ingegneria sismica
International Journal of Earthquake Engineering
Anno XLIII - Num. 1 - 2026

Cross-domain Data Security Protection System for New Energy Vehicle Shared Charging Piles Constructed on the Basis of Blockchain Technology

Yi Pan[1,*], *Yajuan Guo*[1], *Mingshen Wang*[1] *and Xiaodong Yuan*[1]

[1] Electric Power Research Institute, State Grid Jiangsu Electric Power Co., Ltd., Nanjing, Jiangsu, 211103, China

SUMMARY: *In recent years, new energy vehicle ownership and charging loads have shown a rapid upward trend, and the amount of data on charging platforms has increased dramatically. However, the traditional centralized data storage method will be more and more difficult to cope with the increasing massive data. For this reason, blockchain technology is introduced, and a charging transaction data storage scheme is designed by using blockchain technology to select a number of charging stations as data center nodes in the new energy vehicle charging platform. In this shared charging pile cross-domain data security protection system running consensus process adopts EPBFT consensus algorithm, the data center nodes use the consensus mechanism between the encrypted data for decentralized synchronous storage. Finally, relevant experiments verify the effectiveness of the cross-domain data security protection system for shared charging piles of new energy vehicles proposed in this paper. In the security performance test experiments, the time-consuming method of this paper can meet the efficiency requirements of new energy vehicle charging data aggregation scenarios, and at the same time, it ensures that the charging data aggregation process is not tampered with and privacy protection. In the operation efficiency comparison experiments, the protocol proposed in this paper in the generation of authentication messages needed to increase the random number of four times the elliptic curve on the multiplier operation, authentication messages and other comparative schemes compared to the length of the token there is a significant reduction in the signature checking process is more efficient advantage. In the charging right allocation analysis, by adding the credit value method, this paper's method can improve the reasonableness of the charging right allocation of each charging station, and at the same time, it can incentivize each charging station to obtain a higher credit value through better quality service. This proves the superiority of the system designed in this paper.*

KEYWORDS: *blockchain technology; charging platform; decentralization; EPBFT consensus algorithm; new energy vehicle*

1 Introduction

With the strengthening of environmental policies, electric vehicles, which use clean and renewable energy, will gradually become the mainstream of travel tools. Electric vehicles not only have the advantages of low noise and low price, but also can reduce air pollution caused by oil consumption and harmful gas emissions [1-3]. Vehicle-to-grid (V2G) network, as the main component of smart grid, realizes the two-way flow of information and electricity between

*jsdkyp@163.com
https://doi.org/10.65102/is2026012
Published: 30 April, 2026

electric vehicles and the grid, and the smart, convenient and low-cost features of electric vehicles have attracted the attention of researchers [4]. Since EVs communicate through public networks while enjoying charging/discharging services, this may cause many privacy and security risks, such as message tampering, spoofing or denial of service (DoS) and man-in-the-middle attacks that lead to malfunctioning of charging services, and identity tracking, and illegal export of location information that lead to leakage of private information [5]. These attacks threaten the confidentiality and integrity of exchanged information, user privacy, and the security of electric vehicles. On the other hand, charging pile equipment in EV charging stations may have an impact on public safety and user privacy and information security due to vulnerabilities such as hardware damage and sensitive data theft [6]. Therefore, it is essential to design an efficient and secure authentication system for V2G networks to ensure data integrity and confidentiality.

So far, most of the new energy vehicle shared charging pile service providers in China adopt a centralized operation model, i.e., the charging piles are centrally managed by the service providers, and there are certain problems with this transaction management model: the management and maintenance of transaction data and transaction process by the transaction center bring high costs [7]; there is a mistrust problem between the transaction center and the users participating in the transaction, and the over-centralization will lead to the collection of a large amount of user privacy [8]; centralized database brings the risk of transaction data being tampered with, which not only harms the interests of the transaction parties, but also threatens the security of the transaction data [9]; charging pile service providers are endless and lack of a unified management approach, each service provider has its own standards and usage specifications, which brings certain difficulties to the users [10]. Blockchain, as a distributed ledger, allows nodes to realize peer-to-peer services in an untrustworthy distributed network [11]. Therefore, the blockchain system can fulfill the two-way needs of privacy protection and identity authentication of users in the charging pile environment.

However, considering the mobility of EVs, users can drive their EVs to different areas or choose different charging service operators to request charging services, due to the differences in authentication modes and certificate forms among different charging service operators [12-14]. This results in significant segregation of EV users' authentication, forming multiple trust domains and causing users to need to re-register in order to gain the trust of the authentication center [15]. How to realize efficient and secure cross-domain authentication of electric vehicle users among different charging service operators is a problem worth studying.

To address the data privacy security and protection of electric vehicles in V2G communication, researchers have proposed many authentication schemes for V2G communication, which not only focus on the security of the protocol, but efficiency is also one of the design priorities. Abdallah and Shen [16] analyzed the security and privacy issues in V2G communication and proposed an authentication scheme based on bilinear mapping technique, which achieves the bi-directional authentication in V2G communication, which ensures that the communicating peer entities have legitimate identities and can effectively resist masquerade attacks. Roman et al [17] proposed an authentication protocol for managing and distributing keys in V2G networks, which is based on groups for managing keys, elliptic curves for sharing keys, and bilinear pairing, which achieves authentication of EVs while guaranteeing communication confidentiality. Rajasekaran et al [18] designed an anonymous authentication protocol to verify the identity of EV users and charging stations, a blockchain based transmission mechanism protocol between charging stations to ensure the transmission of confidential information of the users, and an effective revocation mechanism was proposed in order to achieve the removal of malicious charging stations from the V2G network. Eiza et al

[19] investigated the security and privacy issues when using mobile IP communication in V2G networks and proposed a mobile agent IPv6 protocol that uses blind signatures based on the RSA algorithm in conjunction with built-in tagging technology to achieve mutual authentication between the vehicle and the server and vehicle traceability. Chen et al [20] proposed an effective privacy-preserving data aggregation and dynamic pricing service in V2G IoT by designing an identity-based sequential aggregation of signature data based on factorization and threshold homomorphic encryption, which not only successfully decrypts aggregated power consumption data, but also protects the personal privacy of EV users, and even prevents malicious charging stations and malicious EV users from collusion between malicious charging stations and malicious EV users.

In cross-domain data authentication, different solutions have been proposed in different domains. Among the traditional solutions, there are two main frameworks, one is the key-based authentication scheme and the other is the traditional certificate-based authentication scheme [21, 22]. Among the key-based authentication schemes, Park et al [23] proposed a dynamic privacy-preserving scheme for V2G communication in the Internet of Things (IoT) as well as a lightweight key negotiation protocol, which aims to enhance the security of the V2G system to ensure that the user's privacy is not compromised, and at the same time, provide an efficient key management mechanism to adapt to the resource constraints of the IoT environment. Gope and Sikdar et al [24] proposed a privacy-preserving and key negotiation scheme in the energy Internet, which utilizes hash functions to reduce the computational complexity during authentication, and users and service providers securely interact with each other through negotiated symmetric keys. Ahmed et al [25] developed a secure and scalable authentication key negotiation scheme for V2G communication environments using signed and unsigned techniques, while using only one-way hash functions and XoR operations to make the protocol lightweight. Su et al [26] proposed a privacy-preserving scheme considering the communication efficiency and untrustworthy third party problem during authentication in V2G networks, which uses non-singular elliptic curves to build a lightweight authentication protocol between the vehicle and the grid, while the third-party organization negotiates the master key of the system with the dispatch center using a secure two-party protocol to prevent internal attacks. Vijayakumar et al [27] proposed an anonymous authentication method for identity privacy preservation, which improves the existing authentication support for electric vehicles, and then proposed an anonymous key distribution protocol that distributes the group key to a group of vehicles within the communication range of the roadside unit (RSU).

Among the authentication schemes based on traditional certificates, Bansal et al [28] proposed an authentication scheme based on Physical Unclonable Function (PUF) in V2G, which realizes two-way authentication between EVs, charging piles, and grid servers based on the uniqueness of the device's physical configuration, while the scheme improves the efficiency of authentication with the use of lightweight cryptographic primitives under the premise of guaranteeing security. Li et al [29] proposed Portunes+, an authentication protocol that provides location privacy through the use of pseudonyms, which achieves fast authentication by relying on a symmetric key and the spatio-temporal location of the new energy vehicle, the above scheme does not consider the trust between entities. Sureshkumar et al [30] analyzed the vulnerabilities in the SU scheme and proposed an efficient authentication protocol using elliptic curve ciphers to provide mutual authentication and session key establishment between EVs, charging stations and charging service operators. Stichow and Rempel [31] presented a comprehensive framework for cybersecurity vulnerabilities in the authentication chain of EV charging stations, focusing on data security threats to the shared charging point protocol (OCPP) and including simulation tests for user spoofing attacks. Garg et al [32] proposed an innovative layered authentication mechanism, which is based on blockchain technology and aims to

enhance secure communication between vehicles, charging piles, and the central aggregator, which utilizes elliptic curve cryptographic algorithms to ensure that all parties can achieve mutual authentication during the authentication process, and thus enhance the overall system's security and protection performance. Luo et al [33] incorporate authentication into key distribution without the need for a trusted third party in order to prevent eavesdropping attacks from compromising the confidentiality of the transmitted information and propose a novel split transmission strategy where sensitive data is divided into multiple segments and forwarded to a centralized system over different random communication links. Xia et al [34] proposed a billing identity authentication scheme based on fog computing, where the fog server verifies the user's identity and saves the relevant power information before charging and discharging the electric vehicle, and in order to improve the authentication efficiency, the scheme adopts the fog computing technology so that the number of interactions between the user and the cloud server is greatly reduced.

Considering the mobility characteristics of EVs, the movement of EVs between regions may bring about changes in the authentication trust domains, and in order to make the authentication scheme more scalable, there is a need to integrate multiple trust domains in the distributed authentication architecture and implement authentication between different trust domains for EVs [35-37]. To address this problem, in the study by Bhattacharya et al [38], a dynamic pricing mechanism is implemented by incorporating a non-cooperative game model to achieve a Nash equilibrium for energy trading between electric vehicles and charging stations, and by optimizing the consensus mechanism within the blockchain the efficiency of the energy trading can be improved, inter-vehicle communication delays can be reduced, and the security and utility of the energy trading system can be improved. Dorokhova [39] designed a smart contract-based optimization algorithm to adjust the charging current based on the current battery level of the EV, the expected departure time, and the availability of renewable energy at the charging station, which maximized the PV self-consumption rate of the charging station to meet the charging demand of the EVs and reduced the charging cost. Pratt and Carroll [40] stated that EV charging infrastructure is vulnerable to cyber-attacks and the principles of EV charging infrastructure security (VCIS) include segregating network communications, continuous monitoring, verifying the consistency of the physical and cyber state, and responding to threats, so information sharing among stakeholders is essential for data security protection.

Recent studies have shown that secure, efficient and transparent power transactions, protection of user privacy and anonymity, optimization of energy allocation and pricing strategies, as well as improvement of system scalability and performance can be achieved through the integration of blockchain with multiple technologies in EV charging scenarios [41-43]. Blockchain enables decentralized management of personal data to protect users' privacy from misuse or disclosure and enables dynamic authorization of identity [44]. For example, Patil [45] proposed an authentication protocol based on blockchain technology and PUF technology, which utilizes smart contracts in the blockchain to defend against data tampering attacks and to ensure the security and privacy of data in the connected car. Yao et al [46], on the other hand, introduced fog services and third parties to build a blockchain and investigated a cross-domain privacy authentication method for electric vehicles, but in the process of cross-domain authentication, multiple servers repeatedly check in order to ensure trustworthy cooperation with each other, which results in a large amount of communication overhead and latency. In a study by Sun et al [47], a power trading system based on multiple federated blockchains is proposed, which utilizes a node voting mechanism to enhance the consensus efficiency, in addition to a public verification mechanism based on BLS (Boneh Lynn Shacham) threshold signatures ensures the consistency and trustworthiness of the output results. Guan et

al [48] proposed an efficient data aggregation scheme based on blockchain for privacy protection of users' electricity consumption data in smart grids, in which Bloom filters are used to achieve fast authentication of identity information, which has higher security performance and communication efficiency compared to other schemes. Ferreira et al [49] applied blockchain technology to enable autonomous identity management, allowing EV users to control digital identities using decentralized logos and verifiable credentials for authentication and transactions, while blockchain supports data traceability and ownership tracking to ensure traceability and auditability of data usage activities and permissions. Shen et al [50] proposed BASA, an efficient blockchain-assisted secure device authentication mechanism for cross-domain IIoT, which improves on the identity management mechanism proposed by Identity-Based Cryptography (IBC) and enables the authenticated device to remain anonymous. Kim et al [51] proposed a blockchain based secure charging system for electric vehicles based on this, which ensures key security, secure two-way authentication, anonymity, forward secrecy, and provides efficient billing, and the scheme prevents replay attacks and man-in-the-middle attacks.

Firstly, the article gives an overview of blockchain technology, introduces the development history of blockchain technology and the basic structure of blocks, and discusses in depth the elliptic curve encryption algorithm, homomorphic encryption algorithm, secure multi-party computation and other algorithms. Secondly, it elaborates on the operation process of the shared charging pile cross-domain data security protection system, adopts the EPBFT consensus algorithm in the consensus process of the system, and proposes a charging transaction data storage scheme by selecting a number of charging stations as data center nodes in the new energy vehicle charging platform by using blockchain technology. Finally, a series of experiments are conducted to experimentally verify the performance of the cross-domain data security protection system for new energy vehicle sharing charging pile proposed in this paper in terms of security, consensus and charging right allocation.

2 Shared charging pile cross-domain data security protection system design

2.1 Blockchain

The block structure of blockchain 2.0 is shown in Figure 1. In a blockchain network, all transactions collected by a node over a period of time are packaged to form a block. Finally, an orderly arrangement of blocks forms a blockchain. Blockchains can be categorized into three types: public chains, which allow anyone to join or leave, such as Bitcoin and Ether. Then there are federated chains, which are mainly used for cooperation between commercial organizations. The key feature of a federated chain is that the entry and exit of nodes is strictly controlled. Finally, there are private chains, which, although less widely used, are primarily suited to large commercial entities.

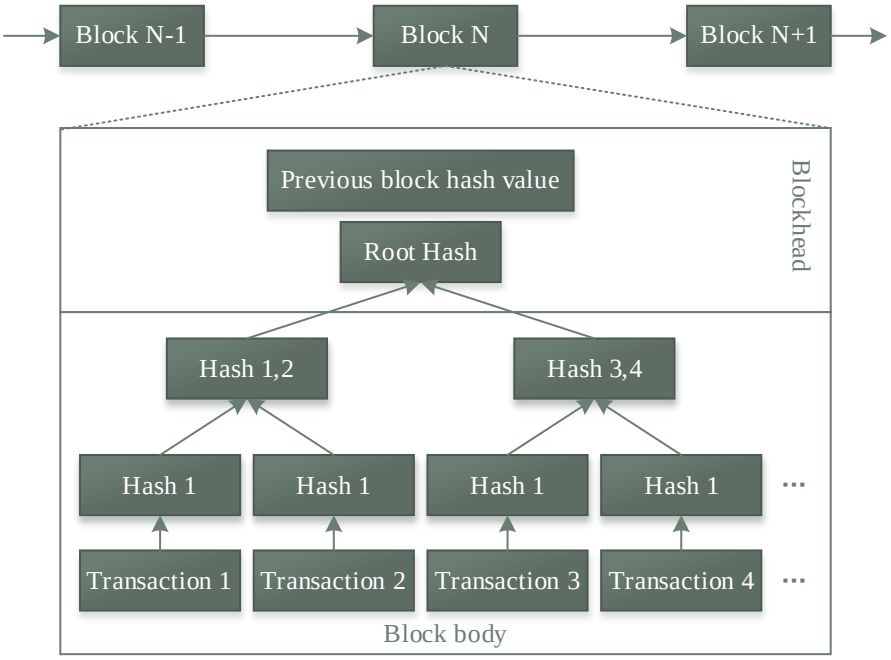

Figure 1: The block structure of Blockchain 2.0

2.2 Components of blockchain technology

2.2.1 P2P network protocols

The core concept of the P2P network protocol is that all nodes in the network communication have equal status, there is no specialized server or client, or each node acts as both a server and a client.1311 At the same time, it is interconnected with the gRPC services of other nodes, and thus acts as both a server and a client. Although this implementation satisfies the concept of node peering in the P2P protocol, it is not suitable for large public chains. For public chains, the number of nodes they face is much larger than that of federated chains, which means that the number of connections faced by the nodes building the gRPC service may increase exponentially. With the expansion of network scale, gRPC service may not be able to meet the demand. On the other hand, existing public chain platforms such as Ether adopt KAD DHT technology, which utilizes cryptographic methods to represent the distance between two nodes instead of physical spatial distance.

2.2.2 Elliptic Curve Encryption Algorithm

The use of encryption algorithms can not be separated from the hash (HASH), its main role is to convert an indefinite length of data into a fixed length of the hash value. the basic principle of ECC is to choose an elliptic curve as the basis of the encryption operation, through the definition of the point of the arithmetic rules to realize the encryption and decryption.

The ellipse in ECC is defined in such a way that a finite field $Fp = \{0,1,2,\ldots,p-1\}$, p is given as a large prime number, and there are p elements in Fp, which satisfy the following equation.

$$\begin{cases} y^2 = \left(x^3 + ax + b\right) (\mathrm{mod}\ p) \\ 4a^3 + 27b^2 \neq 0 (\mathrm{mod}\ p) \end{cases} \tag{1}$$

where a, b, x, y - Fp are all elements in.

mod p - both sides of the equation are equal after modeling p separately.

An ellipse consists of a finite number of points, denote the elliptic curve as $E_p(a,b)$.

The steps of elliptic curve encryption algorithm are as follows:

(1) Construct an ellipse. Choose Fp as a finite area and define an elliptic curve $E_p(a,b)$ on Fp, choose a point G on the curve as a base point, define the infinite point of the ellipse to be $O\infty$, and find the smallest integer n such that $n*G = O_\infty$, then n is the order of the base G.

(2) Generate the public and private keys. An integer k_{pri} is chosen in the range $[1, n-1]$ and this integer k_{pri} is the private key. The public key is obtained from the private key by a simple calculation $K_{pub} = k_{pri} \times G$.

(3) The process of encryption by elliptic curve encryption algorithm. Let Alice have private key k_{pri}, public key K_{pub}, elliptic curve $E_p(a,b)$, and base point G. Alice only keeps the private key, and sends the remaining three elements to Bob, who can complete the encryption of the data to be encrypted m by performing the following operations. Find the point M of m on the ellipse M, generate a random number r, and compute $C_1 = M + rK_{pub}, C_2 = r*G$. Get the ciphertext C_1, C_2 to send to Alice.

(4) Elliptic curve algorithm decryption process. alice only needs to compute $C_1 - k_{pri} * C_2$ to get the ciphertext.

2.2.3 Consensus Algorithms

Consensus is crucial in decentralized blockchain networks as it is the basis for achieving data consistency. Consensus algorithms are also known as distributed consistency algorithms. Consensus algorithms are usually categorized into two types: strong consistency and eventual consistency. Strong consistency is often difficult to implement or performs poorly when implemented. Therefore, in application domains where the requirement for consistency is relatively low, the requirement for consistency can be appropriately reduced and final consistency algorithms can be used. Consensus algorithms that can reach agreement within a specific time frame are called final consistency consensus algorithms.

Consensus algorithms are usually categorized into two main groups: the Paxos family and the Byzantine fault-tolerant family.The Paxos family assumes that there are only faulty nodes in a distributed system and no malicious nodes. On the contrary, Byzantine fault tolerance tolerates both faulty and malicious nodes. While the general distributed consensus problem can be solved with the Paxos algorithm, the consensus of a blockchain requires the Byzantine fault-tolerant consensus algorithm. The main difference between a federated chain and a public chain is the choice of consensus algorithm.

2.2.4 Homomorphic encryption algorithms

Homomorphic encryption enables computation without decryption of the ciphertext.Paillier homomorphic encryption algorithm has significant advantages. The following is a brief description of the Paillier algorithm process.

(1) Generate public and private keys, the owner user has the pair of public and private keys which are used to encrypt and decrypt the text. Randomly choose two large primes p and q, p and q are unequal such that $n = pq$, and then randomly choose an integer g within

the range of $\left[2, n^2\right]$, and utilize Equation (2) to generate the public key (n, g) and private key (λ, μ).

$$\begin{aligned} &\lambda = lcm(p-1)(q-1) \\ &L(x) = (x-1)/n \\ &\gcd\left(L\left(g^2 \bmod n^2\right), n\right) = 1 \\ &\mu = \left(L\left(g^2 \bmod n^2\right)\right)^{-1} \bmod n \end{aligned} \tag{2}$$

where $\gcd(\cdot)$ - find the greatest common divisor of the input data.

$\mathrm{lcm}(\cdot)$ - find the least common multiple of the input data.

(2) Encryption process. The plaintext m and a random integer r are chosen to first satisfy $m < n$ and $0 < r < n$ and $\gcd(r, n) = 1$. Then the ciphertext c is obtained from equation (3) and is written as the function $\mathrm{E}(m)$.

$$c = \mathrm{E}(m) = g^m \cdot r^n \bmod n^2 \tag{3}$$

(3) Decryption process. The decrypted message is denoted as asm and is written as a function $\mathrm{D}(m)$.

$$asm = \mathrm{D}(m) = \mathrm{L}\left(c^{\lambda \bmod n^2}\right) \mu \bmod n \tag{4}$$

For homomorphism verification, there are two arbitrary plaintexts m_1 and m_2, and two positive integers r_1 and r_2 are randomly generated, corresponding to the ciphertexts $c_1 = \mathrm{E}\left(m_1, r_1\right), c_2 = \mathrm{E}\left(m_2, r_2\right)$. This can be introduced according to the encryption formula.

$$\begin{aligned} c_1 \cdot c_2 &= \left(g^{m_1} \cdot r_1^n \bmod n^2\right) \cdot \left(g^{m_2} \cdot r_2^n \bmod n^2\right) \\ &= g^{m_1 + m_2} \cdot \left(r_1 \cdot r_2\right)^n \bmod n^2 \end{aligned} \tag{5}$$

Comparing the encryption and decryption formulas, it can be seen that $c_1 \cdot c_2$ decrypted results in $m_1 + m_2$. From this we can conclude that when the ciphertext is multiplied, the plaintext contained is added exponentially, so after decryption we can get the result of plaintext addition.

2.2.5 Safe multiparty calculations

Secure Multi-Party Computing (SMPC) is a data privacy-preserving method of comparing sizes that can be used to solve the famous millionaire problem. In SMPC, each participant only knows his/her own private data, while the other participants do not know these data and learn the size result through a series of their own calculations. Thus, SMPC allows multiple participants to perform calculations without revealing their private data.

SMPC includes several protocols, the most basic of which is the secret sharing protocol. The most basic protocol is the secret sharing protocol, which allows multiple participants to

share a secret, and each participant only knows a part of the secret, and it requires the cooperation of multiple participants to restore the complete secret. The secret sharing protocol can be used to implement other protocols of SMPC, such as encryption protocols and comparison protocols.

In SMPC, the security of protocols is usually realized by techniques such as homomorphic encryption and zero-knowledge proofs. These techniques ensure the correctness of computation and confidentiality of data, thus ensuring the security of SMPC.

In this paper, we use secure multi-party computation to solve the millionaire problem, so as to order the orders according to the bidding level under the condition of protecting the privacy of the owner's bidding, so that the owner-users can get a good charging experience.

2.2.6 Smart Contracts

The main goal of smart contracts is to automate the execution of common contractual conditions, minimize malicious behavior and surprises, and reduce reliance on trusted intermediaries. Digital contracting means expressing everyday contracts in code. Distributed finite state machines imply that in a distributed system, if all nodes have the same starting state and the same state transition conditions, they will eventually reach a consistent result.

Therefore, smart contracts must be deterministic in nature, and consensus cannot be reached if the outcome between nodes is not consistent. This property ensures that smart contracts always produce the same output for a given input. The structure of a smart contract is shown in Figure 2. Contracts are stored in the blockchain as bytecode instructions, usually written in Go or Solidity languages. When the parties sign the contract, the program code of the smart contract is stored in the blockchain.

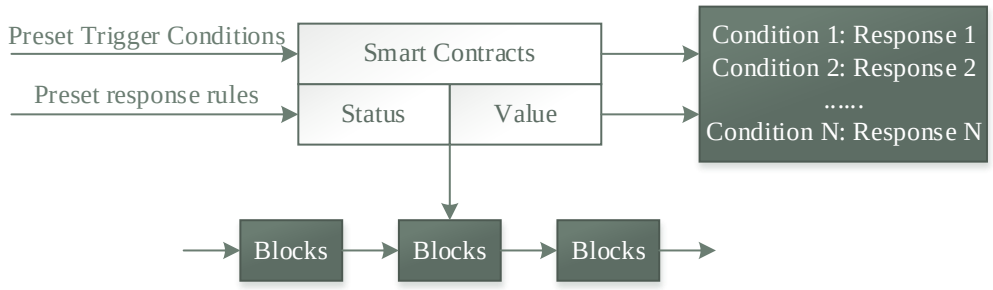

Figure 2: Smart contract configuration

2.3 Shared charging pile cross-domain data security protection system operation process

The charging data storage platform stores the data generated by each user in the data center set up in the new energy vehicle charging station. The charging data is collected by the charging pile and uploaded to the data center, and the data is encrypted after the user reviews the data to protect the data security. The symbols used and their meanings are shown in Table 1.

Table 1: The corresponding meanings of each symbol

Symbol	Meaning
CS_i	The i-th charging station
DC_j	The j-th data center
$PK_i, SK_i, Cert_i$	The public key, private key and certificate
U_i	The i-th user e
$Timestamp$	Timestamp
$i \to j$	i sends the information to j
$E_{PKi}(m)$	m is encrypted by public key i
$Sign_{Ski}(m)$	Sign the information m with the private key i
$Hash(m)$	Hash the information m

(1) System initialization and key distribution: When the system is initialized, each charging pile is set as a blockchain node by the system administrator, and the corresponding chaotic number and public and private keys of each node are distributed to each charging pile, denoted as $\left\{i, PK_{CS_i^k}, SK_{CS_i^k}\right\}$.

(2) Uploading charging data: the charging pile CS_1 will request transaction data uploading to the data center DC_1 inside the charging station after the collected data is encrypted by the user's confirmation and the request message contains the digital signature Sig_1 of CS_1 as a proof that the transaction data is valid. Upon receiving the message, DC_1 verifies it and allows the CS_1 to upload the encrypted charging data after confirming that it is correct. The user U first encrypts the charging $Data$ of CS_1 after verifying it using his personal public key $PK_{U_i^k}$, then CS_1 encrypts it using the public key of the current codename pseudonym $PK_{CS_1^k}$, and signs it using his own private key, and finally the DC_1 encrypts the recorded message using its own public key PK_{DC_1} to get the final data FR_data that can be written to the blockchain, the specific process described above is as follows:

$$\begin{aligned} &CS_1 \to DC_1: \\ &FR\_data_1 = E_{PK_{DC_1}}\left(Data_i \| Sig_1 \| timestamp\right) \end{aligned} \tag{6}$$

Among them:

$$Data_i = E_{PK_{CS_1^k}}\left(E_{PK_{U_i^k}}(Datal \| timestamp)\right) \tag{7}$$

$$Sig_1 = Sign_{SK_{CS_1^k}}\left(Data_i\right) \tag{8}$$

(3) Charging station data center aggregates the uploaded data from charging piles: DC_1 verifies the FR_data uploaded from all charging piles, and if the data Data is safe and valid,

it can be stored in DC_1. If the validation is not passed, the data will be received directly.

(4) Charging station data center workflow: after a period of time, the local data center DC_1 packages all the qualified FR_data during this period of time into a dataset denoted as:

$$Data_{set} = \{FR\_datas \| timestamp\} \tag{9}$$

(5) Block consensus process between data centers in the charging station: the consensus process adopts EPBFT consensus algorithm, and the data storage platform can designate any data center as the master node, and the remaining m data center will become the slave node. The flow of EPBFT algorithm is shown in Fig. 3.

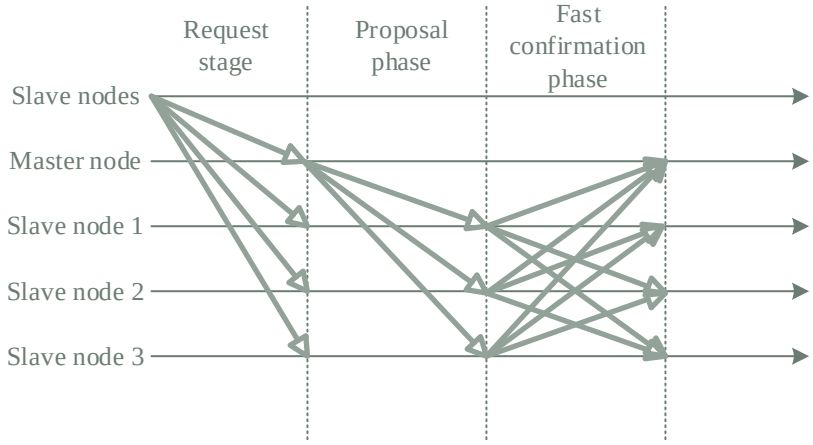

Figure 3: The EPBFT algorithm process

Step 1 A slave node data center broadcasts and sends a $Data_{set}$ to all nodes in the blockchain platform, each consensus node receives the transaction and verifies the legitimacy of the transaction, and if it is legitimate, caches it. The master node waits until it receives enough data or until after a time interval to generate a $Block$.

Step 2 DC_1 generates a proposal message M for the generated block, assigns a number n and appends a signature message DC_1 of $Sign_{SK_{DC_1}}$ as well as the hash value of the block after hashing $Hash_{Block}$ for other nodes to review and verify its contents. The message is then broadcast to all slave nodes set up in the blockchain in the format $< n, Sign_{SK_{DC_1}}, Hash_{Block}, Block, timestamp >$, where $Block$ is the block that requires consensus. The slave node $i \in \{0,1,\cdots,m\}$ examines the proposal message after receiving it, and if it agrees with the proposal message, it enters the fast confirmation phase. The specific process described above is as follows:

$$\begin{aligned} &DC_1 \to m: \\ &M =< n, Sign_{SK_{DC_1}}, Hash_{Block}, Block, timestamp > \end{aligned} \tag{10}$$

Among them:

$$Hash_{Block} = Hash\left(Block \| timestamp\right) \tag{11}$$

Step 3 Fast validation phase. After the data storage platform enters the quick confirmation phase, each data center will broadcast their audit results and their respective digital signatures to the slave nodes of other data centers to achieve the purpose of mutual supervision and verification. The format of the fast confirmation message is $< Fast\_Confirm, n, j >$, where j is the other data center's own number. The completion of the fast confirmation phase is signified by DC_1 receiving $2f+1$ fast confirmation messages consistent with M from other different data centers, and if sufficient fast confirmation messages are not received by the timeout, the block will be discarded. It is expressed as follows:

$$\begin{aligned} &DC_j \to m: \\ &Fast\_Confirm = E_{PK_{DC_j}}\left(Data_j \left\| Sig_{DC_j} \right\| timestamp\right) \end{aligned} \tag{12}$$

Among them:

$$Data_j = \left(M \| V\_results\right) \tag{13}$$

$$Sig_{DC_j} = Sign_{SK_{DC_j}}\left(Data_j, j\right) \tag{14}$$

Step 4 When the data center DC_1 completes the fast confirmation phase, the block is sent to the slave nodes on the blockchain along with all corresponding digital signatures. Thereafter, the data block will be written into the blockchain platform in an in-block timestamp order. The specific process described above is as follows:

$$\begin{aligned} &DC_1 \to All: \\ &Data_{block} = \left(Data_n \left\| Sig_{DC_1} \cdots Sig_{DC_j} \right\| timestamp\right) \end{aligned} \tag{15}$$

Among them:

$$Data_n = \left(Data_{sets} \| Data_{hash} \| timestamp\right) \tag{16}$$

(6) User data authorization sharing process

The real holders of the data on the data storage platform are the operation platform and the relevant users, and each user encrypts the data with his/her personal private key when it is generated, and the user has the right to control whether his/her personal data is shared with others or not. In this paper, data sharing is guaranteed to be legitimate and fair through user authorization to write into the blockchain.

The data sharing mainly includes the following process: when the operation platform requests the user to use the data and obtains the user's consent, the user needs to access the data storage platform to use the private key to unveil his data and write it to the blockchain. Each data center first needs to verify the user's identity, and after consensus is reached, the user decrypts the corresponding data and reuses the public key of the platform's data center to encrypt and write it into the storage platform. The specific expressions are as follows:

$$\begin{aligned} &U_i \rightarrow All: \\ &Request = \left(Data_r \left\| Cert_i \right\| timestamp \right) \end{aligned} \tag{17}$$

Among them:

$$Data_r = \left(D_{SK_{U_i^k}} \left(E_{PK_{U_i^k}} \left(Data_i \| \ timestamp_i \right) \| \ timestamp_i \right) \right. \tag{18}$$

$$\begin{aligned} &DC_1 \rightarrow All: \\ &M = \left(Data_{seti} \left\| Cert_i \right\| timestamp \right) \end{aligned} \tag{19}$$

3 Experimental analysis

3.1 Analysis of safety performance

To verify the effectiveness of the algorithm in this paper, this section tests the method of this paper in an arithmetic example system containing 10 regions with 78 charging piles in each region. The simulation is done on a personal computer with Intel i7-10700 CPU and 16GB RAM, and the functional code of the data aggregation algorithm is developed based on Matlab, which simulates the computing process of each node and the communication process between nodes, so as to test the anti-tampering performance and privacy protection performance of this paper's method and compare the aggregation efficiencies of this paper's method (Shared Charging Pile Cross-domain Data Security protection system), the aggregation method based on PBFT consensus blockchain, and the aggregation efficiency of the direct aggregation method. In the method of this paper, it is assumed that each encrypted aggregation group contains 7 encrypted representatives and the threshold value is taken as q = 3.

3.1.1 Tamper-resistant performance validation

In the method of this paper, the malicious representatives in both encryption aggregation groups 1 and 2 tamper with their calculated ciphertext charging scheme aggregation results. At the decryption submission layer, the decryption master representative receives the tampered results from the encrypted aggregation groups 1 and 2, and receives the correct results from the other encrypted aggregation groups. The region 2 aggregation charging load enumeration is shown in Fig. 4. In this paper's algorithm, each decryption representative can enumerate to get 16 times the same decryption result as the actual aggregation load, while all other incorrect decryption results are enumerated only once, so the non-malicious decryption representative will get the correct decryption result. Since the number of malicious representatives among all decryption representatives is not more than 1/3, the grid enterprise can receive enough correct aggregated charging load results, thus ensuring the correctness of the aggregation results. As a comparison, if the aggregation method based on PBFT consensus blockchain is adopted, the correctness of the aggregation results of the charging data in region 2 cannot be guaranteed due to the proportion of malicious representatives in the regional aggregation group in region 2 is more than 1/3. If the direct aggregation method is adopted, it is impossible to prevent the tampering behavior of the data aggregation center in region 2.

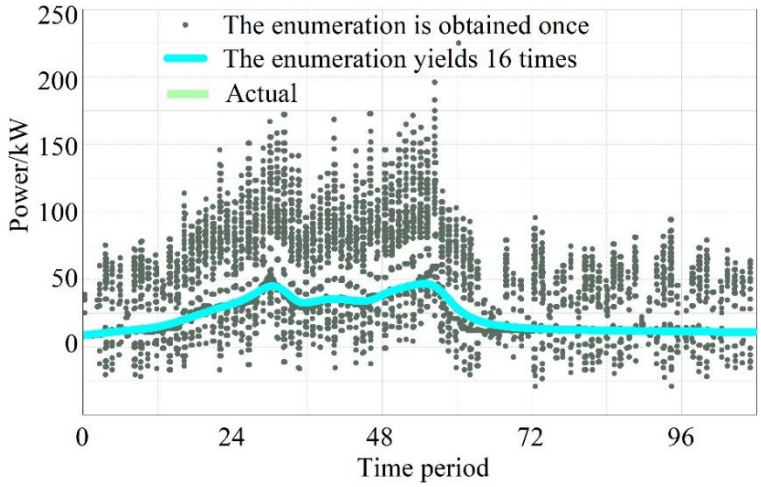

Figure 4: The enumeration of aggregated charging loads in Area 2

3.1.2 Privacy protection performance validation

To verify the privacy protection performance of the algorithm in this paper, the actual charging plan of a charging pile in region 1 and the ciphertext charging plan received by the encrypted representatives in aggregation groups 1 and 2 are shown in Fig. 5. As can be seen from the figure, the malicious representatives in aggregation groups 1 and 2 can only receive the ciphertext charging plan that is significantly different from the actual charging plan of the charging pile. At the same time, since the malicious representatives cannot get hold of a sufficient number of ciphertext charging plans, they cannot decrypt the charging pile charging plan information through the formula. In contrast, if the aggregation method based on PBFT consensus blockchain is adopted, any malicious representative in the regional aggregation group in region 1 can get hold of the actual charging plan of the charging pile and leak it. If the direct aggregation method is adopted, the data aggregation center in region 1 can directly obtain the actual charging plan information of the charging pile, which leads to the risk of potential privacy exposure.

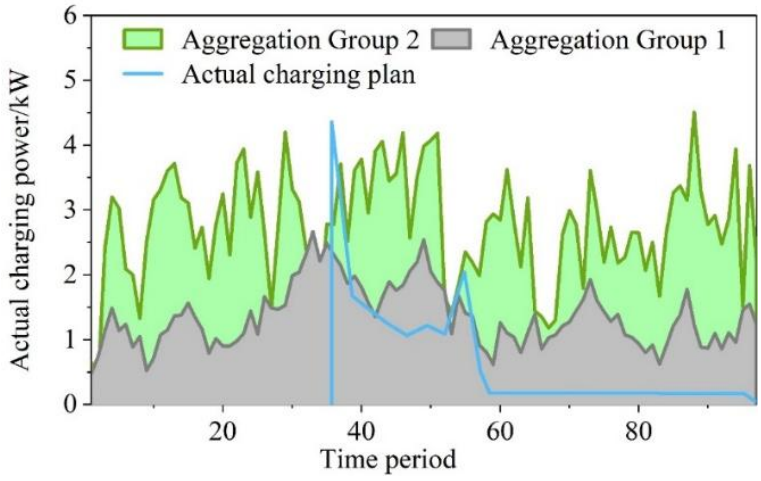

Figure 5: Actual coal charging piles and ciphertext charging plans

3.1.3 Charging data aggregation efficiency test

This section compares and tests the aggregation efficiency of this paper's method, the aggregation method based on PBFT consensus blockchain and the direct aggregation method.

Among them, the aggregation group and representative node settings under the aggregation method based on PBFT consensus blockchain are consistent with the method in this paper.

Comparison of time consuming aggregation operations of different charging data aggregation methods is shown in Table 2. Among them, all the times are obtained by taking the average value of 10 tests. As can be seen from the table, compared with the direct aggregation method, the aggregation time consumed by the two blockchain-based aggregation methods, PBFT consensus-based aggregation method and this paper's method, is significantly increased, which is mainly due to the need to spend a longer time for multiple rounds of cross-communication between representative nodes in the blockchain environment. Compared with the PBFT consensus-based aggregation method, the aggregation time of this paper is longer, which is mainly due to the fact that this paper requires the decrypted delegates to perform enumeration computation at the decryption submission layer, which leads to longer time consumption. However, the time consumption of this method can still meet the efficiency requirements of the new energy vehicle charging data aggregation scenario. It should be noted that the extra time consumed by this method compared with other traditional aggregation methods can also be regarded as the price of efficiency that must be paid to ensure that the charging data aggregation process is tamper-proof and privacy-protecting.

Table 2: The aggregation of different aggregation methods is time-consuming

Aggregation method	Time consumption /s
Direct aggregation.	0.15
Based on PBFT consensus aggregation	1.06
Text method	1.36

3.2 Protocol Performance Analysis

This section analyzes the performance of the P2P network protocol proposed in this paper, and compares the scheme of this paper with two schemes, namely, the electric vehicle charging transaction model based on the federated blockchain, and a charging pile edge computing system and method based on blockchain technology, from the perspectives of the system overhead and the operation efficiency. The protocols of these two schemes are referred to as Scheme I and Scheme II in the following description, and the protocol proposed in this paper is referred to as Scheme III. In addition, since the protocol uses ECC signature checking algorithm to complete the authentication, the choice of different elliptic curves will have different impacts on the efficiency of the protocol, so the operational efficiency of the protocol under different elliptic curves is compared in the third part.

3.2.1 Analysis of communications overhead

The communication overhead is analyzed in terms of the number of interactions and the number of bytes transmitted. During the execution of the protocol, the lower the number of interactions and the lower the number of bytes transmitted represent the lower communication overhead of the protocol.

The number of interactions in the registration phase and authentication phase of the three schemes is shown in Table 3. From the table, it can be seen that Scheme 1 and Scheme 2 both realize cross-domain authentication based on blockchain certificates, and the certificates in Scheme 2 are generated locally by the user, thus reducing one interaction in the registration phase. The scheme proposed in this chapter combines the authentication message and the authentication token into one message, thus reducing one interaction in the authentication phase.

Table 3: Comparison of the number of interactions among the three schemes

Plan	Number of interactions		
	Registration stage	Certification stage	Total
Plan 1	6	6	12
Plan 2	2	7	9
The plan of this article	3	5	8

3.2.2 Operational efficiency analysis

The number of main operations in the P2P network protocol determines the operational efficiency of the protocol, so firstly, the amount of computation in the authentication process of the three schemes is theoretically analyzed. In scheme 1, the main operations include SM9 signature verification operation and hash operation. In Scheme 2, the main operations include signature verification and hash operation. In Scheme 3, the main operations include the multiplication operation on elliptic curves, signature checking operation, and hash operation. The computational quantities of the three schemes are shown in Table 4. In this paper, the proposed protocol adds four times the multiplication operation on the elliptic curve when generating the random numbers needed for authentication messages, but the authentication messages have a significant reduction in the token length compared with those in Scheme I and Scheme II, so the signature checking process is more efficient and advantageous.

Next, the time overhead of the three schemes was tested in an experimental environment. Scheme 1 is based on the SM9 algorithm for signature verification and SM3 algorithm for hash operation. Scheme 2 and Scheme 3 both use ECC-based signature checking algorithm, hash operation using SHA256, due to the SM9 algorithm in Scheme 1 in the signature checking process used in the bilinear pairs of operations, so although the number of signatures with the scheme signature checking the same number of times, but the time overhead is higher. The time overhead of Scheme 1 signature is 28.2ms, and the time overhead of signature verification is 27.2ms. The time overhead for signing once in scheme 2 and scheme 3 is 5.3ms, and the time overhead for checking the signature once is 5.9ms.

Table 4: Comparison of the main operation quantities of the three schemes

	Option 1	Option 2	Option 3
Elliptic curve doubling operation	0	0	5
Hash operation	3	2	3
Signature verification	2	2	3

3.2.3 Protocol efficiency analysis

The signature and signature verification efficiency of the three curves is tested in the experimental environment. Ten groups of 1000 tests are used, and the average value of the 10 tests is taken. Since the size of the data volume to be signed will also have an impact on the signature verification efficiency, so in the experiment set 128B, 256B, 512B, 1KB, 32KB, 64KB, 128KB, 256KB, 1MB, 4MB total 10 to be signed to verify the signature data volume. The test results of the signature and signature verification algorithm time overhead are shown in Table 5 and Table 6, in milliseconds (ms). As can be seen from the tables, the signature and signature verification time overheads of secp256k1 and secp256r1 are very close to each other, and the time overheads gradually converge with the increase of data volume. In the case of a small amount of data, the gap between the three curves of the time overhead is also very small, but when the amount of signature checking data increases (greater than 1MB), the time overhead of SM2 increases significantly, this is because the hash algorithm used in SM2 is SM3

hash algorithm, the hash process consumes more time with the increase in the amount of data. The secp256k1 curve is chosen as the test parameter for all other experiments in this paper.

Table 5: Signature Algorithm Time Cost Comparison

Data volume	SM2	secp256k1	secp256r1
128B	357.7	388.9	364
256B	363.8	339.5	409.1
512B	381.2	353.7	360.8
1KB	374.3	405.8	340.7
32KB	468.5	454.4	417.5
64KB	656.5	513.7	536.1
128KB	879.9	659.8	708.7
256KB	1381.2	978.8	946.7
1MB	4413.7	2854	2823.4
4MB	16609.5	10306.9	10311.3

Table 6: Comparison of time and cost of signature verification algorithm

Data volume	SM2	secp256k1	secp256r1
128B	411.7	417.7	409.1
256B	391.7	382	418.3
512B	400.7	422.3	403.7
1KB	337.5	417.9	426.5
32KB	505.3	480.7	495.4
64KB	657.9	556.5	578.2
128KB	874.2	718.1	726.5
256KB	1403.4	985.7	1035.2
1MB	4446	2876.3	2861.4
4MB	16669.7	10292.1	10264.7

3.3 Consensus Performance Analysis

3.3.1 System performance analysis

(1) Performance of credit assessment metrics

In this section, three groups of experiments are done for assessing credit of nodes with good credit, average credit and poor credit respectively. By adjusting the weight coefficients of subjective and objective factors, for charging stations with good credit, their subjective factors will occupy a larger proportion, while the objective factors will occupy a smaller proportion. For charging stations with average credit, the subjective and objective factors will have the same weight. These three types of credit are analyzed separately below. However, for a poor credit charging station, the subjective factor will have less weight and the objective factor will have more weight.

The histogram of the 150 evaluated credits obtained by the node with good credit is shown in Fig. 6, and 160 credit iterations are carried out for the charging station with good credit in this chapter, from which it can be seen that the evaluated credits obtained by the charging station with good credit are basically stabilized around 85, and it can be inferred that the credit value of the charging station with good credit rises very quickly in an ideal state.

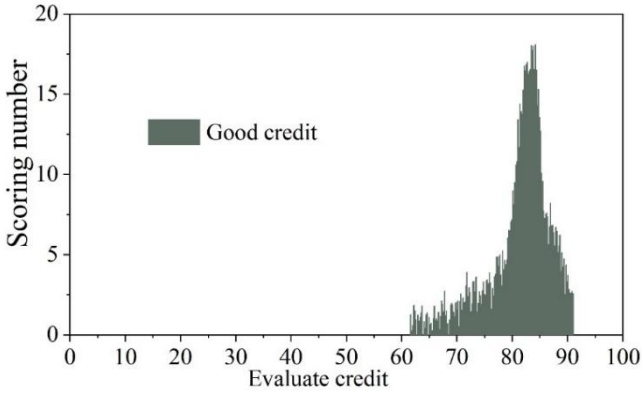

Figure 6: The assessment credit of good credit nodes.

The histogram of assessed credits of charging stations with average credit that have received 160 ratings is shown in Fig. 7, which shows that the assessed credits received by the charging stations are mainly centered in the range of 65-75. Because the node has average credit, it also receives lower ratings, thus the credit value of charging stations with average credit will rise more slowly.

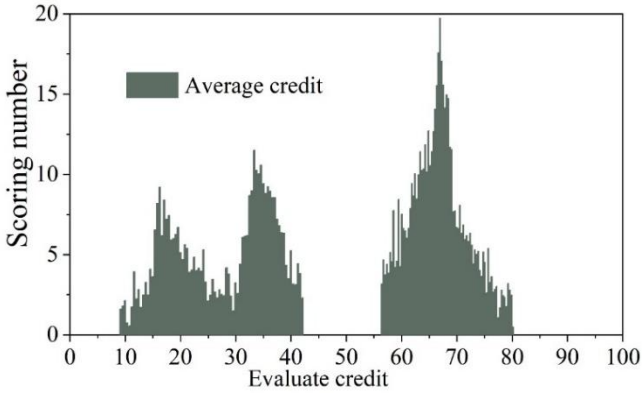

Figure 7: Credit assessment of general credit nodes

The credit histogram of 160 evaluations obtained by poor credit charging stations is shown in Figure 8. Compared with the total evaluation scores obtained by good credit charging stations, the scores obtained by poor credit charging stations are mainly centered around 15-25, which shows that the growth of their credit value scores is very slow.

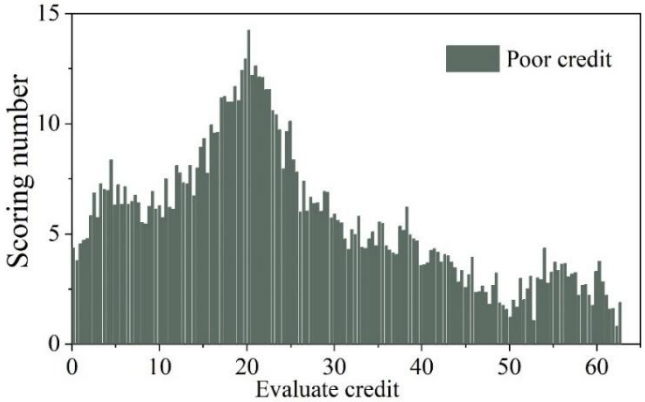

Figure 8: The assessment credit of credit poor nodes

(2) Blockchain bookkeeping right election analysis

The bookkeeping rights are obtained and compared as shown in Table 7.Three groups of experiments are done for comparison when the initial credit value is -5,0,10 respectively. Seven nodes were randomly generated in the experiment, and -5 was set as the lowest initial credit value, and the three groups of experiments were conducted for 1000 times of bookkeeping right election under the same initial credit value, and the number of times of bookkeeping right obtaining was compared under different behaviors with the same initial credit value. In the case of lower credit value or improper behavior, the node still has the chance to be elected as a bookkeeping node. However, the chances of obtaining bookkeeping rights are much lower than for nodes with higher credits.

Table 7: The right to keep accounts is compared

Initial credit value	Credit status	200	400	600	800	1000
-5	Good credit	14.307	23.792	40.294	62.184	75.993
	Average credit	6.452	12.224	26.689	37.419	59.491
	Poor credit	0.000	5.840	12.654	20.283	31.420
0	Good credit	17.470	31.401	49.278	69.703	87.351
	Average credit	7.029	22.589	35.577	47.190	64.380
	Poor credit	0.000	6.570	15.611	23.048	30.025
10	Good credit	27.334	54.873	70.662	81.494	113.990
	Average credit	5.671	23.905	45.603	57.963	79.321
	Poor credit	5.671	9.677	10.934	14.024	18.981

3.3.2 Consensus Delay Analysis

Block consensus delay as shown in Table 8, it can be clearly seen that the length of the delay is positively correlated with the change in the size of the lower block, the more block data, the more significant delay. It can also be seen that when different lower chains are uplinked at the same time, the delay varies significantly. And relative to the size of each block in the lower chain, the more the number of blocks uploaded at the same time in the lower chain, the delay is more obvious, in order to make the upper chain synchronization message delay is reduced, it should be reasonably divided into the lower chain region. In order to reduce the delay of synchronized messages in the upper chain, the lower chain area should be divided reasonably. It is most suitable when the lower chain area is 4-8.

Table 8: Block consensus delay

	128 k	256 k	256 k	1024k
1	2.688	4.032	6.452	8.871
2	1.989	6.129	8.548	14.785
3	2.688	7.849	14.086	22.366
4	4.032	9.946	17.204	30.323
5	6.129	10.968	22.366	43.763
6	7.527	14.785	31.022	56.237
7	8.172	16.505	36.183	78.333
8	9.946	21.344	46.183	100.108
9	12.366	27.903	57.258	128.118
10	13.387	32.742	67.634	152.634
11	15.806	42.043	84.194	185.108

3.4 Charging rights allocation analysis

The charging load curves of each type of new energy vehicle are shown in Figure 9. From the figure, it can be seen that the daily charging load of new energy cabs reaches a low point at about 3:00 a.m., while at 9:30 a.m. and 19:00 p.m. there is a peak, which reaches 130 and 85kW respectively, which is due to the phenomenon that there are single and double shifts for cabs, and the two types of shifts adopt different charging modes. New energy private car daily charging valley is generally around 8:00, and at 20:00 in the evening there is a charging peak and reached 63kW, according to the user's daily travel situation can be analyzed the load peak and valley situation, 19:00 or so at the end of the work period, so there will be a period of peak charging, while the work time will not have a peak period. Since the new energy bus has a fixed travel time, the curve type is similar to the typical daily load curve of the region, and there will be two peak charging periods in the morning peak of work and after the evening.

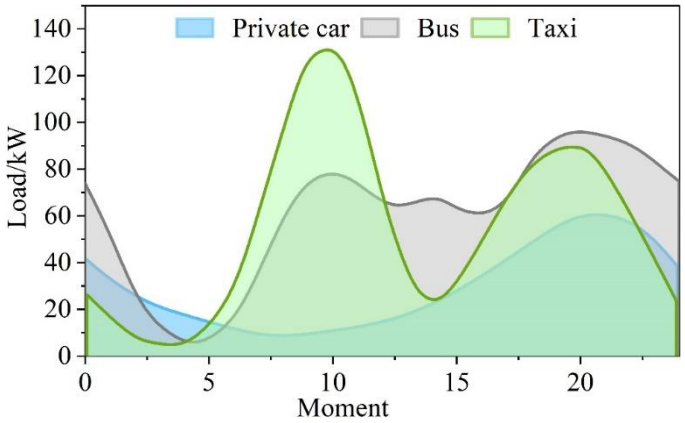

Figure 9: Charging load curves for various types of new energy vehicles

By calculating the total daily charging load, the charging right allocation is analyzed by taking the loads in two time periods. According to the daily charging load curve of new energy vehicles and the assumed maximum daily load of the substation in addition to the base load, two time periods, 9:00-10:00 and 20:00-21:00, are selected for the analysis of charging right allocation. The middle value of the total charging demand in 9:00-10:00 and 20:00-21:00 is taken as the total charging demand in this time period, and the total demand in 9:00-10:00 and 20:00-21:00 is 223.57kW and 225.8kW, respectively. A1, A2, A3, A4, A5, A6, A7 and A8 are used to represent the eight charging stations set up, and the integrated credit value and charging demand assigned to each charging station are shown in Table 9.

Table 9: Comprehensive credit value and charging demand

Charging station	Credit value	9:00-10:00 charging demand/kW	20:00-21:00 charging demand/kW
A1	86	14.73	12.06
A2	66	31.92	31.2
A3	77	39.39	42.99
A4	82	15.04	12.99
A5	85	26.28	26.74
A6	78	29.7	28.56
A7	87	33.17	37.47
A8	88	33.34	33.79

First of all, the charging right between 9:00-10:00 is allocated, from the above it can be seen that the total charging demand in this period is 223.57kW, through the formula it can be concluded that the total demand is within the maximum tolerable range of the transformer in this area, there will be no overloading phenomenon, so through the demand directly on the charging right of each charging station to be allocated. The allocation results are shown in Table 10.

Table 10: The allocation results of charging rights at each charging station

Charging station	9:00-10:00 charging demand/kW	9:00-10:00 Charge allocation/kw
A1	14.73	14.73
A2	31.92	31.92
A3	39.39	39.39
A4	15.04	15.04
A5	26.28	26.28
A6	29.7	29.7
A7	33.17	33.17
A8	33.34	33.34

The results of the charging right allocation for each charging station during overload are shown in Table 11. From the table, it can be seen that the charging rights obtained by A7 and A8 are greater than their own demanded charging, in terms of the credit value, these two charging stations are very high, so they are assigned more charging rights.

Table 11: The distribution results of charging rights at each charging station

Charging station	Credit value	9:00-10:00 charging demand/kW	9:00-10:00 Charge allocation/kw
A1	86	28.84	24.49
A2	66	62.98	47.14
A3	77	27.83	23.47
A4	82	24.84	23.82
A5	85	44.06	35.13
A6	78	33.28	29.27
A7	87	23.1	23.74
A8	88	17.54	21.56

The analysis of the charging right allocation can well illustrate the superiority of the allocation mechanism designed in this paper, which can not only improve the reasonableness of the charging right allocation of each charging station, but also motivate each charging station to obtain higher credit value through better quality service by adding the credit value method.

4 Conclusion

This paper proposes a cross-domain data security protection system for shared charging pile based on blockchain technology. It also demonstrates the superiority of the method proposed in this paper in terms of privacy protection and charging rights through experiments. The conclusions drawn in the article are:

The probability of a node using the strategy proposed in this paper to be elected as a

bookkeeping node at the 500th election of bookkeeping right is less than 0.25, and the competition for bookkeeping right among nodes is fairer, which prevents malicious nodes from obtaining the bookkeeping right in an improper way. After 160 credit iterations for the charging station with good credit, it is found that the evaluation credit obtained by the charging station with good credit is basically stabilized at about 85, and it is inferred that the credit value of the charging station with good credit rises very quickly under the ideal state.

This paper verifies the feasibility and superiority of the system designed in this paper through a series of experiments, and the proposed charging data storage platform can realize the decentralized storage of charging station data with a small cost, which solves the security problems faced by the transaction data under the centralized mode of storage.

Funding

This work was supported by The Science and Technology Project of State Grid Jiangsu Electric Power Co., Ltd. (J2024132).

About the Author

Yi Pan was born in Jiangsu, P.R. China, in 1993. He obtained PH.D from Southeast University in China. I am currently working at Electric Power Research Institute of State Grid Jiangsu Electric Power Co., Ltd., my main research direction is electric vehicle smart charging, and V2G.

Yajuan Guo was born in Shanxi, P.R. China, in 1975. He obtained a Master's degree from North China Electric Power University in China. I am currently working at Electric Power Research Institute of State Grid Jiangsu Electric Power Co., Ltd., my main research direction is Information, Communication and V2G.

Mingshen Wang was born in Hebei, P.R. China, in 1990. He obtained PH.D from Tianjin University in China. I am currently working at Electric Power Research Institute of State Grid Jiangsu Electric Power Co., Ltd., my main research direction is electric vehicle smart charging, and V2G.

Xiaodong Yuan was born in Jiangsu, P.R. China, in 1979. He obtained a Master's degree from Southeast University in China. I am currently working at Electric Power Research Institute of State Grid Jiangsu Electric Power Co., Ltd., my main research direction is electric vehicle smart charging.

References

[1] Pipitone, E., Caltabellotta, S., & Occhipinti, L. (2021). A life cycle environmental impact comparison between traditional, hybrid, and electric vehicles in the European context. Sustainability, 13(19), 10992.

[2] Graditi, G., Langella, G., Laterza, C., & Valenti, M. (2015, June). Conventional and electric vehicles: A complete economic and environmental comparison. In 2015 International Conference on Clean Electrical Power (ICCEP) (pp. 660-665). IEEE.

[3] Al-Ghaili, A. M., Kasim, H., Aris, H., & Al-Hada, N. M. (2022). Can electric vehicles be an alternative for traditional fossil-fuel cars with the help of renewable energy sources towards energy sustainability achievement?. Energy Informatics, 5(Suppl 4), 60.

[4] Yang, Q., Li, D., An, D., Yu, W., Fu, X., Yang, X., & Zhao, W. (2020). Towards incentive for electrical vehicles demand response with location privacy guaranteeing in microgrids. IEEE Transactions on Dependable and Secure Computing, 19(1), 131-148.

[5] Parameswarath, R. P., Abhishek, N. V., & Sikdar, B. (2023, June). Prevent: A mechanism for preventing message tampering attacks in electric vehicle networks. In 2023 IEEE 97th Vehicular Technology Conference (VTC2023-Spring) (pp. 1-5). IEEE.

[6] Garofalaki, Z., Kosmanos, D., Moschoyiannis, S., Kallergis, D., & Douligeris, C. (2022). Electric vehicle charging: A survey on the security issues and challenges of the open charge point protocol (OCPP). IEEE Communications Surveys & Tutorials, 24(3), 1504-1533.

[7] Aljohani, T., & Almutairi, A. (2024). Modeling time-varying wide-scale distributed denial of service attacks on electric vehicle charging Stations. Ain Shams Engineering Journal, 15(7), 102860.

[8] Li, H., Han, D., & Tang, M. (2020). A privacy-preserving charging scheme for electric vehicles using blockchain and fog computing. IEEE Systems Journal, 15(3), 3189-3200.

[9] Parameswarath, R. P., Gope, P., & Sikdar, B. (2022). User-empowered privacy-preserving authentication protocol for electric vehicle charging based on decentralized identity and verifiable credential. ACM Transactions on Management Information Systems (TMIS), 13(4), 1-21.

[10] Irshad, A., Usman, M., Chaudhry, S. A., Naqvi, H., & Shafiq, M. (2020). A provably secure and efficient authenticated key agreement scheme for energy internet-based vehicle-to-grid technology framework. IEEE Transactions on Industry Applications, 56(4), 4425-4435.

[11] Gabay, D., Akkaya, K., & Cebe, M. (2020). Privacy-preserving authentication scheme for connected electric vehicles using blockchain and zero knowledge proofs. IEEE Transactions on Vehicular Technology, 69(6), 5760-5772.

[12] Kwon, D., Son, S., Park, K., Das, A. K., & Park, Y. (2024). Design of blockchain-based multi-domain authentication protocol for secure ev charging services in v2g environments. IEEE Transactions on Intelligent Transportation Systems.

[13] Yuan, T., He, Y., Xiao, P., Xiao, K., & Wu, B. (2025). A Blockchain-based cross-platform authentication scheme for EV aggregate charging platform. Cybersecurity, 8(1), 64.

[14] Chen, Y., Zhang, J., Wei, X., Wang, Y., & Cui, J. (2024). Cross-domain authentication scheme for vehicles based on given virtual identities. IEEE Internet of Things Journal, 11(9), 15869-15879.

[15] Zhang, H., & Zhao, F. (2023). Cross-domain identity authentication scheme based on blockchain and PKI system. High-Confidence Computing, 3(1), 100096.

[16] Abdallah, A., & Shen, X. S. (2016). Lightweight authentication and privacy-preserving scheme for V2G connections. IEEE Transactions on Vehicular Technology, 66(3), 2615-2629.

[17] Roman, L. F., Gondim, P. R., & Lloret, J. (2019). Pairing-based authentication protocol for V2G networks in smart grid. Ad Hoc Networks, 90, 101745.

[18] Rajasekaran, A. S., Maria, A., Al-Turjman, F., Altrjman, C., & Mostarda, L. (2022). ABRIS: Anonymous blockchain based revocable and integrity preservation scheme for vehicle to grid network. Energy Reports, 8, 9331-9343.

[19] Eiza, M. H., Shi, Q., Marnerides, A. K., Owens, T., & Ni, Q. (2018). Efficient, secure, and privacy-preserving PMIPv6 protocol for V2G networks. IEEE Transactions on Vehicular Technology, 68(1), 19-33.

[20] Chen, L., Zhou, J., Chen, Y., Cao, Z., Dong, X., & Choo, K. K. R. (2020). PADP: Efficient privacy-preserving data aggregation and dynamic pricing for vehicle-to-grid networks. IEEE Internet of Things Journal, 8(10), 7863-7873.

[21] Parameswarath, R. P., Gope, P., & Sikdar, B. (2022). Decentralized identifier-based privacy-preserving authenticated key exchange protocol for electric vehicle charging in smart grid. arXiv preprint arXiv:2206.13055.

[22] Almuhaideb, A. M., & Algothami, S. S. (2022). Efficient privacy-preserving and secure authentication for electric-vehicle-to-electric-vehicle-charging system based on ECQV. Journal of Sensor and Actuator Networks, 11(2), 28.

[23] Park, K., Park, Y., Das, A. K., Yu, S., Lee, J., & Park, Y. (2019). A dynamic privacy-preserving key management protocol for V2G in social Internet of Things. IEEE Access, 7, 76812-76832.

[24] Gope, P., & Sikdar, B. (2019). An efficient privacy-preserving authentication scheme for energy internet-based vehicle-to-grid communication. IEEE Transactions on Smart Grid, 10(6), 6607-6618.

[25] Ahmed, S., Shamshad, S., Ghaffar, Z., Mahmood, K., Kumar, N., Parizi, R. M., & Choo, K. K. R. (2021). Signcryption based authenticated and key exchange protocol for EI-based V2G environment. IEEE Transactions on Smart Grid, 12(6), 5290-5298.

[26] Su, Y., Shen, G., & Zhang, M. (2019). A novel privacy-preserving authentication scheme for V2G networks. IEEE Systems Journal, 14(2), 1963-1971.

[27] Vijayakumar, P., Azees, M., Chang, V., Deborah, J., & Balusamy, B. (2017). Computationally efficient privacy preserving authentication and key distribution techniques for vehicular ad hoc networks. cluster computing, 20(3), 2439-2450.

[28] Bansal, G., Naren, N., Chamola, V., Sikdar, B., Kumar, N., & Guizani, M. (2020). Lightweight mutual authentication protocol for V2G using physical unclonable function. IEEE Transactions on Vehicular Technology, 69(7), 7234-7246.

[29] Li, H., Dán, G., & Nahrstedt, K. (2016). Portunes+: Privacy-preserving fast authentication for dynamic electric vehicle charging. IEEE Transactions on Smart Grid, 8(5), 2305-2313.

[30] Sureshkumar, V., Mugunthan, S., & Amin, R. (2022). An enhanced mutually authenticated security protocol with key establishment for cloud enabled smart vehicle to

grid network. Peer-to-Peer Networking and Applications, 15(5), 2347-2363.

[31] Stichow, A., & Rempel, P. (2024, June). Securing electric vehicle charging stations: A critical analysis of authentication vulnerabilities. In 2024 IEEE 32nd International Requirements Engineering Conference Workshops (REW) (pp. 231-240). IEEE.

[32] Garg, S., Kaur, K., Kaddoum, G., Gagnon, F., & Rodrigues, J. J. (2019, May). An efficient blockchain-based hierarchical authentication mechanism for energy trading in V2G environment. In 2019 IEEE international conference on communications workshops (ICC workshops) (pp. 1-6). IEEE.

[33] Luo, J., Yao, S., Zhang, J., Xu, W., He, Y., & Zhang, M. (2020). A secure and anonymous communication scheme for charging information in vehicle-to-grid. IEEE Access, 8, 126733-126742.

[34] Xia, Z., Fang, Z., Gu, K., Wang, J., Tan, J., & Wang, G. (2021). Effective charging identity authentication scheme based on fog computing in V2G networks. Journal of Information Security and Applications, 58, 102649.

[35] Li, Z., & Sun, Z. (2023, December). A Cross-Domain Authentication Scheme for Electric Vehicle Intelligent Charging for Multiple Power Service Providers. In Proceedings of the 2023 13th International Conference on Communication and Network Security (pp. 26-31).

[36] Li, P., Ma, H., Lai, J., Zhou, D., Huang, L., Li, Y., ... & Fang, J. (2024). BlockPPA: Blockchain-Assisted Privacy-Preserving Authentication for Cross-Domain Electric Vehicle Charging. IEEE Transactions on Vehicular Technology.

[37] Huang, L., Sun, Z., Wu, M., & Zhang, X. (2024, October). A Security Authentication Scheme for Electric Vehicle Charging Reservation in Cross-Service Provider Domains. In 2024 IEEE 24th International Conference on Communication Technology (ICCT) (pp. 1005-1010). IEEE.

[38] Bhattacharya, P., Tanwar, S., Bodkhe, U., Kumar, A., & Kumar, N. (2022). EVBlocks: A blockchain-based secure energy trading scheme for electric vehicles underlying 5G-V2X ecosystems. Wireless Personal Communications, 127(3), 1943-1983.

[39] Dorokhova, M., Vianin, J., Alder, J. M., Ballif, C., Wyrsch, N., & Wannier, D. (2021). A blockchain-supported framework for charging management of electric vehicles. Energies, 14(21), 7144.

[40] Pratt, R. M., & Carroll, T. E. (2019, January). Vehicle charging infrastructure security. In 2019 IEEE International Conference on Consumer Electronics (ICCE) (pp. 1-5). IEEE.

[41] Huang, X., Xu, C., Wang, P., & Liu, H. (2018). LNSC: A security model for electric vehicle and charging pile management based on blockchain ecosystem. IEEE access, 6, 13565-13574.

[42] Chowdhury, A., Shafin, S. S., Masum, S., Kamruzzaman, J., & Dong, S. (2025). Secure electric vehicle charging infrastructure in smart cities: A blockchain-based smart contract approach. Smart Cities, 8(1), 33.

[43] Luo, H., Yu, H., & Luo, J. (2023). PRAFT and RPBFT: A class of blockchain consensus algorithm and their applications in electric vehicles charging scenarios for V2G networks. Internet of things and cyber-physical systems, 3, 61-70.

[44] Wang, J. (2022). A novel electric vehicle charging chain design based on blockchain technology. Energy Reports, 8, 785-793.

[45] Patil, A. S., Hamza, R., Hassan, A., Jiang, N., Yan, H., & Li, J. (2020). Efficient privacy-preserving authentication protocol using PUFs with blockchain smart contracts. Computers & Security, 97, 101958.

[46] Yao, Y., Chang, X., Mišić, J., Mišić, V. B., & Li, L. (2019). BLA: Blockchain-assisted lightweight anonymous authentication for distributed vehicular fog services. IEEE Internet of Things Journal, 6(2), 3775-3784.

[47] Sun, Z., Zhao, P., Wang, C., Zhang, X., & Cheng, H. (2022). An efficient and secure trading framework for shared charging service based on multiple consortium blockchains. IEEE Transactions on Services Computing, 16(4), 2437-2450.

[48] Guan, Z., Si, G., Zhang, X., Wu, L., Guizani, N., Du, X., & Ma, Y. (2018). Privacy-preserving and efficient aggregation based on blockchain for power grid communications in smart communities. IEEE Communications Magazine, 56(7), 82-88.

[49] Ferreira, J. C., Ferreira da Silva, C., & Martins, J. P. (2021). Roaming service for electric vehicle charging using blockchain-based digital identity. Energies, 14(6), 1686.

[50] Shen, M., Liu, H., Zhu, L., Xu, K., Yu, H., Du, X., & Guizani, M. (2020). Blockchain-assisted secure device authentication for cross-domain industrial IoT. IEEE Journal on Selected Areas in Communications, 38(5), 942-954.

[51] Kim, M., Park, K., Yu, S., Lee, J., Park, Y., Lee, S. W., & Chung, B. (2019). A secure charging system for electric vehicles based on blockchain. Sensors, 19(13), 3028.