Computer Modeling in Engineering & Sciences

Tech Science Press

DOI: 10.32604/cmes.2023.029461

ARTICLE

Electricity Carbon Quota Trading Scheme based on Certificateless Signature and Blockchain

Xiaodong Yang[1,4], Runze Diao[1,*], Tao Liu[2], Haoqi Wen[1] and Caifen Wang[3]

[1]College of Computer Science and Engineering, Northwest Normal University, Lanzhou, 730070, China

[2]Institute of China Telecom Wanwei, China Telecom Wanwei Information Technology Co., Ltd., Lanzhou, 730030, China

[3]College of Big Data and Internet, Shenzhen Technology University, Shenzhen, 518118, China

[4]Key Laboratory of Cryptography and Data Analytics, Northwest Normal University, Lanzhou, 730070, China

*Corresponding Author: Runze Diao. Email: 2021222163@nwnu.edu.cn

Received: 20 February 2023 Accepted: 22 May 2023 Published: 17 November 2023

ABSTRACT

The carbon trading market can promote "carbon peaking" and "carbon neutrality" at low cost, but carbon emission quotas face attacks such as data forgery, tampering, counterfeiting, and replay in the electricity trading market. Certificateless signatures are a new cryptographic technology that can address traditional cryptography's general essential certificate requirements and avoid the problem of crucial escrow based on identity cryptography. However, most certificateless signatures still suffer from various security flaws. We present a secure and efficient certificateless signing scheme by examining the security of existing certificateless signature schemes. To ensure the integrity and verifiability of electricity carbon quota trading, we propose an electricity carbon quota trading scheme based on a certificateless signature and blockchain. Our scheme utilizes certificateless signatures to ensure the validity and nonrepudiation of transactions and adopts blockchain technology to achieve immutability and traceability in electricity carbon quota transactions. In addition, validating electricity carbon quota transactions does not require time-consuming bilinear pairing operations. The results of the analysis indicate that our scheme meets existential unforgeability under adaptive selective message attacks, offers conditional identity privacy protection, resists replay attacks, and demonstrates high computing and communication performance.

KEYWORDS

Electricity carbon trading; certificateless signature; blockchain; forgery attack; carbon quota

1 Introduction

More than forty percent of all carbon emissions in China are produced by the electric power industry, making it a significant sector. In addition, according to a report by Ember, a UK-based independent climate think tank, carbon emissions from the power industry reached a new peak in 2021, rising by 778 million tons annually. According to research, limiting carbon emissions in the electricity industry is essential for achieving an early carbon emissions peak [1].

Carbon emissions are considered a commodity in carbon trading, which uses a market mechanism to raise the price of carbon emissions to regulate and lower them and to foster low-carbon, sustainable development. Government departments assign carbon emission quotas [2–4] to each firm in accordance with predetermined guidelines to attain the objectives of "carbon peaking" and "carbon neutrality". Suppose the actual carbon emissions of an enterprise are higher than the initial quota allocated by the government. If an enterprise's actual carbon emissions exceed the initial quota assigned by the government, the enterprise must acquire the additional quota on the carbon trading market. Using energy-saving and emission-reduction technologies, if an enterprise's actual carbon emissions are lower than the government-allocated quota, it can sell and trade the excess carbon quota to generate revenue. Fig. 1 depicts the carbon quota trading procedure between two businesses.

Figure 1: Overview of carbon quota trading

Blockchain technology has the characteristics of immutability and transaction traceability, providing technical support for the realization of secure and trusted carbon quota trading. Zhang et al. [5] established a carbon quota trading model with blockchain technology to ensure the fairness of carbon quota allocation. Zhu et al. [6] proposed a multi-energy primary energy storage optimization configuration model based on blockchain to improve energy self-sufficiency. Ji et al. [7] designed an electricity carbon rights trading mechanism based on an alliance chain to improve the market returns of all participants. Yuan et al. [8] used blockchain technology to build a carbon emission data-sharing platform to realize the traceability and sharing of carbon trading. However, these schemes still suffered from complex key management and low transaction efficiency.

Certificateless signatures maintain the advantages of identity-based cryptographic systems without vital public certificates and can ensure the integrity, identity authentication, and nonrepudiation of carbon quota trading. Electricity carbon quota trading scheme based on certificateless signature and blockchain offers several advantages:

Efficiency: Traditional carbon quota trading requires the involvement of government regulatory bodies for verification and approval, which is time-consuming and costly. However, Certificateless signature and blockchain-based scheme eliminates the need for certificate verification and enables fast, automated transaction verification and settlement, reducing intermediaries and increasing transaction efficiency.

Security: The scheme based on certificateless signature uses digital signatures to verify information authenticity, while blockchain technology ensures the immutability of transaction records, guaranteeing transaction safety and reliability.

Decentralization: The blockchain-based scheme does not require a centralized platform as an intermediary; all transactions are recorded on the blockchain, enhancing transaction transparency and traceability while removing intermediaries.

Compared to traditional schemes, the proposed Electricity Carbon Quota Trading Scheme based on Certificateless Signature and Blockchain has the following advantages:

1. Traditional schemes rely on third-party certificate authorities for identity verification, adding extra time and expense. But the certificateless public key cryptography-based scheme is decentralized and does not require certificate verification, thus enabling faster transactions.

2. The use of digital signature verification ensures transactional authenticity and integrity, while blockchain technology enforces immutability, guaranteeing transaction safety and reliability.

3. Traditional schemes require businesses to purchase a fixed number of carbon quotas. By contrast, the certificateless signature and blockchain-based scheme allow for instantaneous carbon quota trading, making it more flexible.

4. Traditional schemes require payment of multiple types of fees and costs, while the certificateless signature and blockchain-based solution can reduce transaction costs.

In conclusion, the electricity carbon quota trading scheme based on certificateless signature and blockchain provides greater efficiency, security, and decentralization compared to traditional schemes. Researchers have presented several certificateless signature techniques [9–11] in recent years. The user's private key is divided into two pieces for the certificateless signature: a secret value chosen randomly by the user and a partial private key derived by the semi-trusted key generation center (KGC). For the security of certificateless signature schemes, attackers are divided into two categories: one is the attacker that imitates malicious users, usually known as the first type of attacker A1. It can launch public key replacement attacks and mastering user secret values but is unaware of KGC's master key. The KGC attacker is an additional type of attacker that mimics malicious attacks. It is usually called the second type of attacker A2. It has access to the master key of the KGC, but it is prohibited from launching public key replacement attacks and cannot determine the user's secret value. Mei et al. [12] suggested a certificateless signature scheme that enables conditional privacy protection; however, signature verification efficiency might be improved. Deng et al. [13] proposed a new certificateless signature scheme, but it could not resist replay attacks and did not consider anonymity. To solve these problems, Wang et al. [14] proposed an undocumented signature scheme that supports anonymity and traceability (referred to as Wang et al.'s scheme). Wang et al. [15] have presented a novel blockchain-based smart car carbon emission cap-and-trade system. The proposed system employs a dual-chain architecture, wherein the data chain is utilized to chronicle the data collated from automobiles to guarantee the dependability of the data, thereby ensuring correctness of the carbon emission calculation outcomes. Luo et al. [16] have proposed a carbon quota trading scheme for power generation based on blockchain technology, which integrates lightweight certificateless signature technology and smart contracts to realize an automated carbon quota trading mechanism. However, we find that Wang et al.'s scheme has security defects and cannot resist signature forgery attacks launched by two types of attackers.

Our contributions: To ensure the integrity and identity authentication of electricity carbon quota trading, we propose a scheme of electricity carbon quota trading based on the blockchain and certificateless signatures. The main work is as follows:

(1) We evaluate the security of Wang et al.'s scheme and present two types of forgery attacks.

(2) Aiming at the security defects of Wang et al.'s scheme, we propose an improved certificateless signature scheme.

(3) We suggest an improved signature method and blockchain technology-based trading scheme to make electric carbon quota trading tamper-proof and traceable.

(4) A security study demonstrates that our scheme has low computing and communication costs, provides anonymity and traceability of power enterprise identification, and can withstand forgery and replay attacks.

2 Preparatory Knowledge

Let p and q be two large prime numbers, G_1 and G_2 be two cyclic groups of order q, G be a cyclic group of order p, and $\tilde{P}$ and P be generators of G and G_1, respectively.

2.1 Bilinear Mapping

A bilinear map $e: G_1 \times G_1 \rightarrow G_2$ has the following properties:

(1) Bilinear: For any $a, b \in Z_q^*$, there is $e(aP, bP) = e(P, P)^{ab}$.

(2) Nonregressive: $e(P, P) \neq 1$.

(3) Validity: There is an effective algorithm to calculate $e(aP, bP)$.

(q, G_1, G_2, e, P) satisfying the above conditions is usually called a bilinear group [14].

2.2 Difficult Assumptions

Computational Diffie Hellman (CDH) problem: Given a tuple $(P, aP, bP) \in G_1^3$, where $a, b \in Z_q^*$, calculate abP.

Definition 1 The CDH hypothesis is said to be valid if there is no polynomial-time algorithm that can solve the CDH issue with a nonnegligible probability [8].

Discrete Logarithms (DL) Problem: Given a tuple $\left(\tilde{P}, \tilde{P}^z\right) \in G^2$ and calculate $z \in Z_p^*$.

Definition 2 The DL hypothesis is said to be true if there is no polynomial-time algorithm that can solve the DL problem with a nonnegligible probability [11].

2.3 Security Model

The central objective of our security model is to comprehensively address the security challenges related to carbon emission quotas in the electricity trading market. Specifically, the proposed model strives to prevent various types of malicious attacks, such as data falsification, tampering, forgery, and replay attacks.

To overcome the limitations imposed by traditional cryptography's reliance on fundamental certification requirements and avoid critical custody issues based on identity-based cryptography, a certificate-free signature scheme has been proposed as a feasible solution. The proposed certificate-free signature scheme is highly secure and efficient, aimed at ensuring the validity and non-repudiation

of all transactions involved in carbon emission quota trading. In addition, blockchain technology has been deployed to achieve the immutability and traceability of all power carbon quota transactions. This scheme provides conditional identity privacy protection, enhances defense against replay attacks, and has high computational and communication performance.

In response to the security vulnerabilities of Wang et al.'s scheme, we propose the security model for our scheme and divide the adversaries of the certificate-free signing scheme into two categories: $\mathcal{A}_1$ and A_2.

$\mathcal{A}_1$: These are adversaries who launch forged attacks against malicious users. They can select a target user with a pseudonym PID_1^*, obtain their secret value x_1^* and public key $PK_1^* = \left(X_1^*, R_1^*\right)$, and attempt to obtain a legal signature for any message of the target user through a series of forged attacks, as described in detail in the following text.

A_2: These are adversaries who launch forged attacks against malicious KGCs. As malicious KGCs, they not only know the main secret key of KGC and partial private key d_2^* of users but also can modify system parameters. They can first select a target user for the attack, obtain their pseudonym PID_2^* and public key $PK_2^* = \left(X_2^*, R_2^*\right)$, and then attempt to forge a legal signature for any message of the target user through a series of forged attacks, as described in detail in the following text.

3 Security Analysis of Wang et al.'s Scheme

This section focuses mostly on reviewing the certificateless signature scheme proposed by Wang et al. [14], analyzing its security, and presenting the related enhancement scheme.

3.1 Wang et al.'s Scheme Description

The certificateless signature of Wang et al.'s scheme consists of the six methods listed below:

(1) System establishment: Given a security parameter ζ, the KGC generates system parameters and master keys using the following procedures.

① Select bilinear groups (q, G_1, G_2, e, P) and $Q \in G_1$.

② Select random number $s, k \in Z_q^*$ as the master key and then calculate $P_{pub} = sP$.

③ Select three hash functions $H_1: G_1 \to Z_q^*$, $H_2: \{0,1\}^* \times G_1 \to Z_q^*$, and $H_3: \{0,1\}^* \times \{0,1\}^* \times G_1 \times G_1 \times G_1 \to Z_q^*$.

④ Expose the system parameter $params = \left\{q, G_1, G_2, e, P, P_{pub}, Q, H_1, H_2, H_3\right\}$.

(2) Pseudonym generation: The user whose real identity is ID_i selects a random number $t_i \in Z_q^*$, calculates $T_i = t_i P$, and secretly sends (ID_i, T_i) to the KGC.

After receiving (ID_i, T_i), the KGC verifies the correctness of ID_i, computes $PID_i = ID_i \oplus H_1(kP + T_i)$ using the master key k, and finally sends the user the pseudonym PID_i.

(3) Generation of partial private keys: The KGC generates partial private keys for users with the alias PID_i using the following methods:

① Select a random number $r_i \in Z_q^*$ and then calculate $R_i = r_i P$.

② Calculate $k_i = H_2(PID_i, R_i)$.

③ Calculate partial private key $d_i = r_i + k_i s \bmod q$.

④ Send (d_i, R_i) to the user through the secure channel.

(4) Public/private key generation: After receiving (d_i, R_i) from KGC, the user using pseudonym PID_i chooses a random number $x_i \in Z_q^*$, computes $X_i = x_i P$, and establishes public key $PK_i = (X_i, R_i)$ and private key $SK_i = (x_i, d_i)$.

(5) Signature generation: For message m_i, the user with pseudonym PID_i generates the signature of m_i.

① Randomly select $u_i \in Z_q^*$, and calculate $U_i = u_i P$ and $V_i = u_i Q$.

② Select a timestamp TS_i and calculate $h_i = H_3(m_i \parallel TS_i, PID_i, U_i, V_i, PK_i)$.

③ Calculate $W_i = (d_i + h_i x_i) Q + V_i$.

④ Output a signature $\sigma_i = (U_i, V_i, W_i)$ of $m_i \parallel TS_i$.

(6) Signature verification: The verifier goes through the following motions to ensure that $m_i \parallel TS_i$'s signature on $\sigma_i = (U_i, V_i, W_i)$ is legitimate.

① Check the freshness of TS_i. If TS_i is within the effective time, perform the following operation ②; otherwise, terminate the operation.

② Calculate $k_i = H_2(PID_i, R_i)$ and $h_i = H_3(m_i \parallel TS_i, PID_i, U_i, V_i, PK_i)$.

③ Verify equation $e(W_i, P) = e\left(R_i + k_i P_{pub} + h_i X_i + U_i, Q\right)$.

The verifier accepts the signature if the aforementioned equation is true; otherwise, σ_i is rejected.

The relevant process of the Wang et al.'s scheme is shown in Fig. 2.

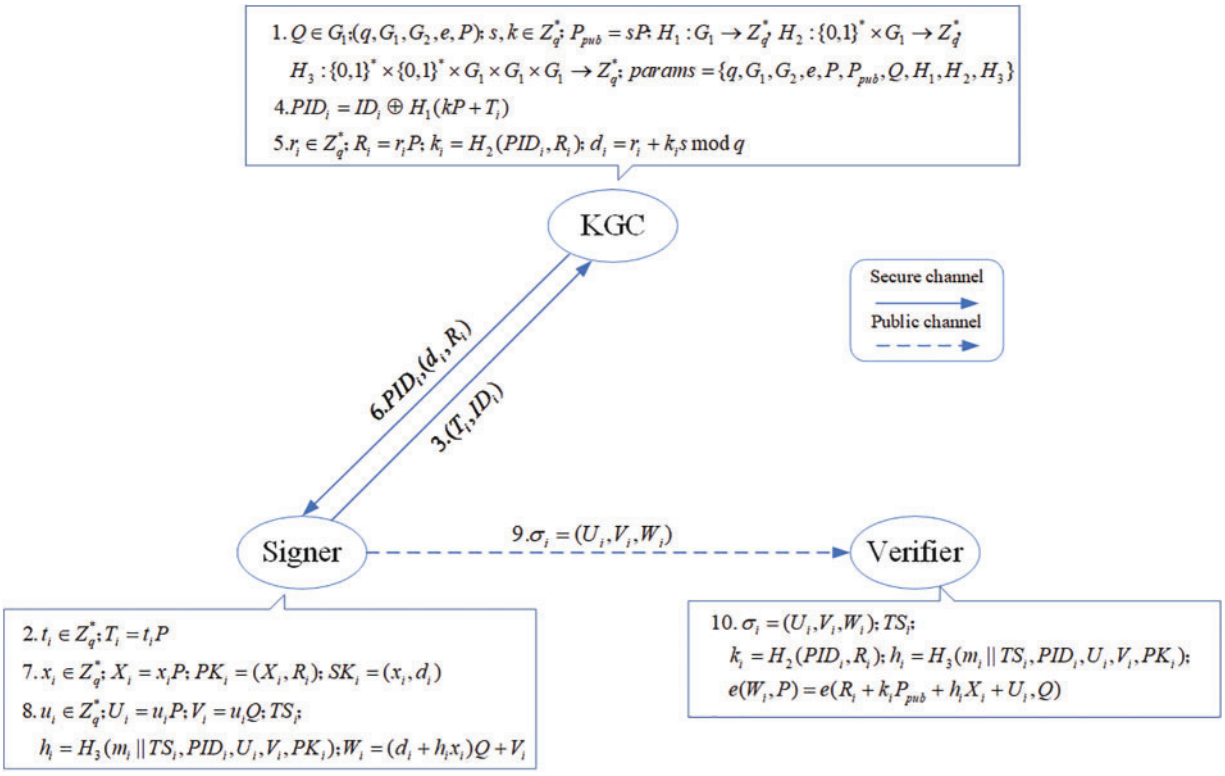

Figure 2: Wang et al.'s scheme

3.2 Forgery Attack of Wang et al.'s Scheme

Here are the specific steps for the two forgery attacks that Wang et al.'s scheme cannot resist.

(1) Forgery attack by malicious users: Let $\mathcal{A}_1$ be the first type of attacker targeting Wang et al.'s scheme. $\mathcal{A}_1$ selects a target user with pseudonym PID_1^* and obtains its secret value x_1^* and public key $PK_1^* = \left(X_1^*, R_1^*\right)$. Through the subsequent attack methods, $\mathcal{A}_1$ can falsify the target user's actual signature on any message.

① Calculate $k_1^* = H_2\left(PID_1^*, R_1^*\right)$.

② Select $z_1^* \in Z_q^*$ at random and compute $U_1^* = z_1^* P - k_1^* P_{pub} - R_1^*$ and $V_1^* = z_1^* Q$.

③ Select message m_1^* and timestamp TS_1^* at random and calculate $h_1^* = H_3(m_1^* \parallel TS_1^*, PID_1^*, U_1^*, V_1^*, PK_1^*)$.

④ Calculate $W_1^* = \left(z_1^* + h_1^* x_1^*\right) Q$.

⑤ Output $m_1^* \parallel TS_1^*$ to forge signature $\sigma_1^* = \left(U_1^*, V_1^*, W_1^*\right)$.

The following verifies the legitimacy of $\mathcal{A}_1$'s forged signature σ_1^*:

$$\begin{aligned} e\left(W_1^*, P\right) &= e\left(\left(z_1^* + h_1^* x_1^*\right) Q, P\right) \\ &= e\left(\left(z_1^* + h_1^* x_1^*\right) P, Q\right) \\ &= e\left(z_1^* P + h_1^*\left(x_1^* P\right), Q\right) \\ &= e\left(\left(U_1^* + k_1^* P_{pub} + R_1^*\right) + h_1^* X_1^*, Q\right) \\ &= e\left(R_1^* + k_1^* P_{pub} + h_1^* X_1^* + U_1^*, Q\right) \end{aligned}$$

The given reasoning demonstrates that σ_1^* satisfies Wang et al.'s signature verification equation. In the above attack, $\mathcal{A}_1$ does not know the master key of the KGC. Therefore, $\mathcal{A}_1$'s assault based on forgery is successful. Wang et al.'s scheme is not secure against the first type of forgery attacker $\mathcal{A}_1$.

(2) Forgery attack of malicious KGC: Let A_2 be the second type of attacker against Wang et al.'s scheme. A_2 selects a target user and obtains its pseudonym PID_2^* and public key $PK_2^* = \left(X_2^*, R_2^*\right)$. Because A_2 is a malicious KGC, it not only knows the KGC's master key and part of the user's private key d_2^* but can also modify system parameters. A_2 can fake the valid signature of the target user for any information via the following attack techniques:

① Select a random number $z_2^* \in Z_q^*$, calculate $Q^* = z_2^* P$, and make parameter $params = \left\{q, G_1, G_2, e, P, P_{pub}, Q^*, H_1, H_2, H_3\right\}$ public.

② Select $u_2^* \in Z_q^*$ at random and calculate $U_2^* = u_2^* P$ and $V_2^* = u_2^* Q^*$.

③ Select message m_2^* and timestamp TS_2^* at random and calculate $h_2^* = H_3(m_2^* \parallel TS_2^*, PID_2^*, U_2^*, V_2^*, PK_2^*)$.

④ Calculate $W_2^* = d_2^* Q^* + h_2^*\left(z_2^* X_2^*\right) + V_2^*$.

⑤ Output $m_2^* \parallel TS_2^*$ to forge signature $\sigma_2^* = \left(U_2^*, V_2^*, W_2^*\right)$.

The following verifies the legitimacy of the signature forged by A_2:

$$\begin{aligned} e\left(W_2^*, P\right) &= e\left(d_2^* Q^* + h_2^*\left(z_2^* X_2^*\right) + V_2^*, P\right) \\ &= e\left(d_2^* Q^* + h_2^* z_2^*\left(x_2^* P\right) + V_2^*, P\right) \\ &= e\left(d_2^* Q^* + h_2^* x_2^*\left(z_2^* P\right) + V_2^*, P\right) \\ &= e\left(d_2^* Q^* + h_2^* x_2^* Q^* + V_2^*, P\right) \\ &= e\left(\left(d_2^* + h_2^* x_2^*\right) Q^* + V_2^*, P\right) \\ &= e\left(R_2^* + k_2^* P_{pub} + h_2^* X_2^* + U_2^*, Q^*\right) \end{aligned}$$

The given reasoning demonstrates that σ_2^* satisfies Wang et al.'s signature verification equation. However, A_2 does not know the target user's secret value x_2^* in the above attack. Therefore, A_2's forgery attack is successful. Wang et al.'s scheme is also unsafe for the second type of forgery attacker A_2.

3.3 Improved Certificateless Signature Scheme

To address the security flaws of Wang et al.'s scheme, we provide an enhanced certificateless signing scheme below. The cyclic group of the elliptic curve is chosen to improve the communication performance of the updated scheme. The specific description is as follows:

(1) System establishment: The KGC performs the following actions to produce system parameters and master keys based on security parameter ζ:

① Select an elliptic curve cyclic group G of prime p and a generator P of G.

② Select a random number $s, k \in Z_p^*$ as the master key and then calculate $P_{pub} = sP$.

③ Select four hash functions: $H_1: G_1 \to Z_q^*$, $H_2: \{0,1\}^* \times G_1 \times G_1 \to Z_q^*$, $H_3: \{0,1\}^* \times \{0,1\}^* \times G_1 \times G_1 \to Z_q^*$, $H_4: Z_q^* \times G_1 \to Z_q^*$.

④ Expose system parameter $params = \left\{q, G_1, G_2, e, P, P_{pub}, H_1, H_2, H_3, H_4\right\}$.

(2) Kana generation: This algorithm is the same as Wang et al.'s scheme.

(3) Partial private key generation: This algorithm is the same as Wang et al.'s scheme, but the only difference is that the value of k_i is $k_i = H_2\left(PID_i, R_i, P_{pub}\right)$.

(4) Public/private key generation: This algorithm is the same as Wang et al.'s scheme.

(5) Signature generation: For message m_i, the user with pseudonym PID_i generates m_i's signature.

① Randomly select $u_i \in Z_p^*$ and then calculate $U_i = u_i P$.

② Select a timestamp TS_i and calculate $h_i = H_3\left(m_i \parallel TS_i, PID_i, U_i, PK_i\right)$, $l_i = H_4\left(h_i, P_{pub}\right)$.

③ Calculate $w_i = u_i + h_i x_i + l_i d_i \bmod p$.

④ Output signature $\sigma_i = (U_i, w_i)$ of $m_i \parallel TS_i$.

(6) Signature verification: The verifier performs the following steps to check the validity of $m_i \parallel TS_i$'s signature $\sigma_i = (U_i, w_i)$.

① Check the freshness of TS_i. If TS_i is within the valid time, perform the following operation ②; otherwise, terminate the operation.

② Calculate $k_i = H_2\left(PID_i, R_i, P_{pub}\right)$,

$h_i = H_3\left(m_i \parallel TS_i, PID_i, U_i, PK_i\right)$,

$l_i = H_4\left(h_i, P_{pub}\right)$.

③ Verify equation $w_iP = U_i + h_iX_i + l_i\left(R_i + k_iP_{pub}\right)$.

If the above formula is true, the verifier accepts the signature; otherwise, it rejects σ_i.

The related process of the Improved certificateless signature scheme is shown in Fig. 3.

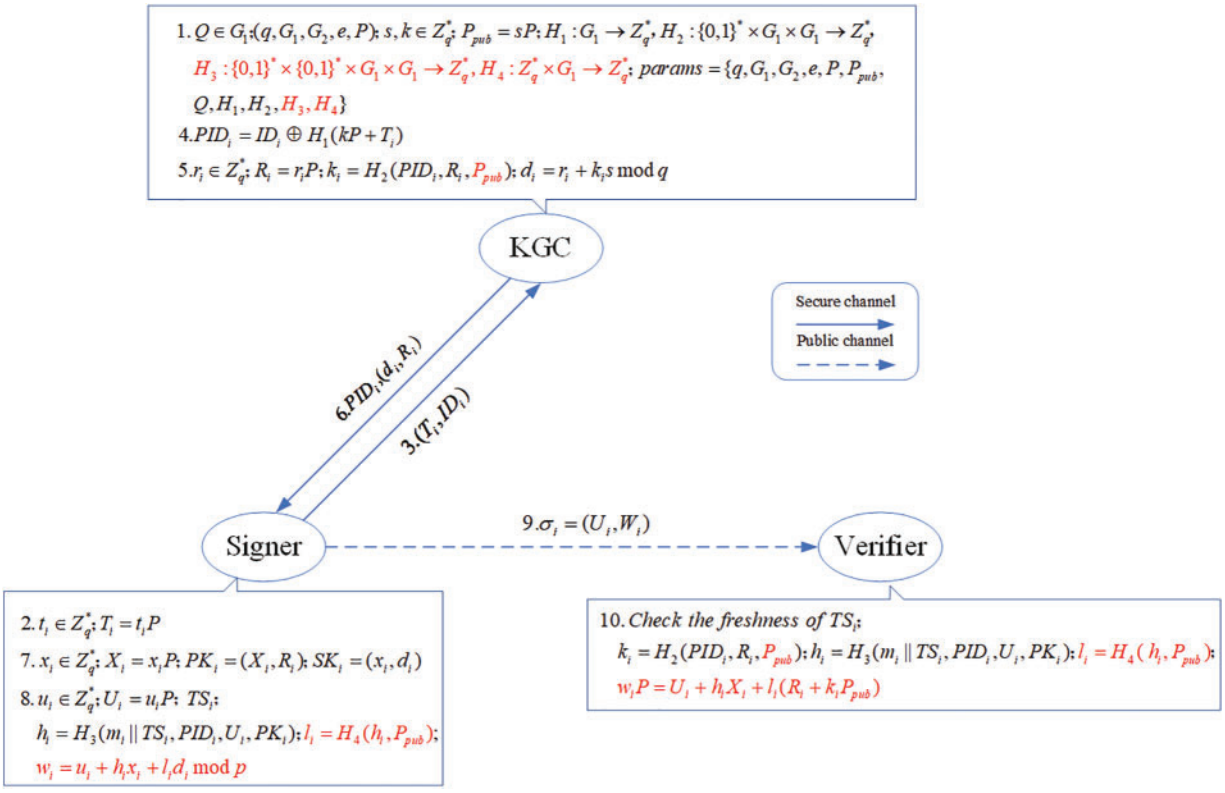

Figure 3: Improved certificateless signature scheme

In the hash value $h_i = H_3(m_i \parallel TS_i, PID_i, U_i, PK_i)$, (U_i, PK_i) is the input value of h_i; in $k_i = H_2\left(PID_i, R_i, P_{pub}\right)$, $\left(R_i, P_{pub}\right)$ is the input value of k_i; and in $l_i = H_4\left(h_i, P_{pub}\right)$, $\left(h_i, P_{pub}\right)$ is the input value of l_i. In addition, w_i binds the hash function to the secret value and partial private key. Based on the unidirectional and anti-collision properties of the hash function, the attacker cannot forge valid signatures by modifying system parameters and replacing public keys. Consequently, the modified scheme is resistant to the two types of forgery attacks outlined in Section 3.2.

4 Electricity Carbon Quota Trading Scheme Based on Certificateless Signature and Blockchain

Based on the improved certificateless signing scheme and blockchain technology presented in Section 3.3, we propose and analyze a secure and effective power carbon quota trading scheme.

4.1 System Model

The carbon quota trading model proposed in this paper is shown in Fig. 4, including six participants: the environmental protection management department (EPMD), quota seller enterprise (QSE), blockchain network (BN), quota buyer enterprise (QBE), audit department (AD), and distributed storage hash table (DSHT).

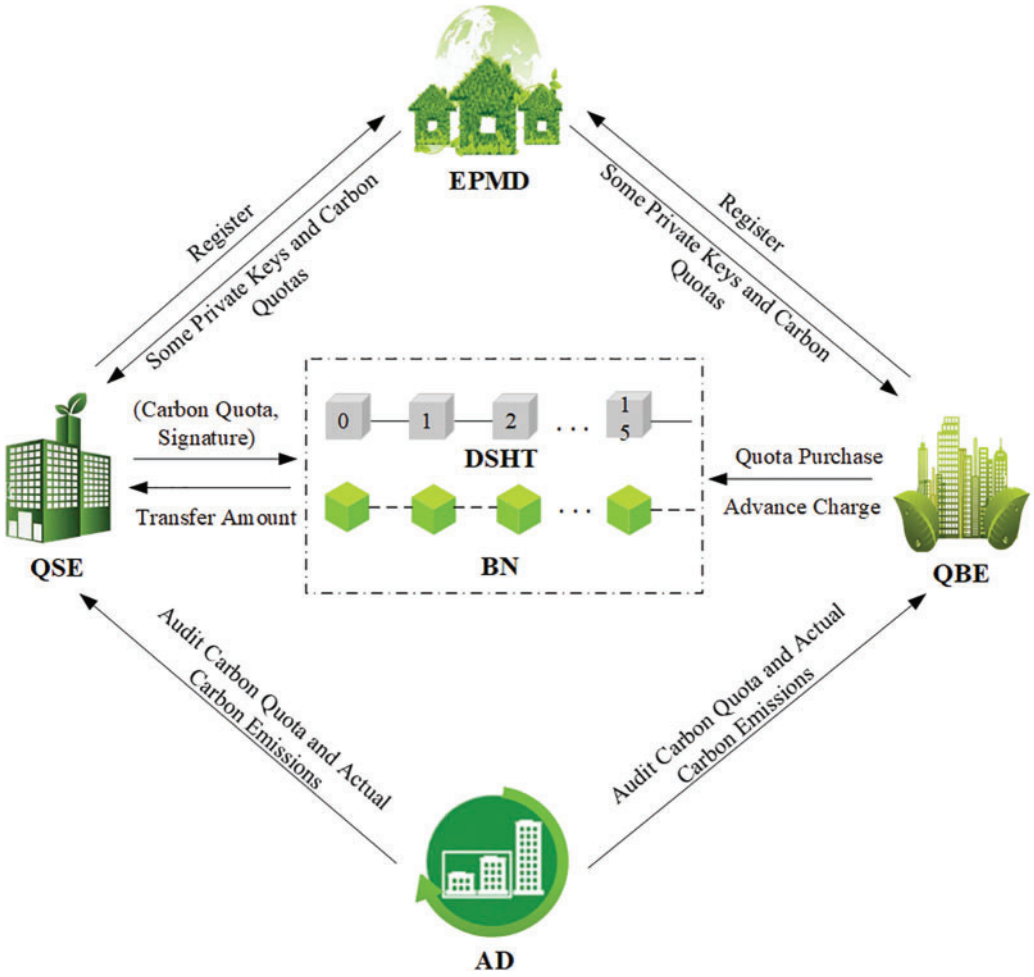

Figure 4: System model

(1) EPMD: Mainly responsible for system initialization, maintenance of the blockchain network, and distribution of some private keys and initial carbon quotas of power enterprises.

(2) QSE: Power enterprises with surplus carbon quotas sign the carbon quota to be sold and then publish it to the blockchain network for trading.

(3) BN: This network is mainly accountable for processing the storage and transaction requests of power carbon quota transactions and validating transaction legitimacy.

(4) QBE: Power enterprises with insufficient carbon quotas purchase carbon quotas through the blockchain network and pay transaction costs to the seller enterprises.

(5) AD: Mainly audits electric power enterprise carbon emission quotas and actual carbon emissions and assists the environmental protection management department in resolving transaction disputes.

(6) DSHT: Mainly stores relevant data on electric power enterprises and carbon quota transactions. Essentially, it is a distributed storage space that divides the data into several small pieces, gives them to different clients for storage, and then uses the storage address to read the data.

4.2 Scheme Description

(1) System initialization: The environmental management department runs the system establishment algorithm of the improved certificateless signature scheme described in Section 3.3 and sets $s, k \in Z_p^*$ as the master secret key and public parameter $params = \{q, G_1, G_2, e, P, P_{pub}, H_1, H_2, H_3, H_4\}$.

(2) Enterprise registration: The power enterprise whose real identity is ID_i selects a random number $t_i \in Z_p^*$, calculates $T_i = t_i P$, and secretly sends (ID_i, T_i) to the environmental protection management department.

After receiving (ID_i, T_i), the environmental protection management department performs the following operations:

① Verify the identity information of ID_i and then calculate the corresponding power enterprise pseudonym $PID_i = ID_i \oplus H_1(kP + T_i)$.

② Save (ID_i, PID_i, T_i) in power enterprise information table L_{ID}.

③ Select a random number $r_i \in Z_q^*$ and then calculate $R_i = r_i P$.

④ Calculate $k_i = H_2(PID_i, R_i, P_{pub})$.

⑤ Calculate the partial private key $d_i = r_i + k_i s \bmod q$.

⑥ Allocate the initial carbon emission quota m_i of power enterprises.

⑦ Send (PID_i, d_i, R_i, m_i) to the enterprise through the secure channel.

⑧ Publish a correctly registered transaction $T_{ID} = \{PID_i, m_i, Addr_{ID_i}\}$ of the power enterprise on the blockchain network, where $Addr_{ID_i}$ is the address of the distributed storage hash table used for storage. Create the enterprise credit pool KC in the common storage area and save (PID_i, c_i, m_i) in KC. c_i represents the enterprise credit degree, and the initial value is 0. If $c_i = 0$, the enterprise credit rating is good; if $c_i = 1$, the enterprise credit rating is poor.

After receiving (PID_i, d_i, R_i, m_i) from the department of environmental protection management, the power enterprise chooses a random number $x_i \in Z_q^*$ and generates the private key $SK_i = (x_i, d_i)$ and the public key $PK_i = (X_i = x_i P, R_i)$.

(3) Quota sale: For the surplus electric power carbon emission quota $m_{i,1}$, the power enterprise with the pseudonym PID_i performs the following sales operations.

① Execute the signature generation process outlined in Section 3.3 of the enhanced certificateless signature scheme and generate the signature $\sigma_i = (U_i, w_i)$ of $m_{i,1} \parallel TS_i$.

② Publish on the blockchain a transaction $T_i = \{PID_i, PK_i, m_{i,1}, Addr_i, \sigma_i\}$ for the sale of energy carbon quotas, where $Addr_i$ is the address where $(PID_i, PK_i, m_{i,1}, TS_i, \sigma_i)$ is stored in the distributed storage hash table.

(4) Quota purchase: When the enterprise with the pseudonym PID_j purchases the electricity carbon quota $m_{i,1}$, the purchase transaction $T_j = \{PID_j, PK_j, Addr_i, \theta_j\}$ is broadcast in the blockchain network, where PID_j and PK_j are the pseudonym and public key of the buyer's enterprise, and θ_j is the prepayment amount. The blockchain node takes $(PID_i, PK_i = (X_i, R_i), m_{i,1}, TS_i, \sigma_i)$ from address $Addr_i$ of the distributed storage hash table and then performs the following operations.

① Check the freshness of TS_i. If $|TS_i - TS_0| > \lambda$, terminate the operation; otherwise, perform step ②, where TS_0 and λ represent the maximum values of the current timestamp and the effective time, respectively.

② Find the cred KC value of the buyer's enterprise and the seller's enterprise in the enterprise credit pool KC. If $c_i = 1$ or $c_j = 1$ indicates that the credit degree of the buying and selling enterprises does not match and the electricity carbon quota transaction is risky, terminate the operation.

③ Perform the signature verification procedure described in Section 3.3 of the improved certificateless signature scheme. If σ_i is a legal signature, perform step ④; otherwise, terminate the operation.

④ If θ_j is less than the market selling price of $m_{i,1}$, terminate the operation; otherwise, transfer to the quota seller according to θ_j to pay the purchase cost of the electricity carbon quota.

⑤ Send $\left(PID_i, PK_i, m_{i,1}, TS_i, \sigma_i\right)$ to the buyer's enterprise.

⑥ In enterprise credit pool KC, modify the actual carbon quota of the seller's enterprise to $m_i - m_{i,1}$ and the actual carbon quota of the buyer's enterprise to $m_j + m_{i,1}$.

⑦ The enterprises of both parties shall go through the relevant carbon quota transfer filing formalities in the environmental protection management department and terminate the carbon quota transaction.

(5) Dispute arbitration: If there is a dispute regarding the electric carbon emission quota $m_{i,1}$ sold by the seller's enterprise, the audit department shall investigate the power enterprise's actual carbon emissions and carbon quota. If there is any violation in the power enterprise, the audit department will set the credit value of the power enterprise to 1 in the enterprise credit pool KC and submit it to the environmental protection management department for corresponding punishment. The specific interaction between QSE, QBE, EPMD and blockchain is shown in Fig. 5.

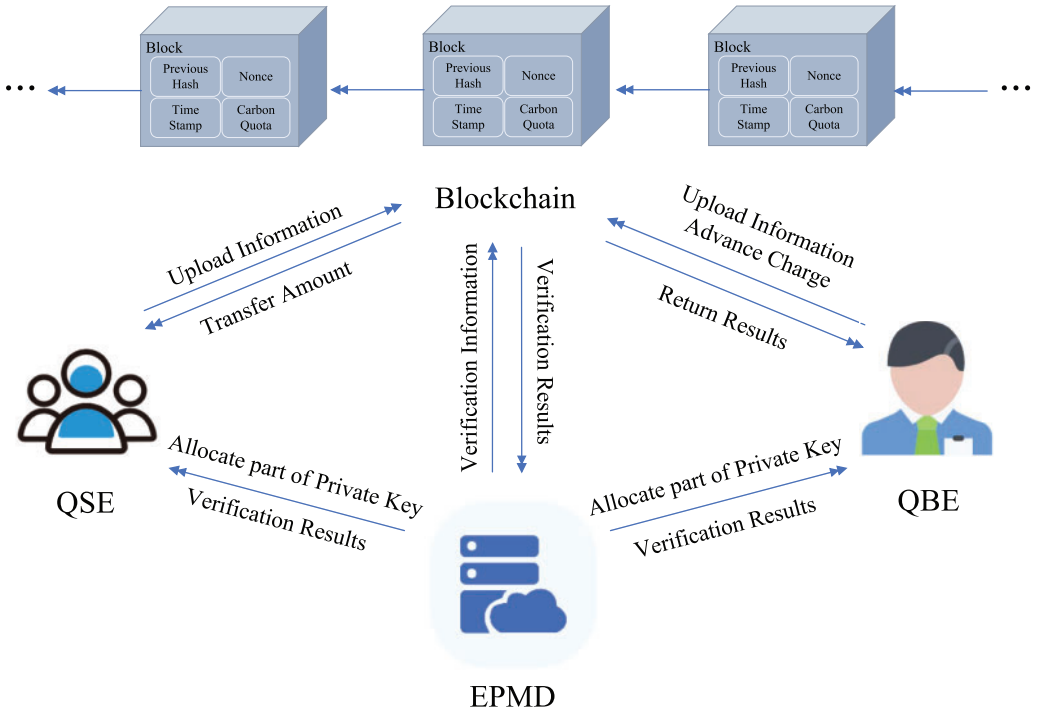

Figure 5: The interactions between blockchain and entities

5 Security and Performance Analysis

5.1 Security Authentication

Based on the methods in [10,14], Theorem 1 and Theorem 2 prove that our proposed scheme can resist signature forgery attacks from malicious users and malicious KGCs.

Theorem 1 If the DL hypothesis is true, our scheme is unfakable for the first type of attacker.

Proof: If the first type of attacker C forges a valid signature of our scheme, then the DL problem can be solved by constructing an Algorithm C as the challenger. Given an instance of a DL problem (P, aP), C aims to calculate $a \in Z_p^*$.

(1) System initialization: C sets $P_{pub} = aP$ and then runs the system establishment algorithm to send the generated parameter *params* to $\mathcal{A}_1$.

(2) Query: C creates 5 blank initialized tables $\{L_1, L_2, L_3, L_4, L_u\}$ in response to $\mathcal{A}_1$'s request. Let PID^* indicate the pseudonym of the target user.

① H_1 query. When $\mathcal{A}_1$ queries $H_1(kP + T_i)$, if $(kP + T_i, h_{ti})$ exists in L_1, C sends h_{it} to $\mathcal{A}_1$; Otherwise, select $h_{it} \in Z_p^*$, store $(kP + T_i, h_{ti})$ in L_1 and return h_{it} to $\mathcal{A}_1$.

② H_2 query. When $\mathcal{A}_1$ queries $H_2\left(PID_i, R_i, P_{pub}\right)$, if $\left(PID_i, R_i, P_{pub}, k_i\right)$ exists in L_2, C sends k_i to $\mathcal{A}_1$; Otherwise, select $k_i \in Z_p^*$, store $\left(PID_i, R_i, P_{pub}, k_i\right)$ in L_2 and return k_i to $\mathcal{A}_1$.

③ H_3 query. When $\mathcal{A}_1$ queries $H_3(m_i \parallel TS_i, PID_i, U_i, PK_i)$, if $(m_i \parallel TS_i, PID_i, U_i, PK_i, h_i)$ exists in L_3, C sends h_i to $\mathcal{A}_1$; Otherwise, select $h_i \in Z_p^*$, return h_i to $\mathcal{A}_1$ and store $(m_i \parallel TS_i, PID_i, U_i, PK_i, h_i)$ in L_3.

④ H_4 query. When $\mathcal{A}_1$ queries $H_4\left(h_i, P_{pub}\right)$, if $\left(h_i, P_{pub}, l_i\right)$ exists in L_4, C sends l_i to $\mathcal{A}_1$; Otherwise, select $l_i \in Z_p^*$, store $\left(h_i, P_{pub}, l_i\right)$ in L_4 and return l_i to $\mathcal{A}_1$.

⑤ Public key query: When $\mathcal{A}_1$ queries PID_i's public key, if $(PID_i, d_i, R_i, x_i, X_i)$ exists in L_u, C sends (X_i, R_i) to $\mathcal{A}_1$; Otherwise, C performs the following operations:

• If $PID_i \neq PID^*$, C randomly select $x_i, d_i, k_i \in Z_p^*$, calculate $X_i = x_iP$ and $R_i = d_iP - k_iP_{pub}$, and there are $(PID_i, d_i, R_i, x_i, X_i)$ and $\left(PID_i, R_i, P_{pub}, k_i\right)$ respectively in L_u and L_2, send (X_i, R_i) to $\mathcal{A}_1$.

• If $PID_i = PID^*$, C randomly select $x^*, r^* \in Z_p^*$, calculate $X^* = x^*P$ and $R^* = r^*P$. If $(PID^*, \perp, R^*, x^*, X^*)$ exists in L_u, send (X^*, R^*) to $\mathcal{A}_1$.

⑥ Secret value query: When $\mathcal{A}_1$ queries the secret value of PID_i, C looks up $(PID_i, d_i, R_i, x_i, X_i)$ in L_u and returns x_i to $\mathcal{A}_1$.

⑦ Partial private key query: When $\mathcal{A}_1$ queries PID_i's partial private key, C looks up $(PID_i, d_i, R_i, x_i, X_i)$ in L_u and returns d_i to $\mathcal{A}_1$.

⑧ Public key replacement query: When $\mathcal{A}_1$ submits $\left(PID_i, X_i', R_i'\right)$, C replaces PID_i's public key in L_u and sets $X_i = X_i'$ and $R_i = R_i'$.

⑨ Signature query: When $\mathcal{A}_1$ queries $(m_i \parallel TS_i, PID_i)$'s signature, C randomly selects $w_i, h_i, l_i \in Z_p^*$, looks up k_i in L_2, calculates $U_i = w_iP - h_iX_i - l_i\left(R_i + k_iP_{pub}\right)$ and returns (U_i, w_i) to $\mathcal{A}_1$.

(3) Forgery: After a finite number of the above queries, $\mathcal{A}_1$ outputs the signature $\sigma^* = (U^*, w^*)$ of $m^* \parallel TS^*$ under PID^* and public key (X^*, R^*). According to forking lemma [17], C obtains another valid signature $\tilde{\sigma} = \left(U^*, \tilde{w}\right)$ by using different output values $\tilde{k}$ of the same random values U^* and H_2. Because $w^*P = U^* + h^*X^* + l^*(R^* + k^*(aP))$, $\tilde{w}P = U^* + h^*X^* + l^*\left(R^* + \tilde{k}(aP)\right)$.

Therefore, $w^*P - \tilde{w}P = l^*k^*aP - l^*\tilde{k}aP$, so we can calculate $a = \left(w^* - \tilde{w}\right)\left(k^* - \tilde{k}\right)^{-1}(l^*)^{-1} \bmod p$.

Nevertheless, the DL problem is difficult to solve in polynomial time, indicating that $\mathcal{A}_1$'s proposed attack is not feasible. Therefore, our scheme can resist signature forging attacks from malicious users.

Theorem 2 If the LD hypothesis is valid, our scheme is unforgeable for the second type of attacker.

The proving procedure for Theorem 2 is comparable to that of Theorem 1. Because the second sort of attacker has access to the KGC's master key, partial private key queries and public key replacement queries are no longer conducted.

5.2 Security Analysis

(1) Anonymity: The real identity ID_i of the power enterprise and the master key k of the environmental protection management department generate the pseudonym $PID_i = ID_i \oplus H_1(kP + T_i)$ of the power enterprise. If the attacker cannot know k and T_i, he cannot calculate ID_i from PID_i. The master key k is kept secret by the environmental protection management department, but deriving t_i from $T_i = t_iP$ is equivalent to solving the DL problem. Therefore, our scheme satisfies the anonymity of power enterprise identity.

(2) Traceability: When there is a dispute in an enterprise-issued energy carbon quota transaction, the environmental protection management department looks up (ID_i, PID_i, T_i) in the information table L_{ID} of the power enterprise through PID_i in the transaction and calculates $ID_i' = PID_i \oplus H_1(kP + T_i)$. If $ID_i' = ID_i$, the environmental protection management department can determine the real identity ID_i of the power enterprise participating in the transaction. Therefore, our scheme satisfies the traceability of power enterprise identity.

(3) Integrity, authenticity, and nonrepudiation: The power carbon quota transaction issued by the enterprise of the seller must be appended with signature $\sigma_i = (U_i, w_i)$, and the transaction information T_i must be maintained in the blockchain. Theorems 1 and 2 demonstrate that adversaries cannot fabricate valid signatures of our scheme, and blockchain ensures the traceability and tamper-proofness of transaction data. Consequently, our scheme satisfies the integrity, authenticity, and nonrepudiation requirements of electrical carbon quota trading and is capable of withstanding attacks such as forgery, impersonation, and tampering.

(4) Resist replay attack: When the buyer's enterprise purchases the electricity carbon quota, it checks the freshness of the transaction through timestamp TS_i. Since TS_i is the input value of hash values h_i and l_i, if the attacker attempts to modify TS_i, the signature cannot be verified. Therefore, our scheme can resist replay attacks.

5.3 Performance Analysis

Tables 1 and 2 exhibit the performance and function comparisons between our scheme and published schemes [10,11,14]. Reference [18] evaluated the operation time of cryptographic operations, where $T_M = 1.9456$ ms, $T_H = 2.3366$ ms, and $T_P = 15.0738$ ms. To achieve the same level of security in schemes based on the bilinear group and elliptic curve group, 512-bit prime numbers q and 160-bit prime numbers p are selected, respectively. Table 1 only considers the operations with high computational overhead. T_M, T_H, and T_P are used to represent a dot product operation, hash operation mapped to point and bilinear pair operation, respectively; $|p|$, $|G|$ and $|G_1|$ represent the length of an element in Z_p, G, and G_1, respectively. Our scheme is based on a cyclic group of an elliptic curve. and the signature verification phase does not involve time-consuming bilinear pair operations.

Table 1: Computational performance and signature length comparison

Scheme	Anonymity	Forgery resistance	Replay resistance	Traceability
Scheme [10]	×	×	×	×
Scheme [11]	×	×	×	×
Scheme [14]	√	×	√	√
Our scheme	√	√	√	√

Note: Description: √ and × indicate whether the function is satisfied or not.

Table 2: Feature comparison

Scheme	Signature generation	Verification (ms)	Signature length (bytes)
Scheme [10]	$4T_M = 7.7824$	$3T_M + T_H + 3T_P = 53.3948$	$2\|G_1\| = 256$
Scheme [11]	$3T_M + T_H = 8.1734$	$2T_M + 2T_H + 3T_P = 53.7858$	$2\|G_1\| = 256$
Scheme [14]	$3T_M = 5.8368$	$2T_M + 3T_P = 49.1126$	$3\|G_1\| = 388$
Our scheme	$T_M = 1.9456$	$4T_M = 7.7842$	$\|G\| + \|p\| = 192$

As seen in Tables 1 and 2, Figs. 6, and 7, compared with other schemes [10,11,14], our scheme has the minimum time cost in generating and verifying signatures and the shortest signature length. Our scheme introduces the use of blockchain technology to eliminate intermediaries and improve the efficiency, transparency, and traceability of carbon quota trading in the electricity industry.

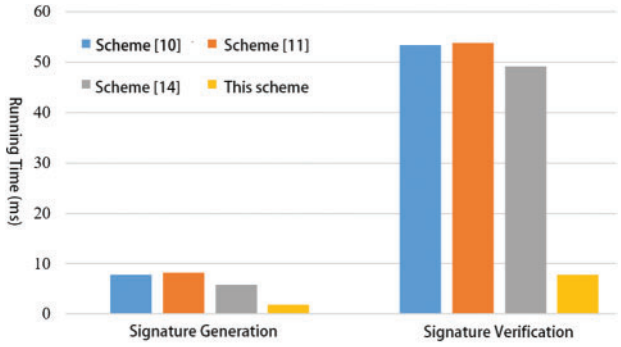

Figure 6: Comparison of computational overhead

The experimental environment for building the blockchain is Intel(R) Xeon(R) Gold 6133 2.50 GHz with Ubuntu Server 22.04 LTS 64-bit operating system, and the underlying platform for the blockchain is Hyperledger Fabric. The experiment simulated the generation of 1,000 to 5,000 user data entries, and tested the time it takes to upload the user data to the blockchain and the time it takes to retrieve the data from the blockchain. The specific test results are shown in Figs. 8 and 9.

The test results show that as the amount of user data increases, the upload time slightly increases and the efficiency decreases slightly, but this decrease is within an acceptable range compared to the significant increase in data volume. When retrieving user data, the blockchain needs to run a consensus

algorithm to disclose data to the nodes, and the degree of impact on time varies depending on the consensus algorithm used, so the retrieval time is slightly lower than the upload time.

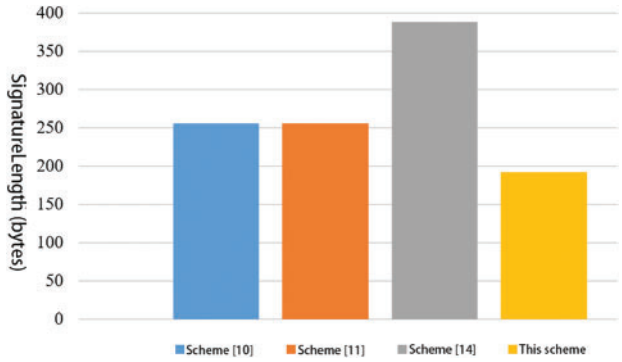

Figure 7: Comparison of signature length

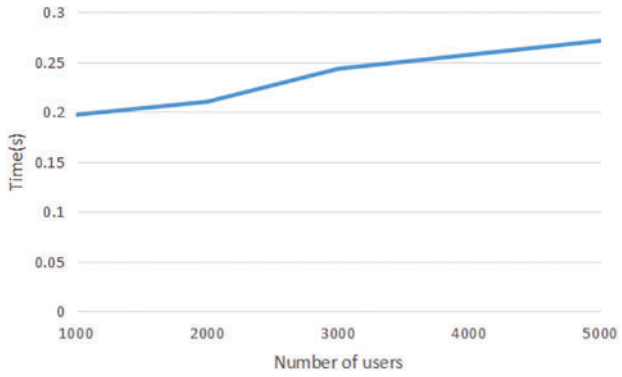

Figure 8: User data upload time

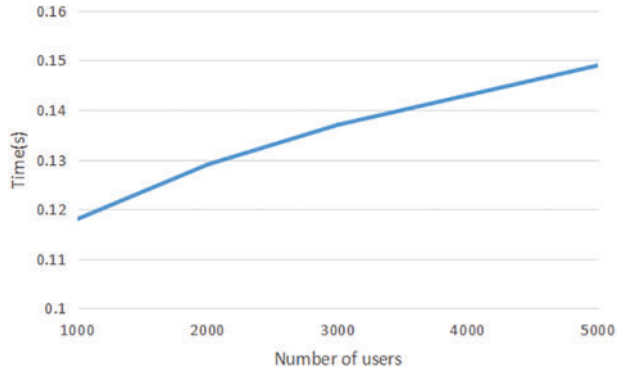

Figure 9: User data return time

6 Conclusions

We propose an efficient electricity carbon emission quota trading scheme based on an improved certificateless signature scheme and blockchain technology. Ensure the integrity and security of the

transaction by signing without the certificate, and using the blockchain to store the transaction data to improve the anti-tampering and traceability of the power carbon quota transaction.

Our scheme provides conditional privacy protection, not only to protect the identity privacy of power enterprises but also to track the real identity of power enterprises that issue disputed transactions. However, our scheme does not consider the confidentiality of transaction data. Therefore, we plan to design a power carbon quota trading scheme based on blockchain and encryption technology in the future.

Acknowledgement: The authors wish to express their appreciation to the reviewers for their helpful suggestions which greatly improved the presentation of this paper.

Funding Statement: This research was supported by the National Fund Project No. 62172337, National Natural Science Foundation of China (No. 61662069) and China Postdoctoral Science Foundation (No. 2017M610817).

Author Contributions: The authors confirm contribution to the paper as follows: study conception and design: Xiaodong Yang, Runze Diao; data collection: Tao Liu, Haoqi Wen; analysis and interpretation of results: Tao Liu, Haoqi Wen. Haoqi Wen; draft manuscript preparation: Xiaodong Yang, Runze Diao. All authors reviewed the results and approved the final version of the manuscript.

Availability of Data and Materials: The data used to support the study's findings are included in the paper.

Conflicts of Interest: The authors declare that they have no conflicts of interest to report regarding the present study.

References

1. Lin, B., Zhou, Y. (2021). Does the internet development affect energy and carbon emission performance. *Sustainable Production and Consumption, 28(6),* 1–10.
2. Wang, R., Cheng, S., Zuo, X., Liu, Y. (2022). Optimal management of multi-stakeholder integrated energy system considering dual incentive demand response and carbon trading mechanism. *International Journal of Energy Research, 46(5),* 6246–6263.
3. Zhang, L., Li, S., Nie, Q., Hu, Y. (2022). A two-stage benefit optimization and multi-participant benefit-sharing strategy for hybrid renewable energy systems in rural areas under carbon trading. *Renewable Energy, 189,* 744–761.
4. Wang, X. Q., Su, C. W., Lobont, O. R., Li, H., Nicoleta-Claudia, M. (2022). Is China's carbon trading market efficient? Evidence from emissions trading scheme pilots. *Energy, 245,* 123240.
5. Zhang, Y., Wu, Q., Hu, W. (2023). Carbon quota trading model based on quantum blockchain. *Journal of Systems & Management, 32(2),* 300–307.
6. Zhu, X., Fu, Q., Wen, H., Zhong, Y., Su, Z. et al. (2020). Optimal allocation model of multi-energy entity energy storage from the perspective of blockchain. *Electric Power Automation Equipment, 40(8),* 47–56.
7. Ji, B., Liu, Y., Zhu, L. (2020). Design of carbon emission permit trading mechanism in power industry based on consortium blockchain. *Huadian Technology, 42(8),* 32–40.
8. Yuan, L., Li, D. (2020). Carbon emission mechanism design based on blockchain technology. *Cyberspace Security, 11(2),* 111– 117.
9. Liu, Y., Wang, D., Wang, Z., Duan, R. (2020). Efficient revocable certificateless signature scheme for cloud computing. *Computer Engineering and Design, 41(9),* 2442–2446.

10. Wang, D., Teng, J. (2018). Probably secure certificate less aggregate signature algorithm for vehicular ad hoc. *Network Journal of Electronics & Information Technology, 40(1),* 11–17.
11. Xu, Z., He, D., Kumar, N., Choo, K. R. (2020). Efficient certificateless aggregate signature scheme for performing secure routing in VANETs. *Security and Communication Networks, 2020(2),* 1–12.
12. Mei, Q., Xiong, H., Chen, J., Yang, M., Kumari, S. et al. (2020). Efficient certificateless aggregate signature with conditional privacy preservation in IoV. *IEEE Systems Journal, 15(1),* 245–256.
13. Deng, L., Ning, B., Jiang, Y. (2020). A lightweight certificateless aggregation signature scheme with provable security in the standard model. *IEEE Systems Journal, 14(3),* 4242– 4251.
14. Wang, H., Wang, L., Zhang, K., Li, J., Luo, Y. (2022). A conditional privacy-preserving certificateless aggregate signature scheme in the standard model for VANETs. *IEEE Access, 10,* 15605–15618.
15. Wang, Y., Li, L., Zhang, Y., Zhao, B. (2022). STRICTs: A blockchain-enabled smart emission cap restrictive and carbon permit trading system. *Applied Energy, 306,* 117848. https://doi.org/10.1016/j.apenergy.2022.117848
16. Luo, J., Han, M., Wang, J. (2020). A blockchain-based electricity carbon quota trading scheme with lightweight certificateless signature. *IEEE Access, 8,* 222830–222840.
17. Bagherzandi, A., Cheon, J. H., Jarecki, S. (2008). Multi signatures secure under the discrete logarithm assumption and a generalized forking lemma. *Proceedings of the 15th ACM Conference on Computer and Communications Security (CCS'08)*, pp. 449–458. New York, NY, USA, Association for Computing Machinery.
18. Cui, J., Wu, D., Zhang, J., Xu, Y., Zhong, H. (2019). An efficient authentication scheme based on semi-trusted authority in VANETs. *IEEE Transactions on Vehicular Technology, 68(3),* 2972–2986.