IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received November 16, 2019, accepted December 2, 2019, date of publication December 6, 2019,
date of current version December 23, 2019.

Digital Object Identifier 10.1109/ACCESS.2019.2958122

Secure Electricity Trading and Incentive Contract Model for Electric Vehicle Based on Energy Blockchain

XIAOFENG CHEN AND XIAOHONG ZHANG
School of Information Engineering, Jiangxi University of Science and Technology, Ganzhou 341000, China

Corresponding author: Xiaohong Zhang (xiaohongzh@263.net)

This work was supported in part by the National Natural Science Foundation of China under Grant 61763017 and Grant 51665019, in part by the Scientific Research Plan Projects of Jiangxi Education Department under Grant GJJ150621, in part by the Natural Science Foundation of Jiangxi Province under Grant 20161BAB202053 and Grant 20161BAB206145, and in part by the Innovation Fund for Graduate Students in Jiangxi Province under Grant YC2017-S302.

ABSTRACT As a neoteric high-tech product, electric vehicles (EVs) can effectively solve the problems of energy shortages and environmental pollution. On the one hand, EV can relieve the peak load of a smart grid and improve the electricity system operation. On the other hand, EV's electricity trading information can provide useful data for vehicle management departments to electricity scheduling. However, hackers can easily obtain data from the central database to simulate both parties involved, which leads to the receiver getting unauthorized information. For these challenges, we propose a novel secure electricity trading and incentive contract model based on the basic rules of China's electricity market. The digital signature technology adopts elliptic curve bilinear pairing to guarantee the reliability and integrity of the transaction information. Energy blockchain is utilized for encryption and distributed storage of energy data with the possession of tamper-proof and traceability. The consistency part of the data block applies a practical Byzantine fault-tolerant (PBFT) algorithm, which not only increases transaction throughput but also reduces transmission delay. The incentive contract based on revenue rewards can promote the benign interaction of EVs. The security analysis reveals that this scheme can achieve better results. Compared with other schemes, our scheme saves about 64.55% of the communication overhead and validates the same number of signed messages in a shorter time. Incentive contracts based on game theory can facilitate EV electricity trading through energy coin rewards. This mechanism makes EV more willing and active to participate in transactions that guarantee the activity and stability of the network.

INDEX TERMS Energy blockchain, electric vehicle (EV), elliptic curve encryption, game theory, incentive mechanism, security analysis.

I. INTRODUCTION

A. BACKGROUND AND MOTIVATION

To response these challenges of the energy crisis and environmental issues, electric vehicles (EVs) are replacing traditional internal combustion vehicles as a solution of sustainability issues [1]. Compared with traditional transportation methods, EV has the advantages of zero tailpipe emissions, high efficiency, and low cost. In the future, EV will conduct charging and discharging services with charging infrastructure (CI), and then CI will conduct information interaction and electricity transmission with smart grid. With the rapid development of smart grids, EV will also play a new role in energy trading with the smart grid. According to studies [2], EV can be used as a distributed energy storage system to reduce the peak load of the smart grid. High expectation for EV, with global sales possibly reaching 5% of the overall light vehicle market by 2020 [3]. Since 2005, the 10th order of China's electric regulatory commission has adopted the basic rules for the operation of the electricity market. An electricity supplier that obtains electricity operation licenses and users approved by electricity regulatory departments may participate in regional electricity market transactions. Electricity dispatching and trading institutions are responsible for electricity dispatching, electricity market trading, and metering.

The associate editor coordinating the review of this manuscript and approving it for publication was Sudhakar Babu Thanikanti.

As far as we know, China's new energy electric vehicles are developing rapidly, and the demand for electric energy is huge. However, there are some problems in the regional electricity market, such as low EV charging efficiency, lagging construction of charging facilities, and difficult management of policy-makers. Because EVs take a relatively long time to charge, electric power can usually be obtained from CI, other EVs, and local photovoltaic (PV) power generation. There are three main types of CI: large charging stations, private charging piles and battery exchange stations. Therefore, the optimization of charging time scheduling and the development of charging pile placement issues require researchers to propose effective models to solve [4]. In the vehicle-to-grid (V2G) energy switching, the electricity company analyzes the generated data to balance the electricity load in the region to prevent overloading of the grid, system instability, and energy loss [5]. These electricity companies can also install distributed PV generation in their distribution networks. For example, MyEnergi recently launched the Zappi solar electricity device, which uses the surplus electricity generated by solar panels to transfer electricity to EVs. Zappi prioritizes the use of local PV and generated electricity to efficiently provide enough electricity for EVs.

Nowadays, there are many challenges that must be faced in V2G networks. On the one hand, the EV needs to provide the identity information of the owner when performing the charging service, and the attacker may forge personal information for a spoofing attack. The transaction data generated during charging and discharging may be maliciously tampered with or lost, which will cause the driver to bear a huge security risk. Therefore, it is very essential to warrant the shelter and privacy of information interaction in an efficient communication network. In the literature [6]–[8], solutions are proposed for the privacy problem of information interaction and the identity authentication problem [9]. If the central node is attacked, which will lead to serious safety and privacy leakage problems. Eventually, poor CI can lead to low power utilization and a waste of resources. From the perspective of the smart grid, due to the random mobility of EVs, there may be problems such as disordered charging, information congestion, and grid load during the charging process.

With the popularity of EVs in the energy market, some malicious operators will seriously threaten the security and privacy of EV through various spiteful attacks [10]. For example, license plate information disclosure, forgery location, illegal advertising services, etc. Note that almost all necessary EV information, driver identification information, and transaction data rely on trusted third-party storage. Fashionable blockchain technology is a decentralized distributed database that uses encryption algorithms and consensus mechanisms to assure that data is tamper-proof and unforgeable. The author of [11] proposed a secure energy trading model based on blockchain technology for the internet of electric vehicles. Blockchain provides a script code system for cryptocurrency (such as bitcoin) and smart contracts, providing excellent technology for energy trading in the energy market [12], [13]. Aiming at the privacy protection and transaction security of EV during charge-discharge services, Kang *et al.* [14] proposed a novel peer-to-peer energy trading model based on a consortium blockchain. On the contrary, Li *et al.* [15] presented a credit-based payment scheme that decreases transactional constraints in the energy blockchain and supports fast and frequent energy transactions. To defend vehicle privacy and stimulate information interaction between vehicles, Li *et al*. [16] proposed a new privacy protection incentive announcement network based on blockchain. Zhang *et al*. [17] combine real-time systems of priority and cryptocurrency to incentive energy trading between EVs. Fan *et al*. [18] proposed a game model of traffic information transmission oriented to the internet of vehicles, which can increase the transmission efficiency of traffic service information and defeat the selfish behavior of nodes. Based on previous studies, we will further investigate the challenges to the energy market posed by the authentication and transaction data preservation of EVs. As far as we know, our proposal is an innovative interdisciplinary work to implement the energy blockchain-based safe electricity trading and incentive contract model for EVs.

B. CONTRIBUTIONS

Following this, there are three parts of our main contribution which are listed below.

1) According to the insecure data transmission and identity authentication, we apply the digital signature based on bilinear pairings on the elliptic curve to the electric power trading between EVs. Its security and feasibility are also analyzed.
2) We focus on improving transaction confirmation speed and storage, using a practical Byzantine fault-tolerant (PBFT) consistency algorithm of energy blockchain as a distributed database of electric power trading data.
3) Based on the game problem of electricity trading strategy, we develop a unique incentive contract model to promote more EVs to participate in electric power trading. Choose the optimal trading strategy through the different rewarded of energy coins.

This article is organized in the following sections. Section 2 introduces the prerequisite knowledge of the elliptic curve cryptosystem, energy blockchain, and game theory. Section 3 presents the system framework and entity introduction of the system. Section 4 introduces the specific process of using digital signature technology to verify the identity and message of EVs. To promote the initiative of vehicle interaction, a unique incentive contract model will be proposed in section 5. Section 6 shows the security analysis and performance evaluation of our scheme. In the end, we summarize the full paper.

II. PREREQUISITE KNOWLEDGE OF RELATED THEORIES

A. ELLIPTIC CURVE CRYPTOSYSTEM AND BILINEAR MAPS

In 1985, V.S. Miller *et al.* [19] proposed the use of elliptic curves for public-key cryptosystems, the security of which is based on the elliptic curve discrete logarithm problem (ECDLP). The elliptic curve cryptosystem (ECC) uses a key length that is shorter than the key length of other public-key cryptosystems, but it can reach the same security level. Advantage of ECC is that it can define the bilinear mapping between groups based on Weil and Tate Pairings [20], [21].

Assume that there is a finite field $GF(p)$, and a large prime number p is the order of $GF(p)$. An elliptic curve $E_p(a, b)$ on the finite field $GF(p)$ is defined as $y^2 \equiv x^3 + ax + b(\mathrm{mod}p)$, where a, b, x and y all belong to the finite field $GF(p)$. The corresponding coefficient satisfies $4a^2 + 27b^3(\mathrm{mod}p) \neq 0$, and the elliptic curve is usually represented by $E_p(a, b)$. The two points on the $E_p(a, b)$ on the finite field $GF(p)$ are mapped to one element in the base domain. Construct a bilinear pair by modifying Weil and Tate Pairings, which is defined as follows. Suppose q is a large prime number, G_1 and G_2 are additive group and multiplicative group of order q respectively, and g is the generator of G_1, the mapping $\hat{e} : G_1 \times G_2 \rightarrow G_2$ is a bilinear mapping. Bilinear mapping satisfies three properties, including bilinearity, non-degenerate, and computability.

On the coordinate system of the elliptic curve $E_p(a, b)$, a special point infinitely far from the X-axis is defined as an O point, and a finite number of points N, wherein N is larger and the safety is higher. Any two points P and Q on the elliptic curve $E_p(a, b)$ are added to generate another point R on $E_p(a, b)$, and the addition and point set $E(GF(p))$ constitute the Abelian group. Determine the integer k and $k \in p$, such that $Q = k \times P$. The difficulty of ECDLP means that knowing P and Q, it is difficult to determine the integer k. The steps for generating a public-private key pair in cryptography are as follows.

1) To select an elliptic curve group $E_p(a, b)$, and the expression is $y^2 \equiv x^3 + ax + b(\mathrm{mod}p)$.
2) Finding a specific base point $G(x_0, y_0) \in E_p(a, b)$ and discloses that $G(x_0, y_0)$ and $E_p(a, b)$ are in the network. Choose a large prime K and satisfy $O = KG$.
3) Randomly choose an integer $k < K$, and $P = k \times G$. Then the private key is k and the public-key is disclosed $(G, K, P, E_p(a, b))$.

Further, the bilinear map can be constructed by modifying the elliptic curve, and it also has some characteristics of the elliptic curve.

B. ENERGY BLOCKCHAIN AND SMART CONTRACT

The untrusted and opaque energy trading market in V2G gradually exposes risks such as transaction efficiency and data security. Blockchain technology originated in 2008, a

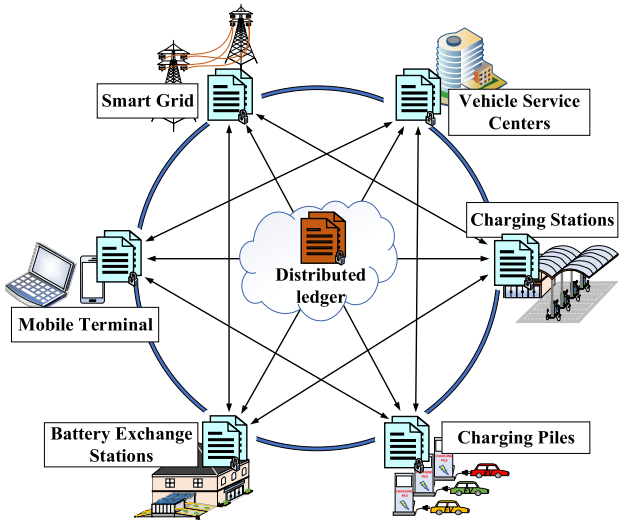


FIGURE 1. Distributed ledger in the energy blockchain.

paper published [22] by Bitcoin founder Nakamoto. As the underlying technology of bitcoin, blockchain is a specific data structure connected in chronological order, which uses Merkel tree and security Hash function (SHA-256) encryption. Data tamper-proof and unforgeable by cryptographic techniques to achieve distributed ledger of data transmission and storage [23]. Blockchain technology and energy trading market have common characteristics of intelligence, distributed nodes, sharing, etc. The combination of the two into an energy blockchain can afford a sustained and reliable guarantee for EV charging and discharging services. They are represented by jointly maintaining a distributed ledger of charging infrastructure, smart grids, mobile devices, and vehicle service centers (VSCs), as shown in Fig. 1.

Huang *et al.* [24] proposed a decentralized security model based on the blockchain ecosystem named LSNC. The LSNC model uses elliptic curve cryptography to intensify transaction security between the EV and the chargers. A shared private charging pile solution based on smart contract is provided in the literature [25], which can provide on-time rental service and defend the security and privacy of payment between untrusted strangers.

Energy blockchain is a decentralized energy interconnection structure [26] in which the energy nodes in the network practice encrypted chain blocks to verify and store energy transaction data and automatically complete the transaction processing with smart contracts. The smart contract is a commitment made by a participant before something occurs and automatically executed by the system when the trigger condition is met. Once the contract is in force, no participant can change it. A trade request is granted to trigger a smart contract, which is automatically executed independently on a node in the system in a specified form based on the data contained in the trigger states [13]. The energy blockchain is federally managed by multiple institutions, which is suitable for electricity trading scenarios. Hyperledger project [27] is

one of the largest typical consortium blockchain development platforms, providing a modular architecture that makes it simple to implement smart contracts, distributed consensus, and member services. Smart contracts in the Fabric platform are called Chaincode, and Docker is used as a sandbox to instantiate and validate the contracts. The peer-to-peer (P2P) protocol of Hyperledger Fabric is completed based on the HTTP/2 protocol. It is an open-source blockchain underlying system, which can accomplish various application scenarios of blockchain.

C. GAME THEORY WITH NASH EQUILIBRIUM

With the growing popularity of EVs and smart grids, the decision-making bodies associated with the operation of leading electricity systems tend to diversify. In this case, it is a challenging problem to determine the best strategy for any decision-maker to balance and optimize the interests of each party in the electricity system. Therefore, game-theory oriented to multiple inter-entity optimization strategies is expected to be an effective means to resolve this problem. Game theory mainly studies that when there is a conflict between the interests of multiple participants, participants can follow the rules to choose the best strategy for themselves or the group of participants according to their abilities and information. The basic form $G = (P_n, S_n, u_n)$ of the game expression is composed of the three elements of the participant $P_n = \{P_1, P_2, \ldots, P_i\}$, the strategy $S_n = \{S_1, S_2, \ldots, S_i\}$ and the utility function $u_n = \{u_1, u_2, \ldots, u_i\}$. Then the profits acquired by the i-th participant under various strategies are expressed as $u_i : S \rightarrow R$. According to whether a requisite agreement has been reached, game theory can be classified into cooperative and non-cooperative games [28].

1) Cooperative game: Refers to all or part of the participants in the game environment playing the game in the form of alliance and cooperation, and analyzing the problem of the income distribution of the participants.
2) Non-cooperative game: The behavior of all participants is treated as a separate behavior, independent of other participants in the environment. The research participants in the mutual influence of interests in the situation how to choose the decision to maximize their gains.

Nash Equilibrium (NE) is the core concept of non-cooperative game [29]. In a strategy mix, the participant's strategy is in the best interest of himself when others do not modify the strategy. In the game model $G = (P_n, S_n, u_n)$ of the system's n participants, the strategy combination is described $s^* = \{s_1^*, s_2^*, \ldots, s_i^*, \ldots, s_n^*\}$, $s_i^* \in S_i$, $s_{-i}^* \in S \backslash S_i$, for a NE where any $\forall i$ is G, this equilibrium means that no individual increase the profit by unilaterally changing his strategy. Let the opponent's strategy combination for $\forall i \in P$, s_i^* is i be the optimal income function of participant i under $s_i \neq s_{-i}^*$ condition, such as

$$u_i(s_i^*, s_{-i}^*) \geq u_i(s_i, s_{-i}^*), \quad \forall s_i \in S_i. \tag{1}$$

If formula (1) is strictly true for each $s_i \neq s_{-i}^*$, then $s^* = (s_1^*, s_2^*, \ldots, s_i^*, \ldots, s_n^*)$ is called the strict Nash equilibrium of G. If s_i^* is a pure strategy, the equalization is called a pure strategy Nash equilibrium. Otherwise, this equilibrium is called a mixed Nash equilibrium.

The authors of [30] proposed a secure and efficient V2G energy trading model based on exploring blockchain and obtained the optimal electricity allocation strategies by the Stackelberg game and backward induction approach. Article [31] contributes monetary rewards with uniform pricing to stimulate the charging process of third-party energy access points (EAPs), to stimulate the activity of nodes in the system. In the paper [32], the author proposed a secured and effective reputation management scheme to support highly reputable miners to use contract theory, participate in block validation to reduce collision between miners.

III. PROPOSAL SYSTEM MODEL

Based on cryptography and blockchain technology theory and combined with China's electricity energy supply rules, this paper analyzes the charging and discharging behavior and needs of EVs. In the blockchain, the encryption algorithm enables the security of storage and transmission of electricity transaction data, while the digital signature algorithm guarantees the reliability of the data. In the part where the consistency agreement is reached in the data block, the efficient fault-tolerant consensus algorithm makes the information synchromesh more time-efficient. Starting from China's electricity market and EV charging situation, we can choose the best game strategy under the incentive contract to promote the benefits of EVs. In this paper, we introduce an EV security electricity trading model based on the incentive contract and energy blockchain, as displayed in Fig. 2. This model is mainly composed of EV to energy market network and energy information processing network. When EV communicates with the CI in the energy market, the scheme provides privacy protection of transaction data through a digital signature algorithm. The smart contract stored in the data processor (DP) automatically executes the command according to the prior agreement, then combined with the game theory the model comes to the optimal charging strategy. Belatedly, the corresponding interactive information is organized into data blocks through the distributed consensus mechanism and stored in the energy blockchain.

A. EV TO ENERGY MARKET NETWORK MODEL

EV to energy market network includes V2G, EV to VSC and EV to CI and so on. The EV electricity supply methods mainly include slow charging (e.g., private charging pile), fast charging (e.g., large charging station) and battery replacement (e.g., battery exchange station). The Zappi solar power plant gives priority to local PV generated electricity to power EVs. Different charging facilities are used as access points to connect the grid or other EVs for charge-discharge services, as shown in the lower part of Fig. 2.

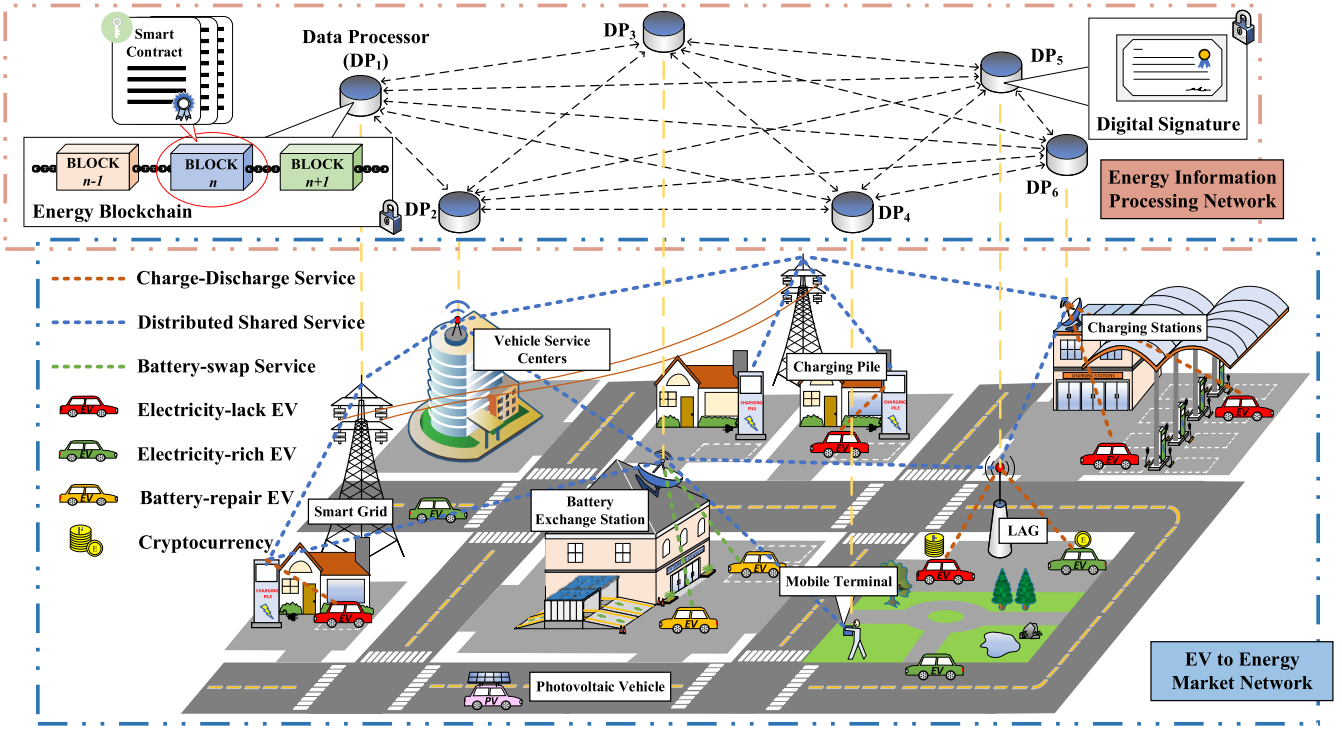


FIGURE 2. Secure electricity trading and incentive contract model for EV based on energy blockchain.

1) PRIVATE CHARGING PILES

With the low construction cost of private charging piles, EV can choose to charge at night while it is cheaper. However, the disadvantage of this service model cannot be ignored. It needs a long charging time, which makes it difficult to meet the urgent demand of customers. As an ordinarily used charging method for EV, charging piles cover small area and are built in an unlimited location. They are normally placed in personal accommodation, shopping malls, and car parks.

2) LARGE CHARGING STATION

The advantage of large charging stations is the short charging time, which can meet the urgent needs of customers, and the ability to charge up multiple EVs at the same time. But the battery lifetime of a vehicle can be decreased if it often receives large amounts of electricity over a slight time. Due to its quick charging mode of supply, the large charging station requires a high position of smart grid, which needs to be close to large substations. Therefore, its construction cost is undoubtedly higher.

3) BATTERY EXCHANGE STATION

Battery exchange station is mainly for the vehicle to replace depleted batteries and to provide maintenance services, with features of short operation time, so it can save a lot of time for the user. Its drawback is that the initial investment cost is powerful, and it needs a lot of space to store the battery. pack.

The EV can communicate with the service providers by Local Aggregators (LAGs), and afford electricity trading services between the electricity-rich EVs and the electricity-lack EVs. We can recognize individual CI, VSC, and mobile terminal in the EV to energy market network as a network node. The transaction data generated at any network node implements distributed Shared services for EV. Photovoltaic EVs need to install solar cells that convert solar energy into electricity to power EVs. However, owing to the high cost of PV panels and weather constraints, the usefulness of photovoltaic EVs is greatly limited.

B. ENERGY INFORMATION PROCESSING NETWORK

Various network node has a DP that collates and transmits the generated data. The distribution characteristics of these network nodes are alike to the distribution of nodes in the blockchain. Electric-lack EV and electric-rich EV can exchange electricity directly through LAG, which will generate price information and vehicle battery status data. In the energy information processing network in the upper part of Fig. 2, two DPs in a distributed node share information, communicating point-to-point to jointly maintain the distributed ledger. The technical process is as follows:

1) The digital signature algorithm based on bilinear pairings on an elliptic curve is applied to confirm the vehicle's legal identity and the authenticity of transaction data. The sender signs the message with its private key before sending the transaction information, and the receiver verifies the signature with the sender's public key. It can not only effectively assure the security and non-repudiation of electricity trading, but also quickly verify whether the trading is legal and effective.

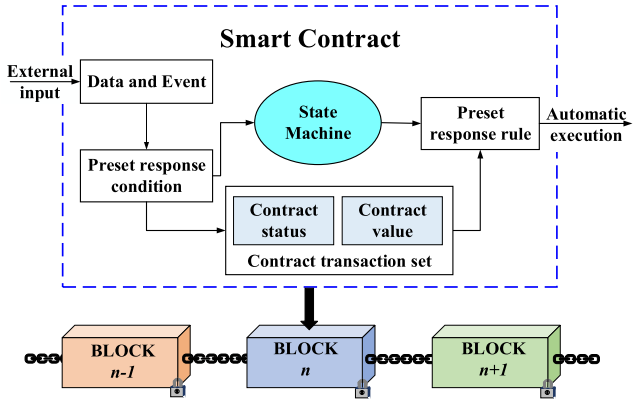


FIGURE 3. Smart contract model based on energy blockchain.

2) Moreover, charging stations, battery exchange stations, and LAG's built-in DP can pack the data into blocks. And data blocks need to build distributed consensus before they are written into the blockchain. The distributed consensus mechanism is the heart of blockchain technology, which is the key to making the whole system work reliably. If most utmost nodes in the network agree on the authenticity and reliability of the data, a consistent statement will be delivered to the ledger. Data blocks require to be verified by total participants for collaborative management to add new blocks to the blockchain. Decentralized control based on neighbors [33] permits all verifiers to reach consensus under limited information exchange and dynamic interaction.
3) We use a PBFT security mechanism that grows transaction confirmation rate and transaction throughput. This PBFT consensus algorithm [34] can prevent many problems such as data corruption and latency, and has a great fault-tolerant ability for energy market nodes. If the network node finds a new ledger, it can get the transfer records automatically generated by the system and a certain amount of cryptocurrency. The energy coin that represents vehicle energy transaction data is described as a new cryptocurrency for vehicle applications.

Smart contracts based on energy blockchain technology can not only give pleasure to the advantages of execution efficiency but also avoid the interference of human interference on the natural execution of contracts. As shown in the smart contract model in Fig. 3, the digital property data and events of the contract participants are externally entered, and the conditions of the incident reply are preset. Through the state machine and contract transaction set, the current asset state and the execution selection of the following contract transaction are judged and docked with the external information. According to the preset response dictate, the trigger condition of the contract is determined and the relevant commands are automatically executed by the computer network. Smart contracts can be combined with game theory, which defines a cryptocurrency payment function to motivate nodes to write new ledgers.

IV. SECURE EV ELECTRICITY TRADING AND INFORMATION INTERACTION

A. PRIVACY SCENARIOS AND NETWORK SECURITY FOR ELECTRICITY TRADING

1) PRIVACY SENSITIVE DATA

Private data (such as ID, charging location, and payment data) will have security associations for EVs, and analysis of this data can unveil customer behavior. EVs performing charging and discharging services can sell electricity back to the grid or other vehicles, which can act as power providers or customers. After performing the charging service, the EV will selectively expose non-sensitive data and hide sensitive data. Although EV is hesitant to disclose personal information to the network, it is essential to provide personal information to confirm that he is a legitimate electricity provider. Smart meters built into each EV report energy consumption meters to support that electricity transactions have been achieved. EVs have ownership of energy consumption, not just electricity service centers or third parties.

2) NETWORK INFORMATION SECURITY

The confidentiality, reliability, and integrity of electricity transaction data have higher security requirements for the network. The information security transmission between LAG and charging stations or EVs is a significant guarantee to prevent attackers from illegally intercepting data. Two-way communication connection methods include EV to LAG, and LAG to the legally authorized maintainer, which is riskier than traditional network communication. More specifically, ensuring the security of information distribution, collection and storage is critical to customers or electricity providers. On the other hand, if the third-party organization is attacked by the attacker, it will lead to the serious disclosure of personal privacy information or even the network paralysis.

B. DIGITAL SIGNATURE ALGORITHM

The EV requires to be registered with the VSC before joining in the electricity transaction, including the owner's intimate information and fundamental information of the vehicle. The VSC will authorize the EV with a legal identity and assign the appropriate authentication information and system parameters. After that, the interaction information is signed and authenticated. An attacker may replace the information to broadcast the wrong content [35] and only authenticated vehicles can be trusted. We improved the digital signature method based on the paper [36] and applied it to the information interaction of EV charging and discharging services. The digital signature authentication scheme based on bilinear pairings on elliptic curve satisfies the pursuit of security and real-time in electricity data interaction system. As shown in Fig. 4, the digital signature algorithm flow graph of the system model, the entities participating in the signature and verification principally have EV, CI, and VSC. The scheme is classified into four main stages: system initialization,

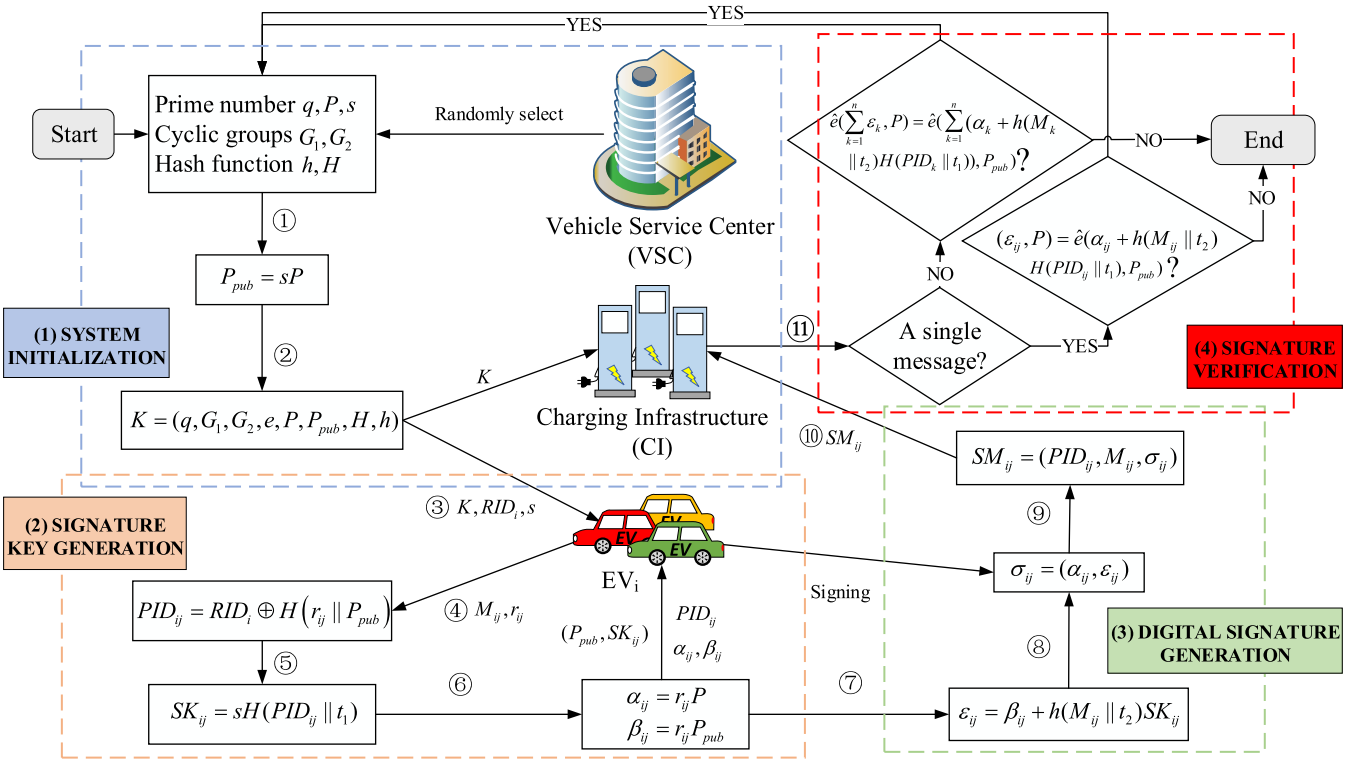


FIGURE 4. Flow chart of digital signature algorithm in EV to energy market network.

signature key generation, digital signature generation and signature verification.

1) SYSTEM INITIALIZATION

At this phase, the VSC initializes parameters in all systems, including basic information on the EV and CI, etc. The initialized parameters and authentication information are distributed to the CI and the newly joined EV, respectively. After selecting an elliptic curve $E_p(a, b)$ that meets the requirements of the elliptic curve cryptosystem, randomly select a prime number q, $q \in Z_q^*$, where Z_q^* is a finite field. The two cyclic groups are G_1 and G_2, respectively, and their order is q, where G_1 is a cyclic addition group and G_2 is a cyclic multiplication group.

VSC randomly selects two prime number of P and s, where s is VSC's own private key, and s belongs to Z_q^*, which is in accordance with $1 < s < q$. P is a generator in the cyclic group G_1, then its public-key is

$$P_{pub} = sP. \tag{2}$$

The one-way Hash function $H : \{0, 1\}^* \rightarrow G_1$, Hashes the true identity RID_i of the i-th EV_i to G_1, and $RID_i \in G_1$. In addition, VSC will specify a normal Hash function $h : \{0, 1\}^* \rightarrow Z_q$. Broadcast the public parameters $K = (q, G_1, G_2, e, P, P_{pub}, H, h)$ of the system to the whole network, then the public parameters of the EV_i tamper-proof device, the real identity RID_i of the EV_i, and the private key of the VSC. If the CI is trusted, it will only be assigned public parameters and will be responsible for verifying the authenticity of the EV_i identity and the reliability of the message. Table 1 summarizes the system parameter symbols used in the schemes herein.

2) SIGNATURE KEY GENERATION

During the generation of the signer's key phase, the CI authenticates the EV_i and prepares for subsequent message signing. If the identity authentication is passed, the interaction of the electricity transaction information is continued, and if the identity authentication is not passed, the communication is terminated. Each EV_i will be signed with a pseudonym identity and a corresponding private key to prevent the user's location privacy from being compromised. Then the j-th pseudonym PID_{ij} adopted by the vehicle EV_i is

$$PID_{ij} = RID_i \oplus H\left(r_{ij} || P_{pub}\right). \tag{3}$$

where r_{ij} is a number randomly generated by the tamper-proof device in EV_i, and $r_{ij} \in Z_q^*$. Suppose the j-th message M_{ij} sent by EV_i, and the j-th private key SK_{ij} used to sign M_{ij}, calculate SK_{ij} as

$$SK_{ij} = sH(PID_{ij} || t_1). \tag{4}$$

where s is the private key of VSC, PID_{ij} and SK_{ij} can be calculated in advance under offline state, so it does not affect the communication delay in the process of information interaction. t_1 is the timestamp of the currently generated

TABLE 1. Related parameter symbols in the system.

Notation	Description
EV_i	The i-th electric vehicle
G_1	A cyclic additive group
G_2	A cyclic multiplicative group
RID_i	The real identity of the EV_i
PID_i	Pseudonym of EV_i
t_1, t_2	Timestamp associated with the transmission time
P	The generators of the cyclic group G_1
q	The order of G_1 and G_2
P_{pub}	The public-keys of VSC
s	The private-keys of VSC
M_{ij}	The j-th message sent by the EV_i
SK_{ij}	The private key of the j-th message signature M_{ij}
α_{ij},β_{ij}	Randomly selected authentication parameters
SM_{ij}	The content after the EV_i signs the message M_{ij}
$\hat{e}$	The bilinear map $\hat{e}: G_1 \times G_2 \to G_2$
$\|\|$	Message concatenation operation
H(.), h(.)	Hash functions such as $H: \{0,1\}^* \to G_1$, $h: \{0,1\}^* \to Z_q$

pseudonym. Select the authentication parameters α_{ij} and β_{ij}

$$\alpha_{ij} = r_{ij}P. \tag{5}$$

$$\beta_{ij} = r_{ij}P_{pub}. \tag{6}$$

After the formula (5) (6) is calculated, the random number r_{ij} is cleaned up and ready for the next random number generation. Finally, EV_i generates the signature key (P_{pub}, SK_{ij}), the identity pseudonym PID_{ij}, and the authentication parameters α_{ij}, β_{ij} at the j-th message at a certain moment. These operations are preparations for the EV_i before signing the message M_{ij}.

3) DIGITAL SIGNATURE GENERATION

During the signing phase of the message, the CI and EV work together to generate a message signature that authenticates between vehicles. EV_i selects the randomization parameter ε_{ij}, where

$$\varepsilon_{ij} = \beta_{ij} + h(M_{ij}||t_2)SK_{ij}. \tag{7}$$

t_2 is the timestamp of the currently generated message signature. Then, the signature of EV_i for the j-th security message M_{ij} is $\sigma_{ij} = (\alpha_{ij}, \varepsilon_{ij})$, where α_{ij} is content that is calculated in advance and is not related to the message. The message after EV_i signs the message M_{ij} is $SM_{ij} = (PID_{ij}, M_{ij}, \sigma_{ij})$.

After SM_{ij} is generated, the signer EV_i sends it to the CI and prepares for the final verification phase. At the same time, the transaction credentials of this stage are cleared, including the current pseudonym PID_{ij} of the EV_i and the private key SK_{ij}, and prepare for the signature of the next message and enter the verification phase.

4) SIGNATURE VERIFICATION

If EV is conducting electricity transactions with private charging piles, then the verification of a single message needs to be considered. If the EV is performing electricity service with a large charging station or a battery exchange station, it may be a verification of the batch message, so we verify separately from the single message and the batch message.

- **A single message verification**: After the CI receives the secure message $SM_{ij} = (PID_{ij}, M_{ij}, \alpha_{ij}, \varepsilon_{ij})$, it authenticates the message by verifying whether the following condition is true.

$$\hat{e}(\varepsilon_{ij}, P) = \hat{e}(\alpha_{ij} + h(M_{ij}||t_2)H(PID_{ij}||t_1), P_{pub}). \tag{8}$$

  If the formula (8) is true, SM_{ij} is indeed signed with SK_{ij} in the name of PID_{ij}, then the verification passes, indicating that the vehicle identity is legal and receives the information. Otherwise the formula is not true, the message is rejected and the communication is terminated, indicating that the signature is invalid. Because EV_i uses dynamic pseudonym identity, CI can't get the real identity RID_i of any vehicle, which effectively protects the user's privacy.
- **Batch message verification**: The same vehicle may send n messages to the CI, and the CI may also receive messages from n different vehicles, so batch verification is required to simultaneously authenticate the received messages. We use $SM_1 = (PID_1, M_1, \alpha_1, \varepsilon_1)$,. $SM_2 = (PID_2, M_2, \alpha_2, \varepsilon_2)$, ..., $SM_i = (PID_i, M_i, \alpha_i, \varepsilon_i)$ to represent all n messages received, where M_1, M_2, ..., M_i may be the same or different, and verify that the following formula is true

$$\hat{e}(\sum_{k=1}^{n} \varepsilon_k, P) = \hat{e}(\sum_{k=1}^{n} (\alpha_k + h(M_k||t_2)H(PID_k||t_1)), P_{pub}). \tag{9}$$

If the formula (9) is true, it is proved that these message signatures are valid, and the verifier receives these messages, otherwise it rejects.

C. DISTRIBUTED CONSENSUS AND STORAGE MANAGEMENT OF INTERACTIVE DATA

After the digital signature authentication of interactive data is finished, the whole network node needs to attain a distributed consensus to package and store the data in the energy blockchain. Distributed consensus is the focus technology of energy blockchain and the key to the stable operation of the system. Therefore, warranting the security and storage of interactive data is crucial to the stability of the system. PBFT security protection mechanism [34] is an improvement

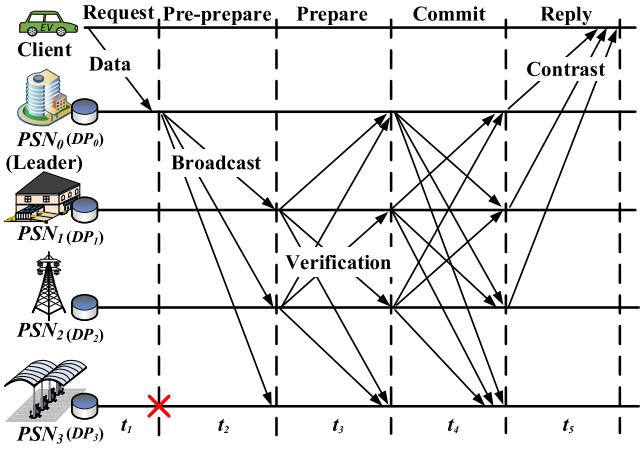


FIGURE 5. Distributed consensus flow of PBFT algorithm.

on the traditional Byzantine fault-tolerant algorithm. Applying PBFT to consensus in EV to energy market networks can advance transmission efficiency and reduce algorithm complexity.

1) MEMBERS OF INTERACTIVE DATA

After all participants reached a decentralized consensus agreement, the data was packaged into blocks and written into the ledger. Not each node in the network participates in the data audit. Only the selected nodes can play in the consensus, which is called the pre-selected node (PSN). EV is a perceptual node responsible for generating and uploading data to PSNs without participating in a consensus. Among them, PSN can be CI, smart grid, VSC and other devices with high storage capacity. One leader from all PSNs is selected as the primary node to execute the write ledger operation, and other PSNs are picked as the replica node to audit the data block. The total number of PSN in the network is n, and the number of abnormal nodes is f. As shown in Fig. 5, it is seized that VSC is indicated as PSN_0 as the leader, and battery exchange station, smart grid and charging station are denoted as PSN_1, PSN_2, and PSN_3 respectively, where PSN_3 is an abnormal node.

2) INITIAL REQUEST PHASE

As a client, EV aggregates the electricity trading data into a data block and uploads it to a nearby leader for audit. This data block contains the digital signature information of the vehicle and the Hash value of the electricity transaction record to be tested. When the leader is decided, the execution privileges and service operations of the node are initiated.

3) PRE-PREPARATION PHASE

The leader assigns a serial number N to the request, and broadcasts the sequence number assignment message and the client's request message m to the PSN of the entire network. Generally, PSN has two choices after receiving broadcast information, one is the normal node (PSN_1 or PSN_2) to accept it, and the other is an abnormal node (PSN_3) to reject it. An abnormal node is ordinarily a bad node or a fault node whose act is manifested as no answer to requests from other nodes.

4) PREPARATION PHASE

Upon receipt of the prepared message by normal PSN_1 and PSN_2, the integrity and legality of the transaction will be validated and audited. Attach a signature to the checking results and broadcast them to other replica nodes. If two different preparation messages are received, the preparation phase for the node is ended. The maximum tolerable number of abnormal nodes in the system is f ($f < (n-1)/3$), and each abnormal nodes cannot broadcast regularly.

5) COMMIT PHASE

The replica node broadcasts the confirmation message while auditing whether the received message signature is correct and comparing it with itself. If the replica node receives $n-f$ confirmation messages including its own, it will feedback to the client.

6) REPLY PHASE

In the last phase, both the primary and replica nodes receive a commit message and want to verify that the commit message signature is true. If the replica receives $2f+1$ authentication commit message, it indicates that most nodes in the network have reached consensus and feedback to the client. If the client receives $f+1$ reply messages, it means that the request sent has attained the consensus of the whole network. Otherwise, the client considers whether to resend the request to the leader.

The PBFT consensus is a consistent algorithm based on message passing, which has the advantages of growing consensus efficiency and data confirmation speed. The content of the data block involves not only the data of power transactions but also the operational data generated by the node's access to the network. After entering a consensus, the accounting node adds the new data block to the energy blockchain. Each PSN protects a copy and stores it in the built-in DP, which stores only the index of the original data. This index indicates the location of the original data so that users can efficiently monitor and inquiry. However, the raw data is stored on cloud servers or in distributed databases. On the other hand, during the feedback effects of the distributed consensus process, the system can also find out abnormal nodes for maintenance or elimination.

V. INCENTIVE CONTRACTS BASED ON GAME THEORY

The electricity transaction scenario based on incentive contracts is shown in Fig. 6, where EV_s represents electric vehicles with pre-sale of electricity and EV_p represents electric vehicles with pre-purchase of electricity.

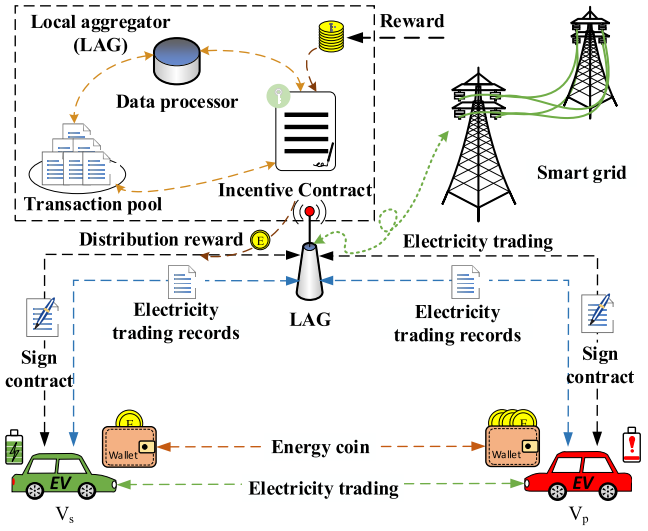


FIGURE 6. Electricity trading scenario based on incentive contracts.

A. DESIGN IDEAS OF INCENTIVE CONTRACT

As can be seen from the previous section, the PSN (where the PSN is LAG) with the fastest completion of effective proof-of-work will be rewarded with a certain number of energy coins. Within the scope of a certain amount of time LAGs according to the dimension of the contribution to electricity or data volume to distribute rewards to EV by contract rules. Besides, LAG acts as an intermediary between the grid and EVs, providing electricity trading services between EV's that are electricity-rich and electricity-lack.

In EV trading, choosing the fittest trading strategy for both parties are a game problem. The research of game theory in the field of cryptography is mainly to make use of the characteristics of rational participants to maximize the benefits and urge them to prefer the best strategy to guarantee the security of the protocol. Dong *et al.* [37] proposed a smart contract to verify collusion in cloud computing in order to prevent collusion attacks. They constructed prisoner's smart contract, conspiracy smart contract, and betrayal smart contract. Forcing participants to post deposits and rewards, and contributing incentives to deter collusion.

In this paper, an incentive contract based on game theory is proposed, in which the binding agreement can be deployed in advance. Mining rewards are replaced by energy coins from the energy blockchain. The incentive contract starts from the digital signature and verification stage of the message and combines with the cooperative game to set the optimal profit function. After debugging on the Docker sandbox on Hyperledger Fabric, the blockchain status database was finally updated and stored. The detailed steps of incentive contract implementation are given next.

B. INCENTIVE CONTRACT GENERATION

1) The new EV_i needs to be registered with the VSC or a government agency and obtain some authentication information, including the public-private key pair (P_{pub}, SK_i) of EV_i and the address W_i of the account. All the authentication information is uniquely identified by binding the license plate number and the customer's personal information. If the distribution of EV obeys the Poisson distribution, then the probability of λ nodes participating in the game is

$$P(X = \lambda) = \frac{e^{-\theta}\theta^{\lambda-1}}{(\lambda-1)!}, \theta > 0, \lambda \geq 1. \quad (10)$$

2) The parties to the contract negotiate to clarify the rights and obligations of EV and LAG. The contract specification and the trigger conditions for the execution of the contract shall be established by authorized legal persons. Define the message SM_i as the digital signature of the Hash digest of the message M_i sent by the node EV_i.
3) LAG and EV_i signed a new smart contract by agreeing on terms and rules and signing them with their own private keys. In order to ensure the security during the execution of the new contract, the deployed contract is packaged into a Docker image and verified on the Docker sandbox.

C. INCENTIVE CONTRACT RELEASE

1) The verified contract is sent to each node in P2P mode, and the node will temporarily store the received contract in memory and prepare for the consensus. In order to prevent the contract or more nodes conspiracy to commit fraud charge service, all participating LAGs and EV_i should respectively from their wallets to contract the address pay enough margin.
2) Let's say that over time, EV_i will always evolve into either EV_s or EV_p. A cooperative game of utility can be written as $G = \{P, S, U\}$, where $P = (EV_s, EV_p)$ represents the set of two game groups, $S = (S_s, S_p)$ corresponds to the strategy set of EV_s and EV_p, and $U = (U_{ij}^s, U_{ij}^p)$ represents the revenue function set of participant P under S strategy pair, and each game group has its own behavior strategy space.

The strategies space that defines EV_s is $S_s = (x_{11}, x_{10}, x_{01}, x_{00})$, as shown in table 2. Where x_{11} represents selling electricity and uploading information. x_{10} means to sell electricity, but not to upload information. x_{01} means not to sell electricity, but upload information. x_{00} means it does not sell electricity and does not upload information.

The strategies space for EV_p is defined as $S_p = (y_{11}, y_{10}, y_{01}, y_{00})$. Where y_{11} represents the purchase of electricity and the uploading of information. y_{10} means to purchase electricity, but not to upload information. y_{01} means not to purchase electricity, but upload information. y_{00} means neither electricity purchase nor information upload.

TABLE 2. Strategies space of s_s and s_p.

Strategy	Sell electricity	Not sell electricity	Purchase electricity	Not purchase electricity
Upload information	x_{11}	x_{01}	y_{11}	y_{01}
Not upload information	x_{10}	x_{00}	y_{10}	y_{00}

D. INCENTIVE CONTRACT EXECUTION

1) After the smart contract reaches the trigger condition, it will be pushed to the execution queue, and the system will execute in sequence automatically. In EV_s of game group, the probability of choosing strategy x_{ij} is p_{ij}, and $p_{ij} \in [0, 1]$. In EV_p of game group, the probability of selecting strategY y_{ij} is q_{ij}, and $q_{ij} \in [0, 1]$. We select one of the EV_s and EV_p strategies to calculate the income function [18], and others are similar.
When the game group EV_s choice strategy x_{ij} revenue probability is P^s_{ij}

$$P^s_{ij} = \frac{1 - \varepsilon^{\lambda_1}}{p_{ij}\lambda_1}. \tag{11}$$

where λ_1 is the number of nodes participating in the game in EV_s group, and ε is the connection probability value of two EVs in time t.
When the game group EV_p choice strategy y_{ij} revenue probability is P^p_{ij}

$$P^p_{ij} = \frac{1 - \varepsilon^{\lambda_2}}{q_{ij}\lambda_2}. \tag{12}$$

Similarly, λ_2 is the number of nodes participating in the game in EV_p group. The parameter symbols used in this model are shown in Table 3.
By substituting the node revenue probability (P^s_{ij}, P^p_{ij}) and formula (10) into the following formula, the final revenue $U = (U^s_{ij}, U^p_{ij})$ of EV_s and EV_p under four strategies can be calculated respectively.

$$U^s_{ij} = \begin{cases} p_{11}[(e_{sell} + e_{r-upload} + e_{receive}) \\ \times \sum_{\lambda_1}^{\infty} P(X = \lambda_1)P^s_{11} \\ -(e_{cha-discha} + e_{c-upload})], \quad S_s = x_{11} \\ p_{10}[(e_{sell} + e_{receive}) \sum_{\lambda_1}^{\infty} P(X = \lambda_1)P^s_{10} \\ -e_{cha-discha}], \quad S_s = x_{10} \\ p_{01}[(e_{r-upload} + e_{receive}) \sum_{\lambda_1}^{\infty} P(X = \lambda_1)P^s_{01} \\ -e_{c-upload})], \quad S_s = x_{01} \\ p_{00}[(e_{receive}) \sum_{\lambda_1}^{\infty} P(X = \lambda_1)P^s_{00}], \quad S_s = x_{00}. \end{cases} \tag{13}$$

TABLE 3. Parameter symbols and descriptions.

Notation	Description
e_{sell}	The EV_s node receives an energy coin reward for selling electricity.
e_{buy}	The amount of energy coin paid by an EV_p node to purchase electricity.
$e_{receive}$	The amount of energy coin awarded for receiving a traffic message.
$e_{r\text{-}upload}$	An energy coin reward for uploading an electricity transaction.
$e_{c\text{-}upload}$	An energy coin consumption for uploading an electricity transaction.
$e_{cha\text{-}discha}$	Amount of energy coin consumed for charge-discharge service

$$U^p_{ij} = \begin{cases} q_{11}[(e_{r-upload} + e_{receive}) \sum_{\lambda_2}^{\infty} P(X = \lambda_2)P^p_{11} \\ -(e_{buy} + e_{cha-discha} + e_{c-upload})], S_p = y_{11} \\ q_{10}[e_{receive} \sum_{\lambda_2}^{\infty} P(X = \lambda_2)P^p_{10} \\ -(e_{buy} + e_{cha-discha})], \quad S_p = y_{10} \\ q_{01}[(e_{r-upload} + e_{receive}) \\ \times \sum_{\lambda_2}^{\infty} P(X = \lambda_2)P^p_{01} - e_{c-upload}], \quad S_p = y_{01} \\ q_{00}[e_{receive} \sum_{\lambda_2}^{\infty} P(X = \lambda_2)P^p_{00}], \quad S_p = y_{00}. \end{cases} \tag{14}$$

2) Participants complete electricity transactions and fund settlement and package the data generated from the transactions. The contract reads the energy consumption of the EV's built-in smart meter to verify the amount of electricity it generates and consumes, and authorizes the payment of energy coin.
3) The smart contract system built in the underlying energy blockchain automatically completes the contract processing process, and has tamper-proof and transparency. More specifically, the system updates the state of the energy blockchain when the contract is completed, and the EV_i specifically updates the wallet's data record and fund balance.

The EV pays energy coins to the system not only to obtain electricity and traffic information, but also to exchange limited vehicle services with insurance companies. Therefore, the energy coin has value to the user, which naturally promotes the users to obtain it by stimulating the performance.

VI. SECURITY ANALYSIS AND PERFORMANCE EVALUATION

In this section, we compare the representative schemes such as SPRING [6], IBCPPA [7], EAAP [8] from three aspects: security analysis, verification delay and communication overhead and performance evaluation of incentive contracts. As shown in Table 4, a comparison of the security features of

TABLE 4. Security comparison between our scheme with others.

Characteristic	Our scheme	Ref. [6]	Ref. [7]	Ref. [8]
Privacy protection	Y	Y	Y	Y
Unforgeability	Y	Y	Y	N
Tamper-proof	Y	Y	Y	Y
Feasibility analysis	Y	Y	Y	Y
Resist man-in-the-middle attack	Y	N	N	Y
Decentralization	Y	N	N	N
Resist collusion attack	Y	N	N	N

several schemes is listed. The comparison results show that our scheme achieves better security effect.

A. SECURITY ANALYSIS

We use an asymmetric encryption and signature verification technology to ensure secure access and data reliability in electricity transactions, and can resist many traditional security attacks. Signed messages are stored on the energy blockchain, which means distributed storage of data and meets the following security requirements.

1) NODE PRIVACY PROTECTION

In our scenario, each EV_i is randomly assigned a dynamic pseudonym PID_{ij}. The attacker cannot deduce the identity of EV_i from a one-time pseudonym without knowing the random number r_{ij}. Therefore, attackers cannot easily find the real identity RID_{ij} of vehicles and users, and cannot break the encrypted data in a short time.

2) UNFORGEABILITY

The VSC or the CI authenticates the current vehicle, and legitimate EVs that passes the authentication can conduct electric power trading. The distributed nature of energy blockchain combined with digital signature transactions makes it impossible for attackers to forge messages. In addition, user information and EV_i license plate number are tied together during the registration phase and stored in trusted authorities as unique identifiers.

3) TAMPER-PROOF

Different from the traditional centralized data storage, energy blockchain is a distributed storage structure. All participants in the network jointly maintain a distributed ledger, and each participant keeps a copy. Blockchain uses asymmetric cryptography to encrypt data and PBFT consensus algorithm to form a powerful computing force.

4) FEASIBILITY ANALYSIS

In addition, the feasibility of the signature verification formula can be verified. If the signature of EV_i sending the first message is SM_{i1}, the following can be obtained from the signature verification formula (8) of a single message

$$\begin{aligned}\hat{e}(\varepsilon_{ij}, P) &= \hat{e}(\beta_{ij} + h(M_{ij}||t_2)SK_{ij}, P)\\ &= \hat{e}(r_{ij}P_{pub} + h(M_{ij}||t_2)SK_{ij}, P)\\ &= \hat{e}(r_{ij}sP + h(M_{ij}||t_2)sH(PID_{ij}||t_1), P)\\ &= \hat{e}(r_{ij}P + h(M_{ij}||t_2)H(PID_{ij}||t_1), sP)\\ &= \hat{e}(\alpha_{ij} + h(M_{ij}||t_2)H(PID_{ij}||t_1), P_{pub}). \qquad (15)\end{aligned}$$

Consequently, formula (15) is valid, and the signature verification of a single message is feasible.

Suppose EV_i sends n different messages SM_{i1}, SM_{i2}, …, SM_{in}, which can be obtained by batch signature verification formula (9)

$$\begin{aligned}&\hat{e}(\sum_{k=1}^{n}\varepsilon_k, P)\\ &= \hat{e}(\sum_{k=1}^{n}(\beta_k + h(M_k||t_2)SK_k), P)\\ &= \hat{e}(\sum_{k=1}^{n}(r_kP_{pub} + h(M_k||t_2)SK_k), P)\\ &= \hat{e}(\sum_{k=1}^{n}(r_kP + h(M_k||t_2)H(PID_k||t_1)), sP)\\ &= \hat{e}(\sum_{k=1}^{n}(\alpha_k + h(M_k||t_2)H(PID_k||t_1)), P_{pub}). \qquad (16)\end{aligned}$$

Consequently, formula (16) is valid, and the signature verification of batch messages is feasible.

5) RESIST MAN-IN-THE-MIDDLE ATTACK

To complete the interception, the attacker maintains a communication connection with the buyer and seller of the EV, and both parties believe that they are communicating with each other in a secure connection. However, in the process of electricity transactions between EV_i and CI or LAG, a random number r_{ij} and dynamic pseudonym PID_{ij} are generated to link each time. The attacker is different from the r_{ij} and PID_{ij} of the buyer and seller, so it cannot establish communication with the user through the man-in-the-middle attack.

6) DECENTRALIZATION

Unlike traditional data storage, power trading information will be stored in a decentralized manner based on blockchain. Major entity nodes in the electric energy market jointly maintain distributed ledgers, such as CI, smart grids, smart terminals, and VSCs. The scheme does not rely on the third-party database and saves the cost of maintaining the central database. At the same time, it can avoid the risk of a centralized malicious attack brought by centralization.

7) RESIST COLLUSION ATTACK

A novel game-based incentive contract in the process of electricity trading and improving the node's income through the incentive mechanism of a rewarding energy coin. If legitimate EV nodes want to collude with other EV nodes to conduct

TABLE 5. Comparison of the verification delay and transmission overhead between different scheme.

Scheme	Sending n messages	Verifying n signatures
SPRING [6]	189 n bytes	$3nT_{par}+11nT_{mul}$
IBCPPA [7]	833 n bytes	$(2+n)T_{par}+4nT_{mtp}$
EAAP [8]	220 n bytes	$(n+1)T_{par}+(n+4)T_{mtp}$
Our scheme	67 n bytes	$2T_{par}+nT_{mtp}+3nT_{mul}$

passive trading or illegal attacks, the incentive of energy coins will be reduced, resulting in the inability to provide funds for electricity trading and forcing other nodes to give up colluding to attack.

B. COMPARISON OF VERIFICATION DELAY AND COMMUNICATION OVERHEAD

In electricity transactions, performance overhead mainly includes the communication overhead of sending a signed message and the verification overhead after receiving the message. As shown in Table 5, a comparison of the communication overhead and verification overhead of our solution with the other three scenarios is summarized. T_{par} represents the time of the bilinear pairing operation, T_{mul} represents the time of the point multiplication operation on the elliptic curve, and T_{mtp} represents the time of the map-to-point Hash operation.

If 20 bytes of the size of the original message is not considered, the communication overhead generally includes the identification information of the vehicle, the certificate, the time stamp, and the pseudonym. Among them, SPRING sends a message communication overhead including 40-byte signature, 121-byte certificate, 26-byte key and 2-byte ID, a total of 189 bytes. The IBCPPA communication overhead has a signature of 826 bytes, a 3-byte ID and a 4-byte timestamp, for a total of 833 bytes. The communication overhead of EAAP contains a 20-byte signature, a 20-byte public-key, and a 180-byte certificate for a total of 220 bytes. However, our proposed scheme only requires a 21-byte signature and a 42-byte pseudonym, as well as a 4-byte timestamp, for a total of 67 bytes. More specifically, our scheme is more advantageous than the other three solutions.

As shown in Fig. 7, the communication overhead of our scheme and the other three schemes increases linearly with the increase of sending messages. Through comparative analysis, we can see that the communication overhead caused by sending the same number of messages accounts for only 35.45% of SPRING, 8.04% of IBCPPA, and 30.45% of EAAP. Therefore, our scheme can save a minimum of 64.55% in communication overhead.

We implement the previously described method [38] for the MNT curve [21] with an embedding degree of 6, which is expressed in the order of 160 bits. The experiments were carried out with Intel Pentium IV 3.0-GHZ system, and the running time of the following operations was obtained: $T_{par} = 4.5$ ms, $T_{mtp} = 0.6$ ms, $T_{mul} = 0.6$ ms.

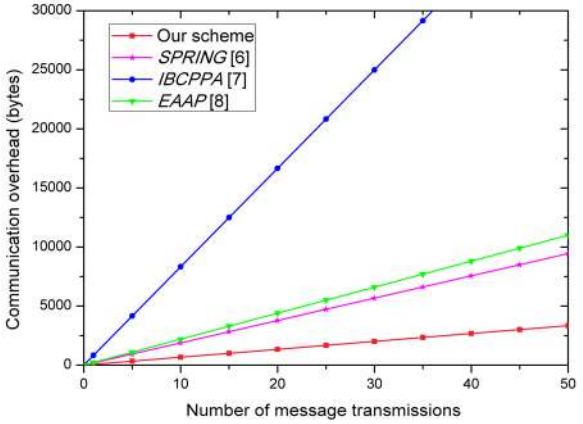


FIGURE 7. Communication overhead and number of messages transmissions.

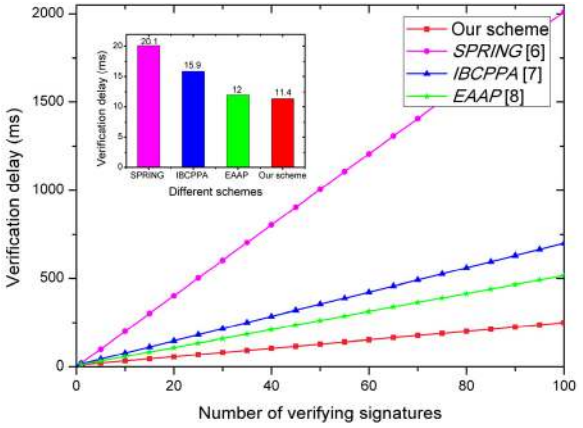


FIGURE 8. Verifying the delay and number of signatures verified.

As shown in Fig. 8, the comparison of the verification delay times between different schemes when verifying n signatures. We substitute the T_{par}, T_{mtp} and T_{mul} values into table 5 and calculate the delay time of signature verification for each scheme respectively. As can be seen from the figure, as the number of signatures increases, the advantage of our scheme in delay time becomes more obvious.

C. PERFORMANCE EVALUATION OF INCENTIVE CONTRACTS

In order to effectively evaluate our proposed new model, we built a simulation environment based on MATLAB simulation software to test the performance of our method in terms of incentive revenue.

Our analysis of a novel game-based incentive scheme [39] and the experiment several times. According to the agreement of vehicle revenue reward and energy consumption coin in this paper, the parameters of the simulation are set as follows. Since $p_{11} + p_{10} + p_{01} + p_{00} = 1$ in the strategy space of game group EV_s and EV_p, it is assumed that the probability of each strategy is the same, that is, $p_{ij} = q_{ij} = 0.25$. Assuming that the average number of vehicles participating in the game is 2, the parameter $\theta = 2$ in the Poisson distribution, and

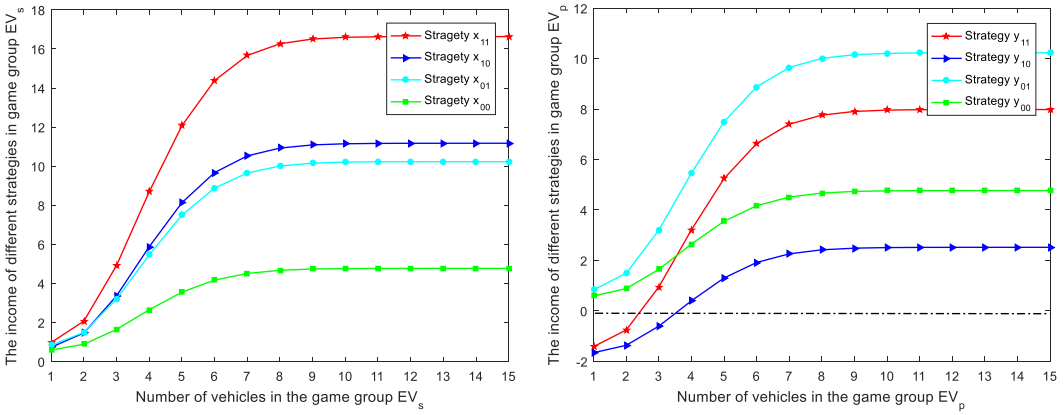


FIGURE 9. (a) and (b) respectively represent the impact of the increase of different vehicle numbers on revenue in the game group of EV_s and EV_p.

since the probability of two EVs connecting is relatively large under normal circumstances, that is, ε is set to 0.8. Revenue parameters $e_{sell} = 6$, $e_{receive} = 4$, $e_{r-upload} = 5$, and energy consumption parameters $e_{buy} = 6$, $e_{cha-discha} = 3$, $e_{c-upload} = 2$ were set. Table 6 lists the value of parameter in this simulation. All set parameters are substituted into formulas (13) and (14) for calculation, and are drawn as shown in Fig. 9 (a).

We calculate the return function of EV_s selection strategy x_{11} and EV_p selection strategy y_{11} respectively, as shown in the following formulas, and others are similar. As can be seen from the above figure, if EV_s choose the strategy x_{00}, the gain obtained is the smallest, the selection strategy x_{11} obtains the largest gain, and the selection strategy x_{10} is slightly larger than the benefit of the selection strategy x_{01}.

Therefore, if the vehicle wants to get more revenue, it needs more contribution electricity and upload information, in line with our incentive setting. And as the number of gaming vehicles increases, the revenue will stabilize at a fixed value.

$$
\begin{aligned}
U_{11}^{s} &= p_{11}[(e_{sell} + e_{r-upload} + e_{receive}) \\
&\quad \times \sum\nolimits_{\lambda_1}^{\infty} P(X = \lambda_1) P_{11}^{s} - (e_{cha-discha} + e_{c-upload})] \\
&= 0.25[(6 + 5 + 4) * \frac{e^{-2}}{0.25} * (\frac{(e^2 - e^{2*0.8})}{2} \\
&\quad - \sum_{i=1}^{\lambda_1 - 1} \frac{0.25^{i-1}(1 - 0.8^i)}{i!}) - (3 + 2)] \\
&= 7.5(1 - e^{-0.4}) - 15e^{-2} \sum_{i=1}^{\lambda_1 - 1} \frac{0.25^{i-1}(1 - 0.8^i)}{i!} - \frac{5}{4}
\end{aligned}
$$

$$
\begin{aligned}
U_{11}^{p} &= q_{11}[(e_{r-upload} + e_{receive}) \sum\nolimits_{\lambda_2}^{\infty} P(X = \lambda_2) P_{11}^{p} \\
&\quad - (e_{buy} + e_{cha-discha} + e_{c-upload})] \\
&= 0.25[(5 + 4) * \frac{e^{-2}}{0.25} * (\frac{e^2 - e^{2*0.8}}{2} \\
&\quad - \sum_{i=1}^{\lambda_2 - 1} \frac{0.25^{i-1}(1 - 0.8^i)}{i!}) - (6 + 3 + 2)] \\
&= 4.5 * (1 - e^{-0.4}) - 9e^{-2} \sum_{i=1}^{\lambda_2 - 1} \frac{0.25^{i-1}(1 - 0.8^i)}{i!} - \frac{11}{4}
\end{aligned}
$$

TABLE 6. Initial value of simulation parameter setting.

Parameter	Value	Parameter	Value
p_{ij}	0.25	q_{ij}	0.25
θ	2.00	ε	0.80
e_{sell}	6.00	e_{buy}	6.00
$e_{receive}$	4.00	$e_{cha\text{-}discha}$	3.00
$e_{r\text{-}upload}$	5.00	$e_{c\text{-}upload}$	2.00

As can be seen from Fig. 9 (b) above, in the initial stage, due to the purchase of electricity by EV_p, The selection of strategies y_{11} and y_{10} requires the payment of energy coins. However, with the increase of the number of game vehicles, there will eventually be benefits, and the order of the strategies for the selection of income from small to large is $y_{01} > y_{11} > y_{00} > y_{10}$, which is in line with our incentive setting. The same gain will eventually stabilize at a fixed value.

For the optimal game x_{ij}^* or y_{ij}^* of the strategy set x_{ij} or y_{ij}, vehicle groups EV_s and EV_p participating in the game satisfy.

$$U_{ij}^{s*}(x_{ij}^*) \geq U_{ij}^{s}(x_{ij}), \quad \forall x_{ij} \neq x_{ij}^*. \tag{17}$$

$$U_{ij}^{p*}(y_{ij}^*) \geq U_{ij}^{p}(y_{ij}), \quad \forall y_{ij} \neq y_{ij}^*. \tag{18}$$

Therefore, the above formulas (17) and (18) satisfy the Nash equilibrium [39] of game group EV_s and EV_p. The results of the above two group game test experiments show that the incentive contract model in this paper can effectively stimulate the nodes to cooperate.

VII. CONCLUSION

Based on the basic operating rules of China's electricity market and rules for consumer particiation. Electricity suppliers with licenses and consumers approved by electricity regulatory departments may participate in regional market transactions, and electricity dispatching agencies are responsible for electricity dispatching, electricity market trading, and metering. We propose a secure electricity trading and incentive contract model. In this model, the message is digitally signed during electricity transactions to guarantee the non-repudiation and security of the data. PBFT consensus algorithm is applied to develop the efficiency of consensus and the speed of transaction confirmation. Data is packaged into blocks and stored on the energy blockchain, and the encryption algorithm ensures tamper-proof. In order to improve the enthusiasm of trading between vehicles, a novel incentive contract based on income and reward is proposed. Eventually, security analysis and performance evaluation show that we have the advantage of lower communication overhead and shorter latency than other recent schemes. Moreover, the incentive contract model that rewards energy coins can advance the active interaction enthusiasm of vehicles. Our results will provide the general public and EV owners with more affordable charging strategies and portable services, as well as ease of management for policymakers. Predictably, our results can also be projected to some other EV-intensive countries. However, malicious vehicles are willing to sacrifice rewards to upset the balance of the system. In future work, we will further research the punishment measures for malicious vehicles to make the system more stable.

REFERENCES

[1] K. M. Tan, V. K. Ramachandaramurthy, and J. Y. Yong, "Integration of electric vehicles in smart grid: A review on vehicle to grid technologies and optimization techniques," *Renew. Sustain. Energy Rev.*, vol. 53, pp. 720–732, Jan. 2016.

[2] W. Han and Y. Xiao, "Privacy preservation for V2G networks in smart grid: A survey," *Comput. Commun.*, vol. 91, pp. 17–28, Oct. 2016.

[3] (May 2018). *The Global Electric-Vehicle Market Is Amped on the Rise*. Accessed: Jan. 25, 2019. [Online]. Available: https://www.mckinsey.com/-industries/automotive-and-assembly/our-insights/the-global-electric-vehicle-market-is-amped-up-and-on-the-rise

[4] C. Gouveia, D. Rua, F. J. Soares, C. Moreira, P. G. Matos, J. A. P. Lopes, "Development and implementation of Portuguese smart distribution system," *Electr. Power Syst. Res.*, vol. 120, pp. 150–162, Mar. 2015, doi: 10.1016/j.epsr.2014.06.004.

[5] E. Sortomme and M. A. El-Sharkawi, "Optimal combined bidding of vehicle-to-grid ancillary services," *IEEE Trans. Smart Grid*, vol. 3, no. 1, pp. 70–79, Mar. 2012.

[6] R. Lu, X. Lin, and X. Shen, "SPRING: A social-based privacy-preserving packet forwarding protocol for vehicular delay tolerant networks," in *Proc. 29th IEEE INFOCOM*, San Diego, CA, USA, Mar. 2010, pp. 1229–1237.

[7] J. Shao, X. Lin, R. Lu, and C. Zuo, "A threshold anonymous authentication protocol for VANETs," *IEEE Trans. Veh. Technol.*, vol. 65, no. 3, pp. 1711–1720, Mar. 2016.

[8] M. Azees, P. Vijayakumar, and L. J. Deboarh, "EAAP: Efficient anonymous authentication with conditional privacy-preserving scheme for vehicular ad hoc networks," *IEEE Trans. Intell. Transp. Syst.*, vol. 18, no. 9, pp. 2467–2476, Sep. 2017.

[9] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, Blockchain and anonymous messaging streams," *IEEE Trans. Depend. Sec. Comput.*, vol. 15, no. 5, pp. 840–852, Sep./Oct. 2018.

[10] N. Saxena, S. Grijalva, V. Chukwuka, and A. V. Vasilakos, "Network security and privacy challenges in smart vehicle-to-grid," *IEEE Wireless Commun.*, vol. 24, no. 4, pp. 88–98, Aug. 2017.

[11] Z. Zhou, B. Wang, Y. Guo, and Y. Zhang, "Blockchain and computational intelligence inspired incentive-compatible demand response in Internet of electric vehicles," *IEEE Trans. Emerg. Topics Comput. Intell.*, vol. 3, no. 3, pp. 205–216, Jun. 2019.

[12] O. Novo, "Blockchain meets IoT: An architecture for scalable access management in IoT," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1184–1195, Apr. 2018.

[13] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.

[14] J. Kang, R. Yu, X. Huang, S. Maharjan, Y. Zhang, and E. Hossain, "Enabling localized peer-to-peer electricity trading among plug-in hybrid electric vehicles using consortium blockchains," *IEEE Trans. Ind. Informat.*, vol. 13, no. 6, pp. 3154–3164, Dec. 2017.

[15] Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang, "Consortium blockchain for secure energy trading in industrial Internet of Things," *IEEE Trans. Ind. Informat.*, vol. 14, no. 8, pp. 3690–3700, Aug. 2018.

[16] L. Li, J. Liu, L. Cheng, S. Qiu, W. Wang, X. Zhang, and Z. Zhang, "CreditCoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles," *IEEE Trans. Intell. Transp. Syst.*, vol. 19, no. 7, pp. 2204–2220, Jul. 2018.

[17] T. Zhang, H. Pota, C.-C. Chu, and R. Gadh, "Real-time renewable energy incentive system for electric vehicles using prioritization and cryptocurrency," *Appl. Energy*, vol. 226, pp. 582–594, May 2018.

[18] N. Fan, Y. Zhu, and G. Zhu, "Game models of forwarding traffic information for vehicular networks," in Chinese, *Comput. Eng. Des.*, vol. 39, no. 8, pp. 2422–2426 and 2563, Aug. 2018.

[19] V. S. Miller, "Use of elliptic curves in cryptography," in *Proc. Conf. Theory Appl. Cryptograph. Techn.* Berlin, Germany: Springer, Dec. 1985, pp. 417–426.

[20] N. Torri and K. Yokoyama, "Elliptic curve cryptosystem," *FUJITSU Sci. Tech. J.*, vol. 36, no. 2, pp. 140–146, 2000.

[21] A. Miyaji, M. Nakabayashi, and S. Takano, "Characterization of elliptic curve traces under FR-reduction," in *Proc. Int. Conf Inf. Secur. Cryptol.* Berlin, Germany: Springer, 2000, pp. 90–108.

[22] S. Nakamoto. (2008). *Bitcoin: A Peer-to-Peer Electronic Cash System*. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[23] Y. Yuan and F.-Y. Wang, "Blockchain: The state of the art and future trends," *Acta Autom. Sinica*, vol. 42, no. 4, pp. 481–494, 2016.

[24] X. Huang, C. Xu, P. Wang, and H. Liu, "LNSC: A security model for electric vehicle and charging pile management based on blockchain ecosystem," *IEEE Access*, vol. 6, pp. 13565–13574, 2018.

[25] Y. Hou, Y. Chen, Y. Jiao, J. Zhao, H. Ouyang, P. Zhu, D. Wang, and Y. Liu, "A resolution of sharing private charging piles based on smart contract," in *Proc. 13th Int. Conf. Natural Comput., Fuzzy Syst. Knowl. Discovery (ICNC-FSKD)*, Jul. 2017, pp. 3004–3008.

[26] C. Xu, K. Wang, and M. Guo, "Intelligent resource management in blockchain-based cloud datacenters," *IEEE Cloud Comput.*, vol. 4, no. 6, pp. 50–59, Nov./Dec. 2017.

[27] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling blockchain: A data processing view of blockchain systems," *IEEE Trans. Knowl. Data Eng.*, vol. 30, no. 7, pp. 1366–1385, Jul. 2018.

[28] D. Gregoratti and J. Matamoros, "Distributed energy trading: The multiple-microgrid case," *IEEE Trans. Ind. Electron.*, vol. 62, no. 4, pp. 2551–2559, Apr. 2015.

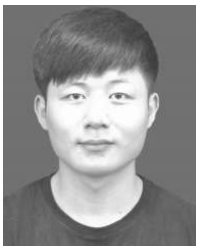
[29] J. F. Nash, Jr., "Equilibrium points in n-person games," *Proc. Nat. Acad. Sci. USA*, vol. 36, no. 1, pp. 48–49, 1950.

[30] Z. Zhou, B. Wang, M. Dong, and K. Ota, "Secure and efficient vehicle-to-grid energy trading in Cyber physical systems: Integration of blockchain and edge computing," *IEEE Trans. Syst., Man, Cybern., Syst.*, to be published.

[31] H. Chen, Y. Li, Z. Han, and B. Vucetic, "A Stackelberg game-based energy trading scheme for power beacon-assisted wireless-powered communication," in *Proc. ICASSP*, Apr. 2015, pp. 3177–3181.

[32] Y. Yuan and F.-Y. Wang, "Towards blockchain-based intelligent transportation systems," in *Proc. 19th IEEE Int. Conf. Intell. Transp. Syst. (ITSC)*, Rio de Janeiro, Brazil, Nov. 2016, pp. 2663–2668.

[33] W. Ren, R. W. Beard, and E. M. Atkins, "Information consensus in multi-vehicle cooperative control," *IEEE Control Syst. Mag.*, vol. 27, no. 2, pp. 71–82, Feb. 2007.
[34] T. Crain, V. Gramoli, M. Larrea, and M. Raynal, "DBFT: Efficient byzantine consensus with a weak coordinator and its application to consortium blockchains," 2017, *arXiv:1702.03068*. [Online]. Available: https://arxiv.org/abs/1702.03068
[35] J. Petit, F. Schaub, M. Feiri, and F. Kargl, "Pseudonym schemes in vehicular networks: A survey," *IEEE Commun. Surveys Tuts.*, vol. 17, no. 1, pp. 228–255, Mar. 2015.
[36] H. Li, "The scheme of anonymous signature and batch verification in vehicular ad hoc networks," (in Chinese). *Comput. Appl. Softw.*, vol. 30, no. 1, Jan. 2013.
[37] C. Dong, Y. Wang, A. Aldweesh, P. McCorry, and A. Moorsel, "Betrayal, distrust, and rationality: Smart counter-collusion contracts for verifiable cloud computing," in *Proc. ACM Conf. Comput. Commun. Secur.*, 2017, pp. 211–227.
[38] M. Scott. (2009). *Efficient Implementation of Cryptographic Pairings*. [Online]. Available: http://ecryptss07.rhul.ac.uk/Slides/-Thursday/mscott-samos07.pdf
[39] Q. Xu, Z. Su, and S. Guo, "A game theoretical incentive scheme for relay selection services in mobile social networks," *IEEE Trans. Veh. Technol.*, vol. 65, no. 8, pp. 6692–6702, Aug. 2016.



XIAOFENG CHEN received the B.S. degree in communication engineering from the Jiangxi University of Science and Technology, Jiangxi, China, where he is currently pursuing the M.S. degree in electronics and communication engineering with the Jiangxi University of Science and Technology, Jiangxi. His current researches include blockchain technology and information security.

XIAOHONG ZHANG received the B.S. degree in physics from Jiangxi Normal University, Jiangxi, China, in 1984, the M.S. degree in optical information processing from the Chinese Academy of Sciences, Changchun, China, in 1990, and the Ph.D. degree in control theory, information safety, from the University of Science and Technology Beijing (USTB) and Beijing University of Posts and Telecommunications (BUPT), in 2002 and 2006, respectively. She was a Visiting Scholar with the University of California, Berkeley, CA, USA, from 2014 to 2015. She is currently a Full Professor with the Department of College of Information Engineering, Jiangxi University of Science and Technology, Ganzhou, China. Her main research interests are blockchain technology, information security, nonlinear dynamics, and wireless sensor networks.