PKIs. Both have essentially similar registration and certificate generation; the major differences are the certificate distribution model and authentication flow.

Finally, the B-PKI has features that are missing in the C-PKI, including certificate transparency and revocation transparency.[2,7] Since certificate signing and revocation operations can be tracked via an append-only public ledger, any fraudulent certificate or illegal actions in the revocation will be picked up by the monitoring or interested participants. In comparison, the C-PKI is less friendly because of nontransparency; that is, the interested parties do not often have oversight permission on operations. With all of the advantages, from an authentication provider's point of view, the B-PKI can be seen as a potential alternative to the C-PKI in practice. For vehicle users, no significant changes to the onboard unit (OBU) are needed because most blockchain processes occur in the service providers' infrastructure. This can significantly

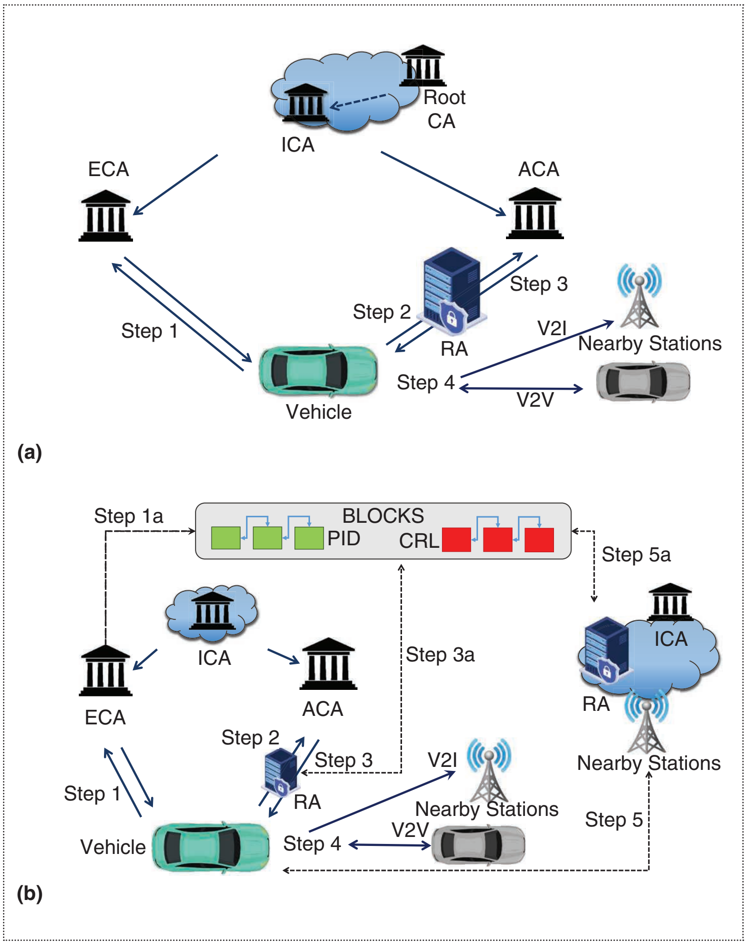

Figure 2. A comparison of the C-PKI versus B-PKI. (a) The registration and authentication process in a C-PKI scheme.[4] (b) The registration and authentication process in a B-PKI scheme. ECA: enrollment CA; ICA: intermediate CA; ACA: authorization CA; RA: registration authority; PID: pseudonym identity.

increase the deployment capability of the B-PKI because, unlike the strong motivations of service providers to find solutions to enhance infrastructure quality, users do not spend extra costs on a paid service.

A Workflow Comparison

In this section, we present the workflow of a B-PKI system in comparison with the C-PKI model. Note that this workflow is primarily invoked during bootstrap or when certificates are rotated. After receiving a bunch of pseudonym certificates, the vehicles may use the granted credentials for V2I/V2V communications until revoked or expired. A comparative overview of the workflow is detailed next.

System Initialization and Authentication Workflow

In initialization, participants prepare the security parameters required for registration and authentication. A PKI typically consists of two types of participants: CAs and entities (such as vehicles and nearby stations). Note that, in cellular V2X, a station can be a roadside unit (RSU)/next-generation node g (gNB)/radio unit. For comparison, we refer to the SCMS, and the terms will be simplified to root CA, intermediate CA (ICA), enrollment CA (ECA), authorization CA (ACA), and registration authority (RA). The root CA initializes and generates the certificates for an ICA, which then generates certificates for the ECA and ACA. Vehicles communicate with each other and the nearby stations through OBUs, which are mounted on the vehicles and support V2X communications. The OBU consists of a unique identity, for example, body serial number, machine number, or OBU identifier. In a typical B-PKI, each RA is also supposed to maintain a public ledger that contains all access records based on the vehicle identities in a city or a state. For illustrating the other steps in detail, Table 1 lists the relevant notation.

Vehicle Registration and Key Distribution

In this phase, the registration procedures in both PKIs, as illustrated in Figure 2(a)[4] and Figure 2(b),[7,8] involve the following similar interactive steps:

Table 1. Notation and definitions.

Notation	Definitions
V_i	Vehicle
PID_i	Pseudonym key
k_i^{Pu}	Public key
k_i^{Pr}	Private key
H_0, H_1	Hash value
Tx	Transaction

- *Step 1*: A registrant vehicle (denoted by V_i, which also implies the vehicle's OBU) sends a registration request, including its real identity (such as the OBU identifier) to an ECA, which returns the enrollment credential (EC) to the vehicle. The request can use a secure WWAN connection such as a cellular network between the ECA and vehicle.[3] The secure connection process is controlled by a device configuration manager.
- *Step 2*: The vehicle requests authorization certificates to the RA with its EC. The ACA verifies the vehicle's EC via the RA. If it is valid for registration, the RA will generate the certificates by communicating with the ACA. Each certificate includes an arbitrary pseudonym of V_i by PID_i, and the associated pair of keys by k_i^{Pu} (public key) and k_i^{Pr} (private key).
- *Step 3*: After generating PID_i, the RA may ask the ECA for a further check of the EC validation. V_i can download PID_i from the RA after getting the location and time to download the certificates with the information such as PID_i, k_i^{Pu}, and k_i^{Pr}.
- *Step 4*: After completing the registration steps, vehicles can use the assigned keys for secure communication with the other V2X entities. A vehicle can communicate with a nearby station via V2I messages or with the other vehicles via V2V messages.

The Differences in B-PKI

Conversely, as seen in Figure 2(b), the B-PKI makes some modifications to the C-PKI process, as described in the following substeps:

- *Step 1a*: After generating the EC, the ECA writes it in the blockchain as the block 0 for V_i.
- *Step 3a*: After generating PID_i, k_i^{Pu}, and k_i^{Pr}, the RA calculates $H_0 = hash\,(PID_i \,\|\, k_i^{Pu})$[8] and then writes it to the blockchain. The RA can also check whether *PID* is in the CRL without MA. The abstract workflow of the blockchain-based V2X authentication model is illustrated in Figure 3. Here, we assume that the RA is a blockchain node and connected to other RAs in different regions as a blockchain network. The RAs also have abundant computation resources to support the blockchain process.

When a vehicle travels to a different region (called roaming in IEEE Standard 1609.2.1-2020[4]), it does not need to reenroll. The vehicle only needs authorization from the RA in the different region to join the new region. The RA can access the blockchain to check whether H_0 is in the *PID* list or the CRL.

- *Step 5*: When the vehicle is in a region, it initiates an authentication request with its own PID_i and k_i^{Pu}. The request is then signed with k_i^{Pr} and sent to the near station (RSU/gNB/radio unit). Note that PID_i is obtained via a secure connection, which is often done in the bootstrap step. The vehicle can download *PID* by batches,[5] for example, 20 certificates per batch per week. The vehicle can then employ these certificates to sign the V2V/V2I messages. For privacy, a vehicle can compute a signature and attach one of its certificates to the message (such as basic safety messages). A vehicle can change *PID* periodically to protect its privacy. Also, the vehicle can transact with the stations (V2I) or nearby vehicles (V2V) as long as its certificate is valid.

- *Step 5a*: After receiving the request, the nearby station will forward it to the RA through a secure channel. Receiving the request, the RA restores the vehicle's identity (PID_i, k_i^{Pu}) and calculates $H_0 = hash(PID_i \| k_i^{Pu})$. If neither PID_i[9] nor k_i^{Pu}[7,8] is in the CRL, the RA will search in the public ledger. If the authentication information (PID_i, k_i^{Pu}) exists, it will update the authentication result in its database. At the same time, it will broadcast the authentication result to all the blockchain nodes. Note that, after receiving the authentication result, the rest of the RAs write a transaction $Tx = (PID_i \| k_i^{Pu} \| signed(PID_i \| k_i^{Pu})$ with the time stamp into the corresponding public ledger using a consensus algorithm, such as Practical Byzantine Fault Tolerance (PBFT). Since CRL processing is part of blockchain consensus synchronization, the records of misbehaving vehicles are updated immediately—at the time of occurrence—instead of waiting for a period as in the conventional C-PKI. This is an advantage of processing the CRL in the B-PKI over that in the C-PKI. Finally, based on the received authentication result from the RA, the nearby station merely forwards it to V_i.

The performance evaluation of both PKI models in the literature includes comparisons with other D-PKI models, which are built on nonblockchain technology and do not have miners to validate transactions. As shown in Table 2, the B-PKI performs authentication substantially faster than the C-PKI or nonblockchain D-PKI, particularly in the case of verifying the certificates of many vehicles simultaneously.

Privacy Preservation, Identity Maintenance, and Pseudonym Revocation

After successful authentication, a vehicle will receive temporary session information,[10] including PID_i and *SessionKey*, as part of authentication, and can use it to exchange messages with others (for example, nearby stations and peer vehicles). In a valid session, the vehicle can transmit data without reauthentication until the session has expired. However, privacy preservation in such data exchanges is of primary concern. To avoid leaking a user's identity in V2X communications, pseudonyms in both PKIs[4] are randomly generated and periodically changed, for example, every 20 min. Note that, with a different pseudonym, reauthentication is needed, and a new session must be initiated. A vehicle's privacy is preserved by using pseudonyms since it is infeasible to reveal its real identity by knowing the pseudonyms only. The integrity of all of the shared records is protected with hash values that are publicly audited/authenticated by the other entities in the blockchain.

However, in some special cases, such as when a misbehaving vehicle is detected, an authorized authority may still need to be able to reveal a vehicle's real identity. In these cases, the authority needs special permission to access the real identity from the PKIs. To use the key/credential space effectively, the study by Zheng et al.[8] of both PKIs proposes to periodically renew the expired credentials (PID_i, k_i^{Pu}) or reallocate the unused credentials to other entities. During reallocation, the CA may randomly choose and shuffle the sets of unused keys/pseudonyms and then randomly allocate them to different regions.[11] The simulation results show that the

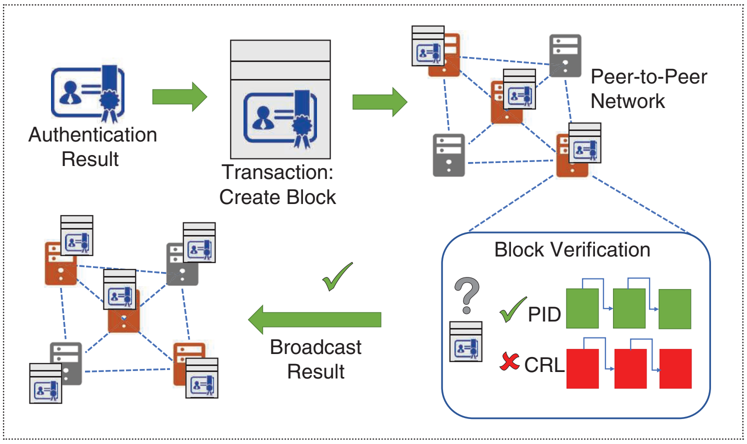

Figure 3. The abstract workflow of the blockchain-based V2X authentication model.

Table 2. The B-PKI performance.

Reference	Performance	B-PKI	C-PKI/ D-PKI*
Lu et al.[7]	Authentication of 120 certificates	80 ms	1,000 ms
Zheng et al.[8]	Authentication of 50 vehicles	1.8 s	4.4 s
Ikram et al.[9]	Verification of 60 signatures	100 ms	300 ms

**D-PKI: decentralized PKI without blockchain technology.*

shuffling process makes the anonymity achieved outperform existing schemes, in which the total processing time for 1,000 blockchain transactions takes 2 s only.[11]

For maintenance, if a vehicle is confirmed as a misbehaving entity (for example, it is forging a message), its keys/pseudonyms may be revoked. Yet, a vehicle may need a fundamental change to its credentials, such as changing the OBU, a system update by the manufacturer, resetting to the default system setting, or merely a change of the cryptographic scheme. All of these can cause the old keys/pseudonyms to be revoked for security reasons. In a blockchain model, the old keys/pseudonyms can be revoked by updating the CRL states of a vehicle in the transaction records.[9] The CA revokes $(PID_i, k_i^{\mathrm{Pu}})$ with a broadcast revocation transaction and then deletes the nodes associated with $(PID_i, k_i^{\mathrm{Pu}})$.[7] Regardless of the revocation approach, to join the V2X network again, the vehicle is required to again initiate reenrollment with the ECA or reauthentication with the RA to renew the *PID*.

Security Advantages and Disadvantages of B-PKI

The B-PKI has certain advantages of security over the C-PKI as follows:

- *Resistance against DDoS attacks*: The RAs responsible for authenticating vehicle authentication requests in the B-PKI are distributed. It is somewhat difficult for an attacker to shut down all of the nodes via volume attacks like DDoS in this case. If a node is overloaded and down from an attack, the other nodes in the chain can immediately take on its role[12] without interruption, which will practically foil the attack.
- *Resistance against impersonation attacks*: Since every vehicle is required to register its identity to the CA via the ECA and the RA through a secure channel, and all of the messages are signed (message, PID_i, k_i^{Pu}),[9] spoofing a vehicle's identity is difficult. To date, the Elliptic Curve Digital Signature Algorithm (ECDSA) is safe from cryptanalysis attacks.
- *Resistance against replay attacks*: Every blockchain record has a nonce and a time stamp field. The nearby stations can check the freshness of time stamps and nonces in the exchanged messages to the closest node to identify any replay attack.[7,9,12]
- *Resistance against man-in-the-middle (MiTM) attacks*: The security of hash and digital signature verification in the B-PKI guarantees the infeasibility of manipulating data and forging a vehicle signature in an encrypted message.[7]
- *Resistance against tampering attacks*: Since the transaction records of the registration information are auditable and immutable, tampering with the data for a vehicle is not feasible. Any modification of transaction records requires a consensus of the blockchain nodes when a change occurs, which reduces the risks of a local tampering action. An attack, if any, can be easily detected by the other peer nodes.[8,9]

Table 3. Prospective approaches for enhancing the B-PKI.

Enhancement target	Technology
Model selection	Consortium blockchain
Node selection	Edge, cloud computing
Consensus algorithm	PBFT, PoW
Key distribution	Instant Karma PKI, distributed PKI, hybrid PKI
Anonymity and pseudonymity	Smart contract, identity data, transaction data, on-chain data, cryptographic methods (such as secure multiparty computation, ZKF, and homomorphic hiding)

PoW: proof of work; ZKF: zero-knowledge proof.

The B-PKI still has a few weaknesses. As the workflow in Figure 2(b) shows, the trustworthiness of nodes is questionable if there is no mechanism to verify such participants in the system initialization. Several scholars have proposed potential solutions to address this issue. For example, in Mollah et al.[2] and Kang et al.,[13] a smart contract is used to provide predefined and important rules for making a decision in any trusted entity.

Prospective Approaches to Enhance the B-PKI

Following the general model in Figure 2, we summarize several prospective approaches to and lessons learned for enhancing the B-PKI (see Table 3).

Selecting the Correct Blockchain Model Can Significantly Boost the Overall Efficiency of B-PKI While Maintaining Affordable Cost of Node Chain Management

Depending on the policy of node selection in a chain, the blockchain model in the B-PKI can be considered as three types: public, private, and consortium. Since a consortium blockchain has multiple organizations instead of a single one (a private blockchain) or all users (a public blockchain) to govern the platform, it brings up the advantages of balancing the tradeoff between authentication efficiency and affordable cost of managing the chain members. The complexity of maintaining the trust of all public users and the high risks of trusting a single organization are the main reasons that the private and public blockchains are uncommon in V2X applications. As the summary in Table 4 shows, the consortium blockchain model will likely become the best choice for a B-PKI in V2X.

Proximity of Hosting Locations of Blockchain Members to Vehicles Makes B-PKI Respond Faster to Authentication Requests

The most common approach is to use edge servers as blockchain nodes. Edge/fog computing has become an essential part of a vehicular environment.[2] A particular advantage of an edge-based blockchain is that it supports cross-domain authentication. In this case, a united V2X authentication service manager at the edge servers can simultaneously handle multiple authentication requests from multitenant V2X services and vehicles in a particular geographic location. Using fog/edge computing for assisting authentication can be a promising approach. Unlike cloud technology, edge technology can satisfy the heavy computation of the blockchain techniques, provide storage for the records, and meet the time-delay constraint resulting from one-hop communications with end users.

> **"ZKF is simple, scalable, and highly secure, but it comes with heavy computation and energy consumption."**

There is a tradeoff between selecting a lightweight consensus algorithm to reduce heavy processing/energy consumption and a more secure version with the powerful protection of authentication transactions. Consensus is required to ensure a transaction record written to a blockchain (Step 5a of the B-PKI workflow). As Kang et al.[13] state, a large number of transactions can occur simultaneously in a large-scale authentication system. In this case, writing the transactions in chronological order becomes nontrivial. Noh et al.[14] compared the consensus algorithms, such as proof of work (PoW) and PBFT, and found that PBFT demands fewer computation resources than PoW does as a result of using fewer nodes for majority voting.

An alternative technology for the consensus scheme is proof of stake (PoS), where the miners mine or validate the transactions based on the number of coins they hold. Unlike a PoW protocol, by limiting the computational power based on the percentage of ownership staked, PoS systems like Cardano are tremendously more energy efficient and thus more environmentally friendly. Finally, zero-knowledge proof (ZKF) is another emerging consensus scheme used in ZCash, where one party (the prover) can prove that a specific statement is true to the other party (the verifier) without disclosing any additional information. ZKF is simple, scalable, and highly secure, but it comes with heavy computation and energy consumption. Some other consensus algorithms include proof of activity, proof of weight, proof of importance, and proof of capacity, although their popularity is not at the level of PoW or PoS.

Table 4. A summary of the prospective approaches for enhancing the B-PKI.

Author	Blockchain model	Issued keys to OBU	Encryption and consensus algorithms	Smart contract	Registration–validation	Revocation support
Zheng et al.[8]	Consortium	Public, private, pseudonym	ECC, PoW	No	CA	Yes
Ikram et al.[9]	Consortium	Public, private, pseudonym	Bilinear pairing cryptography, PoW	No	TA	Yes
Feng et al.[12]	Consortium	Public, pseudonym, biometric	ECC, fuzzy extractor, attribute-based encryption, PBFT	Yes	TA	Yes
Kang et al.[13]	Consortium	Public, private, pseudonym	ECDS, PoW	Yes	CA	No
Noh et al.[14]	Consortium	Public, private, pseudonym	ECC, Advanced Encryption Standard, PoW, PBFT	No	Root TA	No

ECC: elliptic curve cryptography; TA: Trusted Authority.

Smart Contracts and Key Management in B-PKI Are Key Technologies for Further Enhancement

An effective key and identity management model is essential for scalable authentication. There are three dominating key and identity models in the B-PKI: instant Karma based, distributed, and hybrid based. The instant Karma model aims at automating some functions of the B-PKI platform such as using Ethereum to correct the behavior of the CA and report unauthorized certificates.[15] In the distributed model, Bitcoin and Namecoin (the first fork of Bitcoin) are mainly named for their transaction protocols. Finally, a hybrid-based model highlights the intention of balancing the privilege of key revocation initialization[4] and certifying participant admission of the root CA with the regional CAs.[1]

Anonymity and Pseudonymity Enforcement in B-PKI: The Key Component for Enhancing V2X Privacy Preservation

Compared with the C-PKI, the B-PKI has many advantages in privacy preservation with advanced features, such as smart contracts, transaction data and on-chain data. Several prospective technologies applied to the B-PKI are secure multiparty computation, ZKF, and homomorphic concealment[1,2] (as shown in Table 3).

Integrating Blockchain With Existing CMS Components: A Promising Approach to Rapidly Deploy B-PKI and Maintain Backward Compatibility for V2X Authentication and Privacy-Preservation Platforms

While standardizing the B-PKI may take time, the fastest way to bring it into practice is to integrate its key components so as to enhance the CMS for specific applications. For example, Feng et al.[12] proposed a blockchain-assisted privacy-preserving authentication system that implements a public key in a smart contract and manages the linkability between a public key and a vehicle's identity. We summarize the differences among the proposals in terms of registration, validation, and revocation support in Table 4.

Challenges and Future Research Directions

Despite much potential for usage, blockchain technology in PKIs is still at a very early stage of its development cycle, and many of its fundamental components still require standardization. Other than the importance of stabilizing volatility in current blockchain protocols, we consider that a united authentication infrastructure for cross-domain applications and integration with the 5G infrastructure is necessary. The B-PKI can be the answer to satisfy both security and privacy in a united PKI platform. However, there are still several urgent challenges to deploying the B-PKI, as discussed next.

First, reliability and communication security between the CAs and independent participants in the B-PKI are more difficult to maintain perfectly. In the case of Bitcoin, participation is rewarded by receiving a small amount of bitcoin for providing the next block in the chain. Mollah et al.[2] presented a reward-and-penalty system based on nearby stations, which gives a negative rating to detected malicious vehicles; a greater negative rating indicates a low trust value in the vehicles. Vehicles with low trust values are unable to generate any new messages. However, implementing reward and profit according to the entities' contributions in a blockchain that solely carries out V2X authentication has yet to be seen. Also, in a consortium blockchain, a reliable temporary leader to handle the first write of transactions to the ledge is required, but a secure mechanism, such as e-voting,[8] to select a leader has not been well developed and is a topic for further study in the coming years.

Second, responding to audit the trustworthiness of massive messages in real time is still an open challenge for misbehavior detection in the B-PKI. Since V2X services are usually time critical, any delay in preventing an adversary from sharing spoofed messages may cause severe accidents[3] as a result of the confused awareness caused by wrong information. Blockchain operations, such as mining power of work, often demand massive memory and resources. A delay in processing these computing tasks can slow down the convergence of record synchronization among the nodes and thus prohibit responding to requests in time. Also, cloud-native storage can help to secure storage for massive vehicle data, although it may introduce a little more delay in retrieving processed records.[13] Exploiting the low latency of 5G V2X communications, edge intelligence, or PoS algorithms to optimize the time of response in the B-PKI will thus be a key issue for further studies.

Third, the large amount of data in V2X communications opens the door for implementing artificial intelligence (AI) for maintaining trust at best and for detecting the misbehavior of blockchain members. The power of big data analysis and AI can often be abused to undermine user privacy, for example, by analyzing heterogeneous data to determine the linkage or consistency of an entity. In V2X applications, large third parties may benefit from collecting vehicle data, including the privilege to access, analyze, correlate, and control the massive volume of trajectory history. However, clients have few options for controlling their personal data and their privacy during online transactions, including how, when, where, by whom, and what personal information is disclosed in each transaction. This problem becomes intensified in blockchain, as the private data included in a ledger are immutable, and a user's rights to control and rectify personal information decrease.

Fourth, the vulnerabilities of blockchain technology may threaten the potential to deploy the B-PKI. Since the consortium blockchain model is likely the choice to be used in the B-PKI, the issue of few nodes in the blockchain can pose security risks. Suppose an attacker can successfully exploit the blockchain's vulnerabilities, such as using bugs of smart contracts, to attack the blockchain (for example, with parity multisignature attacks, 51% attacks, blockwitholding, Sybil, or eclipse attacks). In that case, V2X authentication can be completely compromised. An attacker can then interrupt the consensus process, create new blocks, change the rewards, manipulate the transactions, and even make the blockchain completely untrusted. The PoW consensus is one resilient method to overcome such attacks.

In this article, we present an overview of the use of blockchain technology in enhancing V2X PKIs. Through a comparative review of the C-PKI and B-PKI, we highlight certain advantages of using blockchain technology to build scalable, secure, and efficient authentication schemes. Although the B-PKI is still at an early stage of development, its key features, such as decentralization, anonymity, and auditability capabilities, can significantly enhance system scalability, availability, and privacy preservation in V2X communications. Further, we also found that a full or even partial integration of several blockchain solutions into the C-PKI can significantly accelerate long-awaited features that have not been well supported by V2X security systems, for example, strong resistance against DDoS attacks and misbehaving CAs. Finally, we identify two promising areas for future research directions: 1) improving the security of smart contracts and stabilizing the reliability of consensus protocols while properly maintaining conditional anonymity and pseudonymity, and 2) proposing solutions to address interoperability among different B-PKI platforms. ■

Acknowledgments

This work was supported in part by the Ministry of Science and Technology (MOST) of Taiwan, under grant MOST 110-2811-E-194-501-MY2, and in part by the Ministry of Education and Training of Vietnam and Thai Nguyen University, under grant B2021-TNA-02. Van-Linh Nguyen is the corresponding author.

References

1. Y. Li, Y. Yu, C. Lou, N. Guizani, and L. Wang, "Decentralized public key infrastructures atop blockchain," *IEEE Netw.*, vol. 34, no. 6, pp. 133–139, Nov./Dec. 2020, doi: 10.1109/MNET.011.2000085.
2. M. B. Mollah *et al.*, "Blockchain for the internet of vehicles towards intelligent transportation systems: A survey," *IEEE Internet Things J.*, vol. 8, no. 6, pp. 4157–4184, Oct. 2020, doi: 10.1109/JIOT.2020.3028368.
3. "Intelligent transport systems (ITS); Security; Prestandardization study on pseudonym change management," ETSI, Sophia Antipolis, France, ETSI TS 103 415, Apr. 2018.
4. *IEEE Standard for Wireless Access in Vehicular Environments (Wave)–Certificate Management Interfaces for End Entities*, IEEE Standard 1609.2.1-2020, Dec. 2020.
5. M. Fallgren, M. Dillinger, T. Mahmoodi, and T. Svensson, Eds. *Cellular V2X for Connected Automated Driving*, vol. 270. Hoboken, NJ, USA: Wiley, Apr. 2021, pp. 63–90.
6. T. Giannetsos and I. Krontiris, "Securing V2X communications for the future: Can PKI systems offer the answer?" in *Proc. 14th Int. Conf. Availability, Rel. Secur. (ARES '19)*, Association for Computing Machinery, Aug. 2019, pp. 1–8, doi: 10.1145/3339252.3340523.
7. Z. Lu, Q. Wang, G. Qu, H. Zhang, and Z. Liu, "A blockchain-based privacy-preserving authentication scheme for VANETs," *IEEE Trans. Very Large Scale Integr. (VLSI) Syst.*, vol. 27, no. 12, pp. 2792–2801, Aug. 2019, doi: 10.1109/TVLSI.2019.2929420.
8. D. Zheng, C. Jing, R. Guo, S. Gao, and L. Wang, "A traceable blockchain-based access authentication system with privacy preservation in VANETs," *IEEE Access*, vol. 7, pp. 117,716–117,726, Aug. 2019, doi: 10.1109/ACCESS.2019.2936575.
9. A. Ikram, M. Gervais, E. Ahene, and F. Li, "A blockchain-based certificateless public key signature scheme for vehicle-to-infrastructure communication in VANETs," *J. Syst. Archit.*, vol. 99, pp. 101–136, Oct. 2019, doi: 10.1016/j.sysarc.2019.101636.
10. X. Wang, P. Zeng, N. Patterson, F. Jiang, and R. Doss, "An improved authentication scheme for internet of vehicles based on blockchain technology," *IEEE Access*, vol. 7, pp. 45,061–45,072, Apr. 2019, doi: 10.1109/ACCESS.2019.2909004.
11. S. Bao *et al.*, "Pseudonym management through blockchain: Cost-efficient privacy preservation on intelligent transportation systems," *IEEE Access*, vol. 7, pp. 80,390–80,403, Jun. 2019, doi: 10.1109/ACCESS.2019.2921605.
12. Q. Feng, D. He, S. Zeadally, and K. Liang, "BPAS: Blockchain-assisted privacy-preserving authentication system for vehicular *Ad Hoc* networks," *IEEE Trans. Ind. Informat.*, vol. 16, no. 6, pp. 4146–4155, Oct. 2019, doi: 10.1109/TII.2019.2948053.
13. J. Kang *et al.*, "Blockchain for secure and efficient data sharing in vehicular edge computing and networks," *IEEE Internet Things J.*, vol. 6, no. 3, pp. 4660–4670, Jun. 2019, doi: 10.1109/JIOT.2018.2875542.

14. J. Noh, S. Jeon, and S. Cho, “Distributed blockchain-based message authentication scheme for connected vehicles,” *Electronics*, vol. 9, no. 1, p. 74, Jan. 2020, doi: 10.3390/electronics9010074.
15. S. Matsumoto and R. M. Reischuk, “IKP: Turning a PKI around with blockchains,” in *Proc. IEEE Symp. Security Privacy (SP)*, San Jose, CA, USA, May 2017, doi: 10.1109/SP.2017.57.

Edy Kristianto is a lecturer in the Department of Computer Science, Krida Wacana Christian University, Daerah Khusus Ibukota Jakarta, 11470, Indonesia. He is currently pursuing a Ph.D. in computer science and information engineering at National Chung Cheng University, Minhsiung, Chiayi, 621, Taiwan. His primary research interests include computer security and machine learning. Kristianto received a B.S. from the Department of Informatics, Duta Wacana Christian University, iIndonesia and an M.Eng. from the Department of Electrical Engineering, Gadjah Mada University, Indonesia. Contact him at edy108p@cs.ccu.edu.tw.

Van-Linh Nguyen is a postdoctoral fellow at National Chung Cheng University, Minhsiung, Chiayi, 621, Taiwan. He has also worked as a lecturer in the Department of Information Technology, Thai Nguyen University of Information and Communication Technology, Vietnam, since 2012. His research interests include cybersecurity, network/edge intelligence, autonomous driving, and vehicular networks. Nguyen received a Ph.D. in computer science and information engineering from National Chung Cheng University, Minhsiung, Chiayi, Taiwan. Contact him at nvlinh@ictu.edu.vn.

Po-Ching Lin is a professor in the Department of Computer Science and Information Engineering, National Chung Cheng University, Minhsiung, Chiayi, 621, Taiwan. His research interests include network security, network traffic analysis, and performance evaluation of network systems. Lin received a Ph.D. in computer science from National Chiao Tung University, Hsinchu City, Taiwan. He is a Member of IEEE. Contact him at pclin@cs.ccu.edu.tw.

Digital Object Identifier 10.1109/MSEC.2022.3183368