# A Blockchain-Based Privacy-Preserving Payment Mechanism for Vehicle-to-Grid Networks

Feng Gao, Liehuang Zhu, Meng Shen, Kashif Sharif, Zhiguo Wan, and Kui Ren

## Abstract

As an integral part of V2G networks, EVs receive electricity from not only the grid but also other EVs and may frequently feed the power back to the grid. Payment records in V2G networks are useful for extracting user behaviors and facilitating decision-making for optimized power supply, scheduling, pricing, and consumption. Sharing payment and user information, however, raises serious privacy concerns in addition to the existing challenge of secure and reliable transaction processing. In this article, we propose a blockchain-based privacy preserving payment mechanism for V2G networks, which enables data sharing while securing sensitive user information. The mechanism introduces a registration and data maintenance process that is based on a blockchain technique, which ensures the anonymity of user payment data while enabling payment auditing by privileged users. Our design is implemented based on Hyperledger to carefully evaluate its feasibility and effectiveness.

## Introduction

Vehicle-to-grid (V2G) networks, which involve electric vehicles (EVs) as both energy suppliers and consumers, are rapidly emerging as a substantial enhancement of future smart grids. In V2G networks, bidirectional electricity transmissions among all participants (e.g., EVs and the grid) generate a large number of payment records of electricity usage, which can be shared to provide valuable services, such as load forecasting, price prediction, optimal energy consumption scheduling, and EV ancillary service behavior modeling [1–3]. However, sharing of payment records may raise privacy concerns of sensitive information leakage, such as identities, locations, and charging or discharging volumes of EVs. Therefore, trade-offs between privacy protection and information disclosure should be carefully analyzed and balanced in V2G networks.

Traditional payment methods, such as credit cards and PayPal transfers, require association with numerous third parties. This association generates distributed payment record information with multiple organizations, which can be shared without the consent or willingness of users. A variety of anonymous payment mechanisms [4–6] enable privacy protection of EVs, a majority of which are centralized and use a trusted third-party to process payments. Although they satisfy the privacy requirements of protecting participant identities, they cannot conceal identities when the payment records are shared among multiple entities for analysis. In addition, the centralized design may encounter the risk of a single point of failure.

As an emerging and promising technique in digital currency systems [7], the blockchain has the advantages of transaction anonymity, credibility, and high distribution, which motivates us to explore its usage in establishing an anonymous payment mechanism while satisfying data sharing requirements.

To achieve this goal, we address two main challenges. The first challenge is simultaneously guaranteeing the reliability and efficiency of transactions. For instance, as one of the most extensively employed blockchain-based applications, Bitcoin only supports seven transactions per second and has limited scalability. A permissioned (private) blockchain technique, such as the Hyperledger [8], achieves better scalability but cannot guarantee the reliability of transactions because it records agreed-upon transactions into a ledger without verifying whether a transaction is valid. The second challenge is the auditability of blockchain-based systems. Users of these systems are encouraged to generate a new pseudonym for each transaction to protect their identities from potential attackers. This privacy-enhancing mechanism establishes a barrier to identify malicious transactions. This limitation has been highlighted in ransomware attacks (WannaCry, May 2017), where ransom transactions were sent to Bitcoin accounts that are not easily traced back to malicious users.

In this article, we introduce various payment scenarios in V2G networks and identify existing problems to emphasize the conflicts between privacy protection and data sharing. Following this, a blockchain-based privacy-preserving payment mechanism for V2G networks is proposed. We leverage a registration process based on digital signatures to protect the privacy of traders while enabling payment auditing by privileged users. Based on Hyperledger, we propose a new type of transaction structure that is customized for payments in V2G networks and a corresponding transaction verification algorithm that guarantees reliable transactions with increased scalability. A proof-of-concept prototype is presented for the proposed mechanism and its feasibility and effec-

Digital Object Identifier:
10.1109/MNET.2018.1700269

*Feng Gao, Liehuang Zhu, Meng Shen (corresponding author), and Kashif Sharif are with Beijing Institute of Technology; Zhiguo Wan is with Shandong University, China; Kui Ren is with Zhejiang University China.*

0890-8044/18/$25.00 © 2018 IEEE

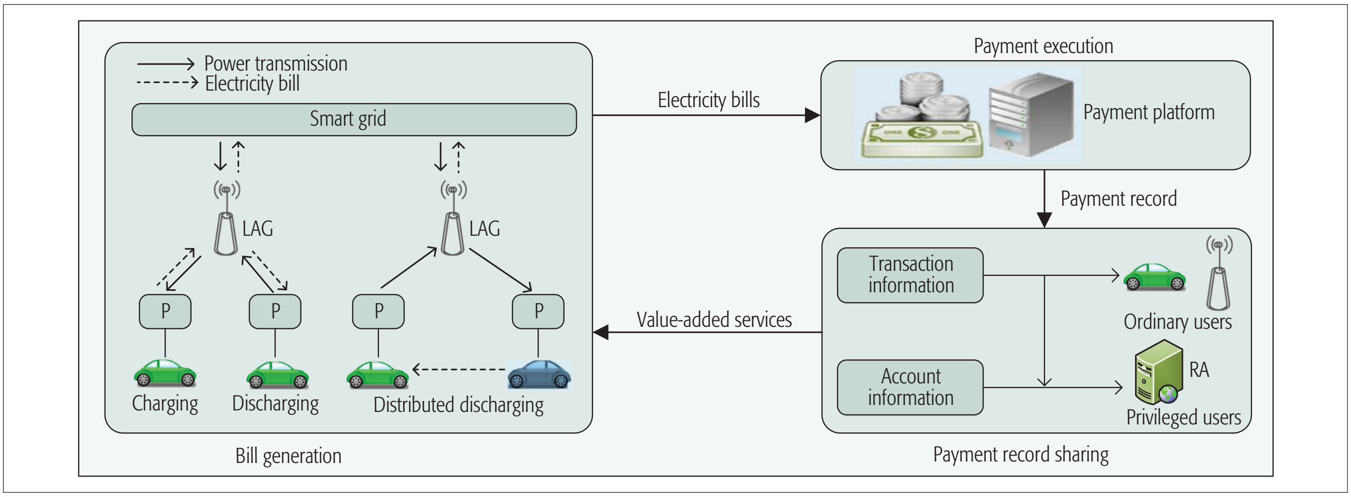


FIGURE 1. Reference model of payment scenarios in V2G networks.

tiveness are demonstrated by experiments. We elaborate on challenges and opportunities for future research investigating blockchain-based payment mechanisms.

## Reference Model

### Payment Scenarios

In V2G networks, frequent bidirectional interactions occur between EVs and a smart grid, in terms of electricity transmissions and payment bills. These bills are sent to a payment platform that is responsible for completing payments and sharing the records with all stakeholders. Based on these payment records, some users in V2G networks can offer value-added services to other participants, such as electricity pricing, optimal charging and discharging strategies. For instance, EV owners can obtain advice about selecting a cost-effective time (e.g., off-peak hours) to charge their EVs. The entire electricity payment process in V2G networks can be divided into three phases, as shown in Fig. 1.

**Bill Generation:** EVs gain access to V2G networks by parking lot-dedicated facilities and provide auxiliary services to the smart grid under the control of local aggregators (LAGs) [5]. As shown in the left part of Fig. 1, EVs have three states: charging, discharging, and distributed discharging. Charging is initiated by an EV, where power is transferred from the smart grid to the EV, which needs to pay the electricity bill to the smart grid. Discharging is initiated by the smart grid when the grid is overloaded during peak hours of user demands. EVs can mitigate power shortages by discharging to the grid and receive financial rewards from the smart grid. Distributed discharging is initiated by one or more EVs when their battery capacities are lower than a certain threshold. Unlike the charging state, an EV with sufficient power will temporarily act as an energy supplier to EVs with power shortages, where the latter should pay electricity bills to the supplier EV. In these scenarios, an EV can either be a payer or a payee, which requires a payment mechanism to support two-way payments.

**Payment Execution:** The upper right part of Fig. 1 shows the process of payment execution. The payment platform is responsible for executing payment upon receiving electricity bills and offering detailed payment records to users in V2G networks. The payment mechanism should provide a reliable transaction to ensure that the transaction is genuine and undeniable. In addition, the payment mechanism should support auditing to resolve payment disputes.

**Payment Record Sharing:** The payment record sharing process is exhibited in the bottom right of Fig. 1. The payment records contain two types of data: transaction information and account information. The transaction information includes total price and unit price, which can be employed to calculate the electricity demand. The account information contains the identities of the traders. Ordinary users (e.g., EVs and LAGs) can obtain the transaction information to provide value-added services, such as forecasting the trend of electricity usage. However, to protect user privacy, account information is anonymous. Since privileged users such as the registration authorities (RAs) are responsible for auditing transactions and identifying malicious users, they need to know details of the transaction and account information. Therefore, the payment mechanism should protect user privacy for the condition of data sharing and enable auditing by privileged users.

### Threat Model

Numerous security challenges arise in electric transaction systems. In this article, we focus on two types of threats: privacy disclosure and unreliable payments.

**Privacy Disclosure:** In V2G networks, EVs are usually connected to LAGs via insecure wireless links. Thus, payment information may be eavesdropped by an attacker. Because payment records will be publicly shared among all participants, potential attackers may speculate sensitive information about EVs, such as charging locations and periods. In addition, an attacker can obtain privacy information from payment records by colluding with malicious users. For instance, a malicious EV owner can send its location information and payment records to an attacker, from which the locations of other EV owners can be inferred.

**Unreliable Payments:** An attacker attempts to cheat honest users (or an LAG) by creating unreliable payments, such as fake payments and

The main task of the registration process is to submit a user-generated account to the RA for authentication and registration. Only accounts that have been signed by the RA are legitimate and acceptable in the payment mechanism.

double-spending (i.e., an error in a digital cash scheme where digital currency is spent at least twice). Detecting and rejecting unreliable payments in a fully distributed system without a trusted third-party are difficult.

### Design Goals

We aim to design an anonymous payment mechanism for V2G networks, which simultaneously satisfies the requirements of data sharing and privacy protection. The design goals are summarized as follows:

**Privacy Preservation of Data Sharing:** Complete payment records, rather than statistics, should be shared among all participants in a secure and efficient manner. The adversary cannot deduce the real identities of traders from payment records.

**Effective Audit of Anonymous Transactions:** Although payment records are anonymous for EVs and LAG, an authorized auditor should be able to obtain the real identities of traders in an anonymous transaction, which should enable their identities to be traced to EVs that participate in malicious transactions. The auditor should not be able to alter transactions.

**Reliable and Efficient Payments:** Efficient blockchain techniques should be selected and improved to achieve a new payment mechanism that supports reliable and efficient payments. The techniques should be capable of discovering and rejecting unreliable payments, such as double payments, fake payments, and payment revocation. In addition, the payment mechanism should have a better scalability than current solutions to satisfy the practical transaction requirements in V2G networks.

## Existing Payment Mechanisms for V2G Networks

During the past decade, numerous research efforts have focused on V2G networks [46]. We briefly summarize recent achievements in anonymous payment mechanisms that can protect the privacy of EVs.

Yang *et al.* [4] proposed the mechanism P2, which leverages a blind signature to achieve anonymous reward payments. Wang *et al.* [5] proposed a traceable and privacy-preserving scheme, which had a permit-based strategy that was similar to P2 with a stronger security guarantee. These anonymous payment mechanisms generally rely on a trusted third-party, which encounters a variety of threats, such as a single point of failure and internal and external intrusions. Man *et al.* [6] and Zhao *et al.* [9] provided decentralized anonymous payment mechanisms without relying on a trusted third-party. These mechanisms require the deployment of a trusted platform module on each EV, which distributes the payment data that are stored on different EVs. Therefore, intermediate nodes and billing servers are not capable of learning specific payment information. Although user privacy is effectively protected, data sharing, such as payment information, is difficult and scattered among different EVs.

## Overview of Blockchain

Blockchain is a distributed database that maintains an ever-growing list of digital deals [7] and provides a secure method for online transactions among anonymous participants. Therefore, this database is inherently consistent with the need to complete a reliable anonymous payment mechanism in the absence of a credible central server. Several pioneering projects have applied blockchain to energy-related transactions [10]. A typical blockchain system usually consists of three main components, which are described as follows:

**Blockchain Network:** A peer-to-peer network that is composed of many nodes (independent host that runs the blockchain client). All participating nodes have the same status to avoid the risk of a single point of failure.

**Blockchain Transactions:** A transaction records the process of data exchange among users, including addresses of senders and receivers and transaction content. An address is a pseudonym that is employed in blockchain transactions and that resembles a bank card number. The transaction content is defined according to specific application scenarios. In a digital currency application, the transaction content represents the transaction amount, and may represent a string or a certificate ID in other applications. In this article, the transaction content should be relevant to the electricity transmission.

Each transaction is broadcasted rather than directly sent to a target node (i.e., the receiver) in a blockchain network. The target node can eventually receive a transaction from the network without having to directly contact the sending node. Therefore, tracking the transaction sources by eavesdropping, which helps to achieve anonymity, is difficult.

**Global Ledger:** A global ledger is used to store all transactions in a blockchain system, which usually comprises a chain of blocks. Each block records a certain number of transactions. A new block is attached to the global ledger by recording the hash value of the previous block. Thus, the ledger forms a data chain from the initial block to the latest block.

Each node in a blockchain network maintains a unique global ledger and synchronizes with other nodes via a consensus algorithm. When a transaction is executed, the payer node broadcasts the transaction information in the blockchain network, which selects a special node according to the consensus algorithm to authenticate and write the transaction into the global ledger. The remaining nodes synchronize their global ledgers through the blockchain network. The consensus algorithm ensures that all legitimate nodes store the same global ledger.

## Blockchain-Based Privacy-Preserving Payment Mechanism

We propose a decentralized anonymous payment mechanism that enables privacy-preserving data sharing for EVs in V2G networks coupled with a registration process to achieve the design goals.

### Description of System Entities

**Users:** The users include EVs and the entities that participate in the transaction process, e.g., charging facilities. They can act as either of the two roles in a payment, namely, payers and payees. Each user installs a blockchain client to handle the payment transaction and maintain a global ledger. Most modern EVs are equipped with computational and communication functions that can be employed to run a blockchain client module.

**Registration Authority (RA):** An RA serves as an authorized auditor, for example, an arbitration authority, that is responsible for account registration and payment record auditing. An RA installs a blockchain client to maintain a global ledger that contains all payment records and maintains a certificate repository that stores all registered accounts and corresponding identities. Therefore, an RA is considered to be a secure entity, which can view not only all payment records but also the real identity of anyone in the anonymous payment record.

**Blockchain Network:** A blockchain network refers to the blockchain infrastructure and the communication and consensus mechanisms. In the proposed payment mechanism, the blockchain network works in the same manner as described below, with the exception of the transaction structure and the transaction verification method.

### Architecture and Functionality

The blockchain-based payment mechanism consists of several components, as shown in Fig. 2.

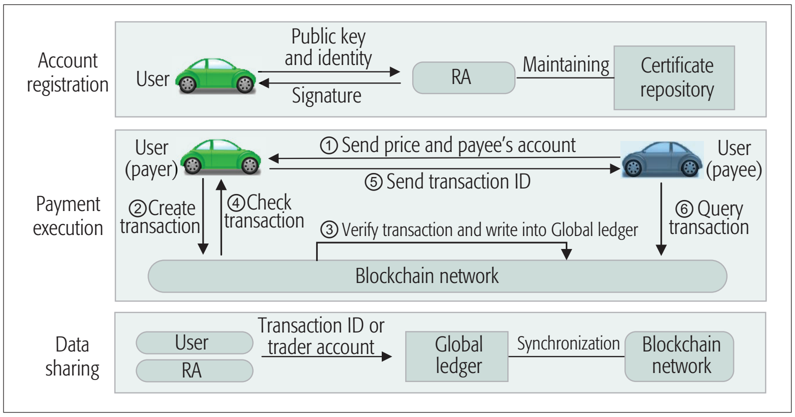


FIGURE 2. Architecture and workflow of the proposed blockchain-based payment mechanism.

**Account Registration:** The main task of the registration process is to submit a user-generated account to the RA for authentication and registration. Only accounts that have been signed by the RA are legitimate and acceptable in the payment mechanism.

The registration process involves the following steps. A user creates a pair of keys ($P_k$_user; $S_k$_user) using asymmetric encryption algorithms, such as RSA or ECC, and then sends $P_k$_user and its identity information (e.g., personal ID or driver's license) to the RA. After checking the identity, the RA replies to the user with the signature δ, which is generated using the private key $S_k$_RA, as depicted in Eq. 1. The RA stores $P_k$_user and the corresponding identity in the certificate repository. The user generates a legal account in conjunction with $P_k$_user and δ. The legal account format is shown in Eq. 2. We assume that the RA's public key $P_k$_RA can be obtained from a public channel. Thus, each user can leverage $P_k$_RA to verify an account, as illustrated in Equation (3), where υ = 1 represents a valid signature and a legal account, and υ = 0 otherwise.

The registration process involves the following steps. A user creates a pair of keys ($P_k$_user; $S_k$_user) using asymmetric encryption algorithms, such as RSA or ECC, and then sends $P_k$_user and its identity information (e.g., personal ID or drivers license) to the RA. After checking the identity, the RA replies to the user with the signature δ, which is generated using the private key $S_k$_RA, as depicted in Eq. 1. The RA stores $P_k$_user and the corresponding identity in the certificate repository. The user generates a legal account in conjunction with $P_k$_user and δ. The legal account format is shown in Eq. 2. We assume that the RA's public key $P_k$_RA can be obtained from a public channel. Thus, each user can leverage $P_k$_RA to verify an account, as illustrated in Eq. 3, where υ = 1 represents a valid signature and a legal account, and υ = 0 otherwise.

$$\delta = \mathtt{Sign}(S_k\_\mathtt{RA};\ P_k\_\mathtt{user}) \tag{1}$$

$$\mathtt{account} = (P_k\_\mathtt{user},\ \delta) \tag{2}$$

$$\upsilon = \mathit{Verify}(P_k\_\mathtt{RA}; \mathit{account}.P_k\_\mathtt{user}; \mathit{account}.\delta) \tag{3}$$

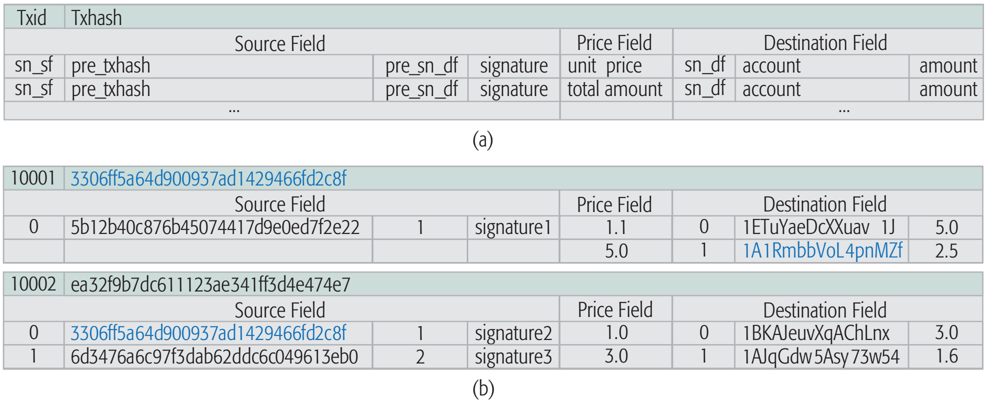
Users can apply for signatures from the RA for multiple public keys at once and reapply when these accounts are exhausted.

**Payment Execution:** This stage ensures that the payer succeeds in paying an electricity bill and enables the payee to verify the receipt. In the proposed payment mechanism, a payment is realized as a blockchain transaction. As a result, the payment execution is actually the process of transactions that are being verified and written into the global ledger.

The payee sends its account and the unit price to the payer. The account is generated during the registration process, which contains the signature information provided by the RA. The payee can use a different account for each transaction to protect privacy. Then, the payer calculates the electricity bill, creates a transaction via its blockchain client, and eventually sends the transaction to the blockchain network. After receiving the transaction, the blockchain network will verify the transaction and write the legal transaction into the global ledger. The payment is completed once the corresponding transaction is recorded in the global ledger.

The payer checks the global ledger until the payment is completed. Then, the payer sends the transaction ID to the payee. If a transaction with the accurate account and amount is identified, the payee begins to provide services, such as electricity transmission.

The payment process is performed more frequently than the registration process, and the EVs are usually equipped with limited computation and communication capabilities, which causes a lack of payment information protection. We have designed an appropriate mechanism to



| Txid | Txhash | | | | | | |
|---|---|---|---|---|---|---|---|
| Source Field | | | | Price Field | Destination Field | | |
| sn_sf | pre_txhash | pre_sn_df | signature | unit price | sn_df | account | amount |
| sn_sf | pre_txhash | pre_sn_df | signature | total amount | sn_df | account | amount |
| ... | | | | | ... | | |

(a)

| 10001 | 3306ff5a64d900937ad1429466fd2c8f | | | | | | |
|---|---|---|---|---|---|---|---|
| Source Field | | | | Price Field | Destination Field | | |
| 0 | 5b12b40c876b45074417d9e0ed7f2e22 | 1 | signature1 | 1.1 | 0 | 1ETuYaeDcXXuav 1J | 5.0 |
| | | | | 5.0 | 1 | 1A1RmbbVoL4pnMZf | 2.5 |

| 10002 | ea32f9b7dc611123ae341ff3d4e474e7 | | | | | | |
|---|---|---|---|---|---|---|---|
| Source Field | | | | Price Field | Destination Field | | |
| 0 | 3306ff5a64d900937ad1429466fd2c8f | 1 | signature2 | 1.0 | 0 | 1BKAJeuvXqAChLnx | 3.0 |
| 1 | 6d3476a6c97f3dab62ddc6c049613eb0 | 2 | signature3 | 3.0 | 1 | 1AJqGdw5Asy73w54 | 1.6 |

(b)

FIGURE 3. Examples illustrating the transaction structure for the payments in V2G networks.

Since the account in payment records is a pseudonym, EVs and malicious users cannot link the payment record to a specific user, which prevents privacy disclosure. The RA can obtain each account's identity information from the certificate repository to effectively audit payment records.

ensure transaction reliability and privacy for EVs in an unreliable communication channel, which is described in the next section.

**Data Sharing:** The data sharing process focuses on the sharing strategy of payment records. In the proposed payment mechanism, all legal payment records are written to the global ledger. Since the global ledger is accessible by all participants, a member who wants to view or query the payment records, can simply synchronize the global ledger in their blockchain client.

Since the account in payment records is a pseudonym, EVs and malicious users cannot link the payment record to a specific user, which prevents privacy disclosure. The RA can obtain each account's identity information from the certificate repository to effectively audit payment records.

## Transaction and Verification

The payment process involves several blockchain techniques, such as information delivery, trading, and consensus mechanisms, which are equivalent to the blockchain techniques that are readily available in the existing blockchain systems. We focus on the design of the transaction structure and the transaction verification method, which are crucial components for achieving our design goals that differ from existing blockchain systems.

To obtain better scalability, we select Hyperledger [8] instead of Bitcoin [7] to implement the proposed payment mechanism. However, Hyperledger is not designed for digital cash, where each Hyperledger transaction is recorded in a global ledger without verifying its legality. As a result, we design a new type of transaction structure and a corresponding verification method based on Hyperledger to guarantee the reliability of payment transactions.

**Transaction Structure:** Inspired by Bitcoin, we design a transaction structure for reliable payment in V2G networks, as illustrated in Fig. 3a. Each transaction has a unique ID *txid* and a unique hash value *txhash* as an index of the transaction. The contents of a transaction consist of three parts: the source field, the price field, and the destination field.

The source field lists one input or multiple inputs in this transaction. An input is a reference to an output from a previous transaction and is denoted by ⟨*sn_sf*, *pre_txhash*, *pre_sn_df*, *signature*⟩. Here, *sn_sf* is the serial number of the input in the source field of this transaction; *pre_txhash* is the *txhash* value of the referenced transaction; and *pre_sn_df* and *signature* are the serial number and the owner's signature, respectively, of the specific output in the referenced transaction. The signature can be used by anyone to verify the payer's ownership of this input.

The price field indicates the unit price (i.e., the electricity price at the payment time) and the total amount of this payment. A validation process is performed to ensure that the sum of all input values is not less than the total amount.

The destination field lists one output or multiple outputs. An output is a reference to a payee's account and is denoted by ⟨*sn_df*, *account*, *amount*⟩, where *sn_df* is the serial number of the output in the destination field of this transaction, *account* is the payee's account, and *amount* is the value of this output. All outputs share the combined value of the inputs in this transaction. An account of the payer can also be listed as an output to receive *change* when the combined input value exceeds the total amount of this payment.

As illustrated in Fig. 3b, the input with *sn_sf* = 0 and *pre_txhash* = *3306ff5a64d900937ad1429466fd2c8f* in Transaction 10002 imports values from the output with *sn_df* = 1 in Transaction 10001. Anyone can obtain the public key from the payee's account in Transaction 10001 and verify *signature*2.

**Transaction Verification Method:** Verification is used to guarantee payment reliability. We propose a verification method to reject forged transactions without authority for input accounts and illegal transactions with illegal accounts. The workflow of the verification method is described as follows:

- Verifying whether the transaction information satisfies the format requirements.
- Verifying whether all accounts are legitimate, including input and output accounts. The verifier can use the RA's public key to verify the signature of the account to check whether the account is legal.

- Verifying whether all signatures in the source field are correct. The public key required to validate the signature is obtained from the corresponding output account in the transaction denoted by *pre_txhash* and *pre_sn_df*.
- Verifying whether the input amount is greater than or equal to the total output amount.

## System Design Analysis

**Data Sharing:** In Bitcoin and Hyperledger, the transaction data are stored by all participants. The main difference is that Bitcoin is a permissionless blockchain that enables anyone to join the Bitcoin network and freely obtain all payment records, whereas the Hyperledger is a permissioned blockchain, in which only authorized users are involved.

The proposed mechanism is built on Hyperledger, where the payment records are only easily shared among registered members, such as EVs, LAGs, and the RA. For instance, a member can obtain a unique global ledger that contains all payment records by running a blockchain client.

**Privacy Preserving:** Bitcoin primarily relies on pseudonyms to realize anonymous transactions. However, traffic analysis attacks can easily identify a source node that creates a transaction [11] and infer trading rules of the pseudonyms by the transaction records in the global ledger [12]. Thus, these attacks reduce the anonymity of pseudonyms and the attacker may infer the identity of a pseudonym.

In Hyperledger, stealing private data is difficult for external attackers because only authorized users can gain access to the blockchain network. The internal attackers, such as malicious authorized users, can infer the identity of pseudonyms by analyzing transaction data in the global ledger.

The proposed mechanism introduces a centralized RA to store the corresponding identity information of pseudonyms to satisfy the audit requirement. The RA simply provides the identity information in the case of a transaction dispute, and therefore, does not frequently participate in the payment execution process. As a result, the RA is capable of handling internal attacks compared with traditional centralized payment mechanisms. Compared with Bitcoin, only authorized users can obtain transaction information, which can protect against external attackers. A user in our mechanism can register multiple accounts during a single registration process and use a different account for each transaction. This one-time account strategy can spread the user's trading rules among different accounts, which inhibits attacks that are based on transaction data analysis.

**Auditing:** In Bitcoin and Hyperledger, auditing is difficult because auditors cannot easily obtain the identity information behind a transaction.

Our mechanism supports effective audits by introducing a registration process and an efficient verification method. By the registration process, the RA maintains a certificate repository that contains all legal accounts and their identity information. Using the transaction verification method, only transactions created by legal accounts can be recorded in the global ledger. Thus, the RA is able to obtain the identity information behind any transaction, which enables auditing.

The proposed mechanism is built on Hyperledger, where the payment records are only easily shared among registered members, such as EVs, LAGs, and the RA. For instance, a member can obtain a unique global ledger that contains all payment records by running a blockchain client.

**Reliable Payment:** A Bitcoin system is designed for digital currency trading and supports reliable payments. The original Hyperledger was not designed for digital cash, and each transaction is directly recorded in a global ledger without verifying its legality.

In our mechanism, we propose a new type of transaction structure and a corresponding verification algorithm that is based on the original Hyperledger system to enable reliable payments. Once the transaction is recorded in the global ledger, it cannot be tampered, which ensures that previously recorded transactions are reliable. Each input in a transaction is reliable and legally authorized by clearly identifying the source of the input and the signature of its owner. Since the global ledger is public, all nodes in the blockchain network can use historical transactions to detect whether an output in a transaction has been previously employed, which helps to prevent a double spending attack.

## Proof-of-Concept and Evaluation

We implement a prototype of the proposed payment mechanism based on Hyperledger (Fabric V0.6) [8]. We employ the OS-level virtualization technique Linux Containers (LXC) to emulate four V2G users with moderate computing and storage capacities, where each user is equipped with an Inter(R) Core(TM) 2.5 GHz 64-bit CPU, 8 G DDR3L RAM, and 1T 5400 rpm HDD. The four users include a payer, a payee, an RA, and an ordinary user for transaction verification.

The time consumption of the registration process is primarily determined by the public-private key pair generation process on the user side and the signature process on the RA side. Therefore, we simulate the time overhead of cryptographic schemes using the Elliptic Curve Digital Signature Algorithm (ECDSA) on the 256-bit curve secp256k1. The average execution time for generating a new public-private key pair and signing a public key is approximately 3.16 ms and 3.45 ms, respectively.

Figure 4a shows the performance of cryptographic schemes in the registration process. The processing time of both schemes linearly increases with an increase in the number of accounts. We assume that each user adopts 10 new public keys per day and performs the registration process on a monthly basis, which approximates the transaction frequency of an individual EV in V2G networks. Thus, each registration process contains approximately 300 public-private key pair generations and 300 signatures, which requires approximately 1.935 seconds.

In the payment process, we focus on the transaction processing speed and transaction confirmation time. The former refers to the number of transactions that the payment mechanism conducts per second, whereas the latter refers to the time interval from the submission of a transaction by a payer to the record of this transaction in the global ledger.

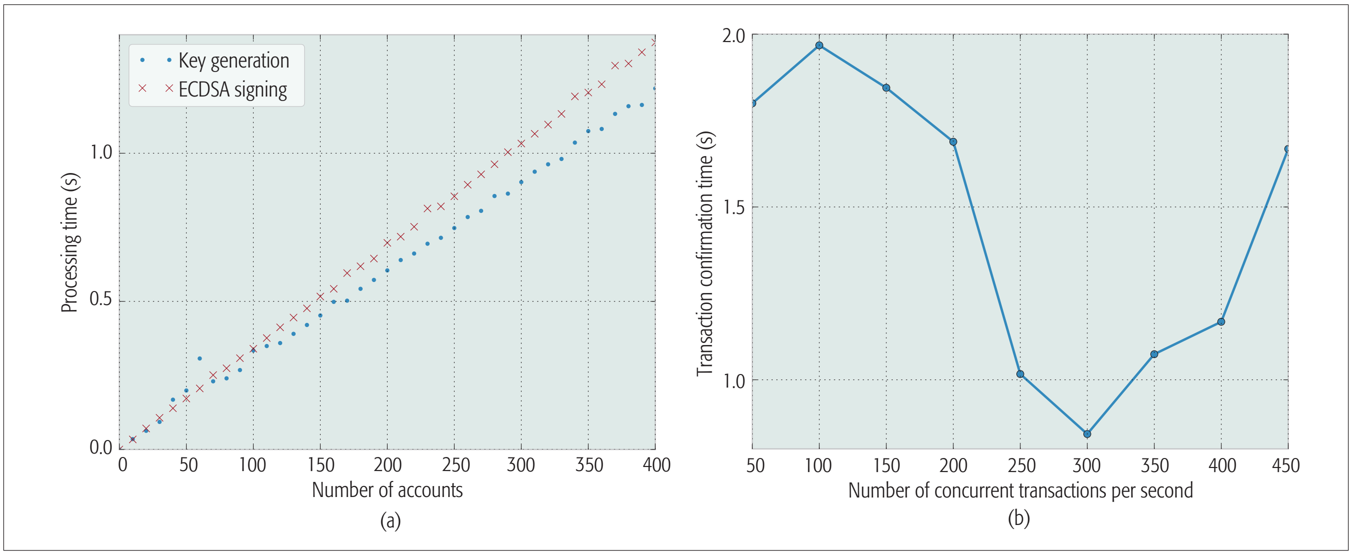


FIGURE 4. Performance Evaluation: a) computation time of cryptographic schemes; b) transaction confirmation time of the proposed mechanism.

The transaction processing speed and confirmation time in typical blockchain systems are significantly lower than the transaction processing speed and confirmation time in a traditional centralized architecture. For example, the Bitcoin system merely supports seven transactions per second and the confirmation time requires almost one hour.

To substantially increase the transaction speed, we employ the Hyperledger to implement the payment mechanism and adopt the Byzantine algorithm to attain a consensus [13]. Our implementation is capable of achieving 300 transactions per second. We discover that the transaction confirmation time can be reduced to less than one second when the configuration parameters in the Hyperledger are fine-tuned, as shown in Fig. 4b.

The x-axis in Fig. 4b represents the number of concurrent transactions per second, and the y-axis represents the average transaction confirmation time. The curve consists of three stages. In the first stage (i.e., 50–250), the time decreases as the transaction throughput increases. This trend is caused by the batch processing mechanism of the blockchain system, that is, when the volume of concurrent transactions is relatively small, the system has to wait for a predefined number of transactions to be recorded in a single block. In the second stage (i.e., 250-350), the system achieves the shortest confirmation time. In the last stage, the transaction confirmation time begins to increase because a large number of transactions cannot be confirmed in a timely manner when the transaction volume exceeds the processing capability.

From Fig. 4b, we can conclude that the transaction confirmation time can be maintained within two seconds on the condition that the number of concurrent transactions is less than the maximum capacity, which satisfies the general requirements.

Our system outperforms Bitcoin [7] and Ethereum [14] in terms of transaction throughput and transaction confirmation time. As shown in Table 1, Bitcoin supports seven transactions per second, and requires 600 seconds for each transaction to be recorded in the global ledger. Ethereum achieves 25 transactions per second and 10 seconds of confirmation time.

| Systems | Throughput (T/s) | Confirmation time (s) |
|---|---|---|
| Bitcoin | 7 | 600 |
| Ethereum | 25 | 10 |
| Proposed scheme | 300 | 2 |

TABLE 1. Performance comparison among different blockchain systems.

In the data sharing process, we focus on storage requirements rather than time consumption because a user can directly view the local global ledger after synchronizing the latest payment records. In the blockchain network, each node retains a copy of the global ledger, which contains all transaction records and some additional parameters. Because the principal storage consumption comprises the transaction data, we estimate the storage consumption of each node based on the size of a single transaction and the number of transactions per day. We assume that the regular transaction contains two inputs and two outputs.

According to the transaction structure in Fig. 3, we can calculate the size of a transaction, as exhibited in Table 2. The size of a transaction is 536 bytes. Assume that a V2G network contains 10,000 EVs, and each EV creates 10 transactions per day, which creates approximately 100,000 payment records per day with a transaction data size of approximately 54 MB per day or 19 GB per year.

## Research Direction and Opportunities

Incorporating the blockchain technique into V2G networks is a promising research topic. However, several challenges in this direction remain, which create additional opportunities for future studies. Based on the work presented in this article, we describe three major avenues that need immediate responses from the research community.

**Diverse Privacy Demands:** In this article, we achieve basic anonymous transactions without considering more complex billing schemes, such as membership benefit policies and cash feedback strategies, which require more sophisticated and targeted privacy policies. With the rapid development of blockchain, many different mechanisms will be designed to satisfy different privacy requirements. As an example, Ethereum provides Turing's complete scripting language, which can be utilized to implement traditional privacy-preserving algorithms in a decentralized environment. The analysis of more sophisticated scripting techniques and associated architectural changes is needed [15].

**Appropriate Pricing Policy:** This factor is important for attracting EVs to adopt the blockchain-based payment mechanism. Blockchain supports high-frequency, low-value, and reliable transactions, which facilitate the realization of more flexible and efficient pricing policies. For instance, appropriate pricing policy enables accurate billing for auditing the amount of power transmission, which can be used to support customized power purchasing and selling prices for EVs.

**Efficiency and Practicability:** Blockchain can be used to simplify the payment process; however, it faces a performance bottleneck due to a special consensus mechanism. Verifying a high volume of transactions in V2G networks in a time-efficient manner is challenging. An increasing number of new proposals have been made to improve the efficiency of blockchains, such as the Lightning network, which supports more than 47,000 transactions per second. With the development of new blockchain techniques, we can foresee that the transaction efficiency will be continually improved to satisfy the requirements of V2G networks.

## Conclusions

This article presented a blockchain-based privacy-preserving payment mechanism that can satisfy the requirements of data sharing and privacy protection in V2G networks. By designing a registration process, the new payment mechanism enabled payment auditing while preserving data privacy. Value-added service providers can easily obtain payment records for analysis without inferring the identities or private information of EVs. The blockchain techniques used in the payment mechanism guaranteed the reliability of the payment process. Once a signed transaction was written into the global ledger, the corresponding payment record was tamper-resistant and non-repudiable. We implemented a prototype of the proposed payment mechanism and demonstrated its feasibility and effectiveness using simulations. We also discussed future challenges and research opportunities.

## Acknowledgments

This work was supported in part by the China National Key Research and Development Program under Grant 2016YFB0800301; in part by the National Science Foundation of China under Grant no. 61772236, no. 61602039, and no. 61370027; and in part by the CCF-Venustech Open Research Fund. Dr. Meng Shen is the corresponding author.

By designing a registration process, the new payment mechanism enabled payment auditing while preserving data privacy. Value-added service providers can easily obtain payment records for analysis without inferring the identities or private information of EVs.

| Parameter | Size (bytes) | Number | Total size (bytes) |
|---|---|---|---|
| Txid | 2 | 1 | 2 |
| Txhash | 32 | 1 | 32 |
| Sn_sf | 2 | 2 | 4 |
| Pre_txhash | 32 | 2 | 64 |
| Pre_sn_df | 2 | 2 | 4 |
| Signature | 71 | 2 | 142 |
| Unit price | 2 | 1 | 2 |
| Total amount | 2 | 1 | 2 |
| Sn_df | 2 | 2 | 4 |
| Account | 138 | 2 | 276 |
| Amount | 2 | 2 | 4 |

TABLE 2. Transaction size.

## References

[1] E. Sortomme *et al.*, "Optimal Scheduling of Vehicle-to-Grid Energy and Ancillary Services," *IEEE Trans. Smart Grid*, vol. 3, no. 1, Mar. 2012, pp. 351–59.

[2] Z. M. Fadlullah *et al.*, "GTES: An Optimized Game-Theoretic Demand-Side Management Scheme for Smart Grid," *IEEE Systems J.*, vol. 8, no. 2, Jul. 2013, pp. 588–97.

[3] Y. Wu *et al.*, "Optimal Pricing and Energy Scheduling for Hybrid Energy Trading Market in Future Smart Grid," *IEEE Trans. Industrial Informatics*, vol. 11, no. 6, Dec. 2015, pp. 1585–96.

[4] Z. Yang *et al.*, "P2: Privacy-Preserving Communication and Precise Reward Architecture for V2G Networks in Smart Grid," *IEEE Trans. Smart Grid*, vol. 2, no. 4, May. 2011, pp. 697–706.

[5] H. Wang *et al.*, "TPP: Traceable Privacy-Preserving Communication and Precise Reward for Vehicle-to-Grid Networks in Smart Grids," *IEEE Trans. Information Forensics & Security*, vol. 10, no. 11, Jul. 2015, pp. 2340–51.

[6] H. A. Man *et al.*, "A New Payment System for Enhancing Location Privacy of Electric Vehicles," *IEEE Trans. Vehicular Technology*, vol. 63, no. 1, Jul. 2013, pp. 3–18.

[7] Bitcoin: A Peer-to-Peer Electronic Cash System, https://bitcoin.org/bitcoin.pdf.

[8] Hyperledger/fabric-chaintool, https://github.com/hyperledger/fabric-chaintool.

[9] T. Zhao *et al.*, "An Anonymous Payment System to Protect the Privacy of Electric Vehicles," *Proc. Wireless Communications and Signal Processing (WCSP)*, Dec. 2014, pp. 1–6.

[10] LO3 Energy and ConsenSys: Transactive-Grid, http://transactivegrid.net.

[11] A. Biryukov *et al.*, "Deanonymisation of Clients in Bitcoin P2P Network," *Proc. ACM Conf. Computer Commun. Security (ACM CCS)*, Nov. 2014, pp. 15–29.

[12] J. V. Monaco, "Identifying Bitcoin Users by Transaction Behavior," *Proc. SPIE Defense, Security, and Sensing (SPIE DSS)*, May. 2015, pp. 33-47.

[13] A. Clement *et al.*, "Making Byzantine Fault Tolerant Systems Tolerate Byzantine Faults," *Proc. USENIX Symposium on Networked Systems Design and Implementation (USENIX NSDI)*, Jan. 2009, pp. 153–68.

[14] A next-generation smart contract and decentralized application platform, https://www.ethereum.org/pdfs/Ethereum-WhitePaper.pdf/.

[15] M. Shen *et al.*, "Cloud-Based Approximate Constrained Shortest Distance Queries over Encrypted Graphs with Privacy Protection," *IEEE Trans. Information Forensics and Security*, vol. 13, no. 4, Apr. 2018, pp. 940–53.

## Biographies

Feng Gao received the B.Eng. degree from the School of Software Engineering, Beijing Institute of Technology, Beijing, China in 2010. He is currently a Ph.D. candidate at the School of Computer Science and Technology, Beijing Institute of Technology, Beijing, China. His research interests include data privacy, Blockchain and smart grid.

Liehuang Zhu is a professor at the School of Computer Science and Technology, Beijing Institute of Technology. He has been selected into the Program for New Century Excellent Talents in University from the Ministry of Education, P.R. China. His research interests include Internet of Things, cloud computing security, Internet and mobile security.

Meng Shen received the B.Eng. degree from Shandong University, Jinan, China in 2009, and the Ph.D. degree from Tsinghua University, Beijing, China in 2014, both in computer science. He is currently an assistant professor at the School of Computer Science and Technology, Beijing Institute of Technology, Beijing, China. His research interests include privacy protection and cloud computing. He is a member of IEEE.

Kashif Sharif received his M.S. degree in information technology in 2004, and the Ph.D. degree in computing and informatics from the University of North Carolina at Charlotte, USA in 2012. He is currently an associate professor at Beijing Institute of Technology, China. His research interests include wireless and sensor networks, network simulation systems, software defined and data center networking, ICN, and Internet of Things. He is a member of IEEE and ACM.

Zhiguo Wan is an associate professor at the School of Computer Science and Technology, Shandong University, Jinan, China. His main research interests include security and privacy for big data, cryptocurrency, smart grid, and so on. He received his B.S. degree in computer science from Tsinghua University in 2002, and the Ph.D. degree from the School of Computing, National University of Singapore in 2007. He worked as a postdoc in Katholieke University of Leuven, Belgium from 2006 to 2008. He is a member of IEEE.

Kui Ren is currently with the Institute of Cyber Security Research and the School of Computer Science and Technology at Zhejiang University. His research interests include cloud and data security, IoT and mobile security, and privacy-enhancing technologies. He is a Fellow of IEEE and a Distinguished Member of ACM.