


Article

A Non-Transferable Trade Scheme of Green Power Based on Blockchain

Yang Li ^{1,2}, Mengying Jiang ¹, Mei Yu ^{1,*} , Shouzhi Xu ¹, Xiaojun Liu ^{1,2}, Shirui Zhang ¹, Jia Zhu ², Shurui Peng ² and Zhongming Gu ²

¹ Hubei Key Laboratory of Intelligent Vision Based Monitoring for Hydroelectric Engineering, China Three Gorges University, Yichang 443002, China; liuxiaojun87@sina.com (X.L.)

² Yichang Power Supply Company of State Grid Hubei Electric Power Co., Ltd., Yichang 443000, China

* Correspondence: yumei@ctgu.edu.cn

Abstract: Power consumers can obtain authoritative green environmental value certification through green electricity trading, which plays an important role in improving the production competitiveness of enterprises, especially for international product trade affairs. However, the credibility of green electricity transactions faces serious challenges in the enterprise green authentication affairs, especially the user's identity authentication, the traceability of green electricity transactions, and the standardization of green electricity transactions. Aiming to solve the certification and traceability problem of tradable green certificates, this paper proposes an integrated green certificate trading protocol, which solves its double-trading problem and helps to improve the credibility of renewable energy use. The main contribution is providing a solution based on the consortium blockchain technology to solve the main challenges mentioned above. The main solved scheme designs a series of protocols, which includes a purchase protocol, payment protocol, and non-transferable protocol. The whole process ensures the credibility, traceability, and non-transferability of green certificate trading. Multiple verification measures are adopted to address security and privacy challenges in green certificate management. Through security analysis, the protocol effectively defends against attacks such as double payments, transaction rollback, and transaction replays while ensuring users' privacy.

Keywords: blockchain; non-transferability; green certificate; traceability



Citation: Li, Y.; Jiang, M.; Yu, M.; Xu, S.; Liu, X.; Zhang, S.; Zhu, J.; Peng, S.; Gu, Z. A Non-Transferable Trade Scheme of Green Power Based on Blockchain. *Energies* **2024**, *17*, 4002. <https://doi.org/10.3390/en17164002>

Academic Editor: Michael Negnevitsky

Received: 13 June 2024

Revised: 9 August 2024

Accepted: 11 August 2024

Published: 13 August 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Regarding Tradable Green Certificates (TGCs), each certificate represents a specific amount of renewable energy production and ensures a single, efficient use. These certificates are a key tool for recognizing the production and consumption of renewable electricity. They are closely linked to the carbon accounting system, providing strong support for product carbon footprint management. Through this mechanism, green certificates not only promote transparency and traceability of renewable energy but also strengthen the drive for further development of green energy [1,2].

Existing green policies talk about Fixed Feed-in Tariffs (FiTs), Renewable Portfolio Standards (RPSs), and Emission trading systems (ETSs) in [2] in addition to Tradable Green Certificates (TGCs). FiTs serve as a compensation mechanism to incentivize renewable energy production by guaranteeing that renewable generators will be able to sell electricity at a pre-determined price, and do not, per se, involve specific tracking of the sources and flows of electricity [3]. TGCs can complement FiTs by providing a traceable identifier for each unit of electricity, enhancing market transparency. The RPS mandates that utilities purchase a certain percentage of renewable electricity. Green certificates, as one of the means to fulfill RPS requirements, provide utilities with the flexibility to either purchase green power directly or trade certificates [4]. This mechanism requires a rigorous authentication and traceability system to ensure the one-time use and authenticity of the certificates. The ETS controls overall pollutant emissions by capping emissions and allowing the buying and selling of emission credits, and

companies that successfully reduce their emissions can sell their remaining allowances to companies that need additional allowances. Green certificate trading provides an effective way for companies to demonstrate the effectiveness of their renewable energy emissions reductions [5,6]. By purchasing green certificates, companies can not only demonstrate their support for renewable energy but also optimize their carbon footprint, thereby complying with the requirements of the ETS and contributing to environmental responsibility.

Traditional centralized green certificate systems face the risk of data tampering and fraud, leading to problems such as duplicate transactions, which undermine the credibility of renewable energy and sustainable development. Current research is adopting blockchain technology and combining it with smart grid technology to more effectively address fraudulent double trading of green certificates. Therefore, to better address the aforementioned issues, it is necessary to design a blockchain protocol that integrates blockchain technology with green certificate trading mechanisms, effectively tackling the fraud problems faced in green certificate transactions.

Blockchain protocols are a set of rules that define how data are created, transmitted, and recorded in a decentralized network. A key agreement protocol based on a balanced incomplete block design was proposed in [7], which utilizes the mathematical structure of the block design to distribute the key, which makes the distribution of the key highly symmetric and solves the problem of secure data sharing among multiple participants. A privacy-preserving hybrid scheme was proposed in [8], which introduces a decentralized signature and negotiation process to ensure that no one else has direct access to the real transaction details before the hybrid, reducing single points of failure and trust issues. A new ring-type confidential transaction protocol was designed in [9] to introduce an extended version of multi-choice proof and special multi-signature to realize the privacy protection of user identity and transaction amount in the transaction. In [10], to improve the efficiency of transaction verification and dissemination in blockchain systems, a reputation-based transaction processing mechanism was constructed to evaluate the reputation of the transaction source and prevent suspicious transactions from untrusted nodes. Smart contract automated implementation of the protocol, combined with zero-knowledge proofs and ring-signature techniques, for anonymous transaction tracking and tracking the flow of money without destroying privacy, provide partial ideas for the protocol in this paper [11–13].

Applying blockchain technology to the issuance and management of green certificates can improve the efficiency and responsiveness of transactions. In smart grids, edge computing is often used to move data processing from the centralized system to the edge of the network to ensure fast and efficient transactions [14]. The Stackelberg game theory, which optimizes resource allocation by constructing a leader–follower model, can be used to improve transaction reliability [15]. The application of blockchain in microgrids can prevent data from being tampered with and illegally accessed through an effective authentication mechanism and a tamper-proof distributed ledger [16,17]. By automating and decentralizing the transaction mechanism and accounting for default risk and demand uncertainty, blockchain provides a transparent monitoring mechanism that reduces the likelihood of default [18,19]. Blockchain provides a reliable record of renewable energy ownership and transactions through its decentralized and tamper-proof ledger, ensuring that each transaction is unique and verifiable [20]. IoT devices that automatically collect energy usage data and process and record them through blockchain technology can ensure the accuracy and timeliness of the data while preventing them from being tampered with [21,22]. The protocol in this paper is based on the characteristics of blockchain to ensure that each green certificate transaction is recorded and confirmed, avoiding duplicate sales or misuse of the same energy yield.

In addition, future research should consider adding deep learning techniques to optimize the algorithms in the green certificate trading system. For example, when dealing with complex transactions and decisions, the application of the Markov decision process can ensure efficient transaction execution [23,24]. Bidirectional long- and short-term memory networks can be used to monitor and analyze transaction behavior and identify fraudulent

behavior, thereby enhancing transaction security [25]. In the automatic verification of smart contract terms or transaction statements, multi-task learning models can be used to verify the authenticity of transaction records, identify possible false information, and improve the fraud resistance of the system [26,27]. Deep learning models have been widely used in complex pattern recognition and anomaly detection [28], and dynamic optimization strategies based on deep reinforcement learning have shown significant potential in real-time decision making and adaptation of complex systems [29]. These approaches can enhance the intelligence of trading systems and improve their ability to cope with anomalous behavior.

In summary, green certificates are crucial for promoting sustainable energy utilization, and blockchain technology has the potential to safeguard data tampering and enhance transparency. Therefore, this paper proposes a new blockchain-based green certificate transaction scheme to secure certificate transactions throughout the transaction life cycle.

2. Blockchain-Based Green Certificate Scheme

2.1. Main Goals of the Scheme

The main goals of the green certificate scheme include three functions:

(1) Prevent secondary trading

When certificates are traded multiple times, the green attributes of the same amount of electricity are claimed by multiple users, leading to double counting of the green energy contribution, thereby inflating the actual contribution of renewable energy and undermining the credibility and goals of the green certificate system. To ensure that this amount of electricity is only recognized once, the issue of secondary trading of green certificates needs to be addressed.

(2) Solve the credibility problem

The credibility of green certificates is closely related to the acceptance and effectiveness of green energy projects, and improving the credibility of certificates can have a long-term sustainable impact on the green energy market.

(3) Solve the traceability problem

If market participants are unable to verify the authenticity of certificates or their origin, they may lose confidence in the certification system as a whole, and this confidence may lead to a decrease in participation in the green certificate market; at the same time, the lack of an effective traceability mechanism may lead to an increased likelihood of counterfeiting and reuse of certificates. Unscrupulous actors may exploit loopholes in the system to sell green attributes that do not exist or sell the same attribute multiple times. Improving the traceability of green certificate transactions can ensure the integrity and verifiability of certificates.

To address the above issues, this paper proposes a blockchain-based green certificate transaction scheme that protects the security and uniqueness of the transaction throughout the process and improves the credibility and traceability of the green certificate.

2.2. Technical Principles

(1) Consortium blockchain

The consortium blockchain is a blockchain technology that lies between public and private chains. Unlike public chains, where anyone can join, a consortium chain is controlled by a few pre-selected nodes (usually representatives of different organizations). These nodes work together to maintain the blockchain's ledger and authorize new members or nodes to join the network. Compared to private chains, which are controlled by a single entity, federated chains provide a broader base of transparency and trust because they are jointly managed by multiple trusted entities.

This technology allows multiple pre-selected entities to work together to manage and maintain a blockchain network and is suitable for environments that require high levels of trust and data security. Coalition chains ensure the reliability of the network and the verifiability of

transactions through the participation of trusted organizations, increasing overall credibility. Transactions are immutable once confirmed and recorded on the blockchain, effectively preventing any form of secondary transactions. Each transaction is recorded in detail from initiation to completion, ensuring a high level of transparency and traceability.

(2) Blockchain protocol

Blockchain technology operates as a decentralized, distributed ledger or database governed by specific protocol rules, while the blockchain protocol itself is a collection of rules and algorithms that can be considered the operating system of blockchain technology. This protocol specifies detailed rules for how nodes validate data, how transactions are confirmed, and how data are added to the blockchain. It ensures that all participants in the network adhere to the same standards, thereby facilitating the decentralization and security of the network.

To ensure the security and uniqueness of transactions, the blockchain protocol uses various mechanisms and technologies, such as cryptographic techniques. Hash functions are used to generate a unique hash value for each block, with SHA-256 being a commonly used hash algorithm. Public and private key encryption is used to verify transaction identities and protect data from unauthorized access. Transaction initiators sign their transactions using a private key, while the corresponding public key is made available to anyone to verify the validity of the signature. Each block contains multiple transactions that are encrypted using hash algorithms (including the hash of the previous block) to create a unique hash value. This hash must meet certain conditions before the block is accepted into the chain. Digital signatures are a core part of the blockchain's security architecture, not only protecting transactions from tampering but also ensuring their traceability and transparency. In applications such as financial transactions, contract execution, and legal document storage, digital signatures provide a powerful tool to ensure the legality and security of operations. In this way, blockchain maintains a secure, reliable, and decentralized data management system.

2.3. System Architecture of Green Certificate Trading Management

The proposed scheme in this study is divided into three key components: the purchase agreement, payment agreement, and non-transferable agreement, and the system architecture is shown in Figure 1.

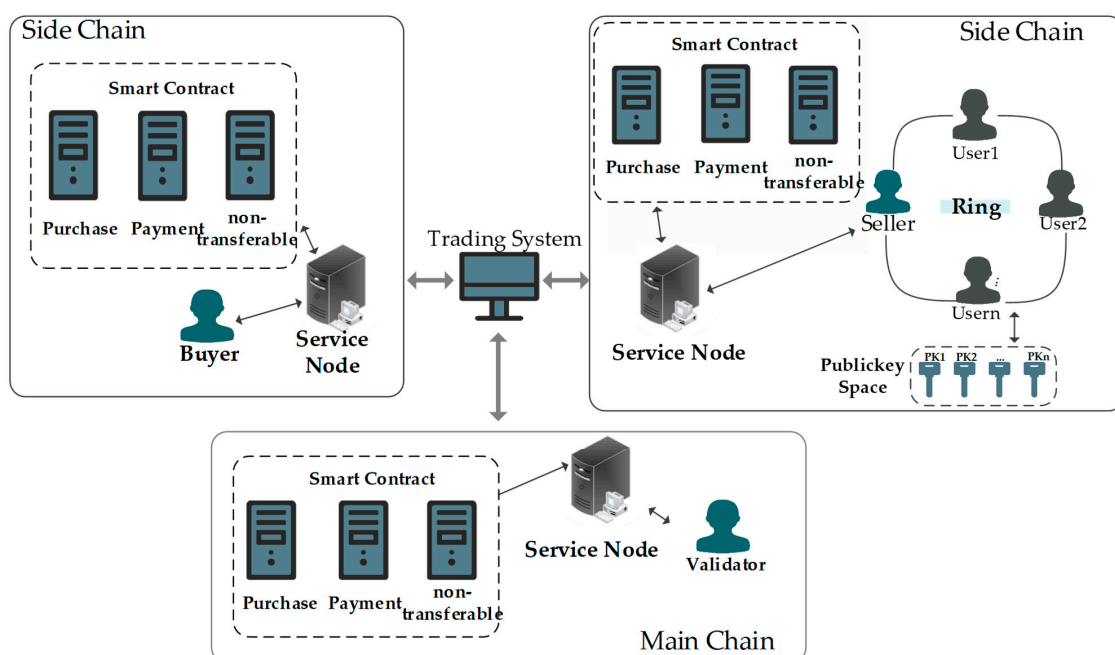


Figure 1. System architecture diagram.

This green certificate trading solution leverages a blockchain-based framework to automate transactions using smart contracts, enhancing the security, transparency, and non-transferability of the process. Smart contracts automate the execution of purchase, payment, and non-transferable agreements on the blockchain, minimizing human intervention and reducing the risks of errors and fraud. These contracts facilitate the automatic processing of payments and certificate transfers once transaction conditions are met, thus streamlining the transaction process and ensuring consistency. Moreover, the solution employs ring-signature technology at the sell-side node to improve anonymity and security, safeguarding user privacy and validating transaction legitimacy. A bespoke non-transferable agreement ensures each green certificate is traded only once, preventing secondary trading and preserving market integrity and credibility. Verifiers utilize smart contracts for tracking and verifying the transaction history and status of certificates on the blockchain, which strengthens regulatory capabilities and promotes market fairness.

Overall, this scheme enhances the efficiency and reliability of green certificate transactions through innovative technology, supports renewable energy utilization, and fosters sustainable environmental development.

3. Main Protocols of the Green Certificate Systems

3.1. Purchase Protocol

The purchase protocol goes through four key stages in turn: certificate on-chain, ring signature verification, certificate on-chain verification, and cryptographic purchase request submission, as shown in Figure 2.

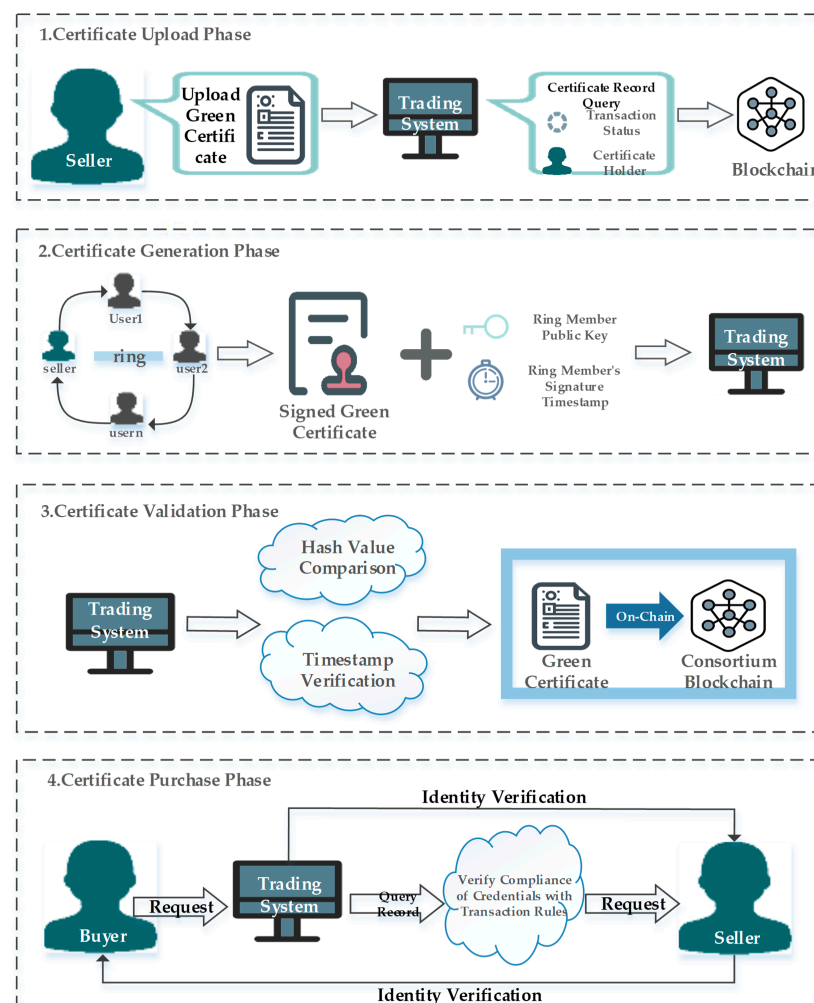


Figure 2. Flow chart of purchase protocol.

(1) Certificate on-chain: The upload process of green certificates is led by the sale, which uploads the certificate data to a blockchain-powered trading platform. After uploading, the system automatically queries the immutable transaction records of the blockchain by executing the smart contract to verify the current transaction status and ownership information of the certificate. This process takes advantage of the decentralization and immutability of blockchain to ensure the authenticity and transparency of certificate data. Through this mechanism, the trading platform can monitor the certificate status in real time, thereby enhancing the security and credibility of the transaction.

Parameter configuration of the initialization protocol, including the construction algorithm of public and private key spaces, the configuration of the secure hash function, and the initialization of the digital credential management mechanism ensure the encryption integrity of the system and the robustness of the authentication mechanism, as shown in Figure 3:

$$\begin{aligned} \text{KeyGen}(\text{key_length}) &\rightarrow (\text{PK}, \text{SK}) \\ \text{HashFunctionSetup}() &\rightarrow H \\ \text{SystemSetup}() &\rightarrow (\text{C}_{\text{id}}, \text{T}_{\text{id}}, \text{Status}, \text{owner}_{\text{id}}) \end{aligned} \quad (1)$$

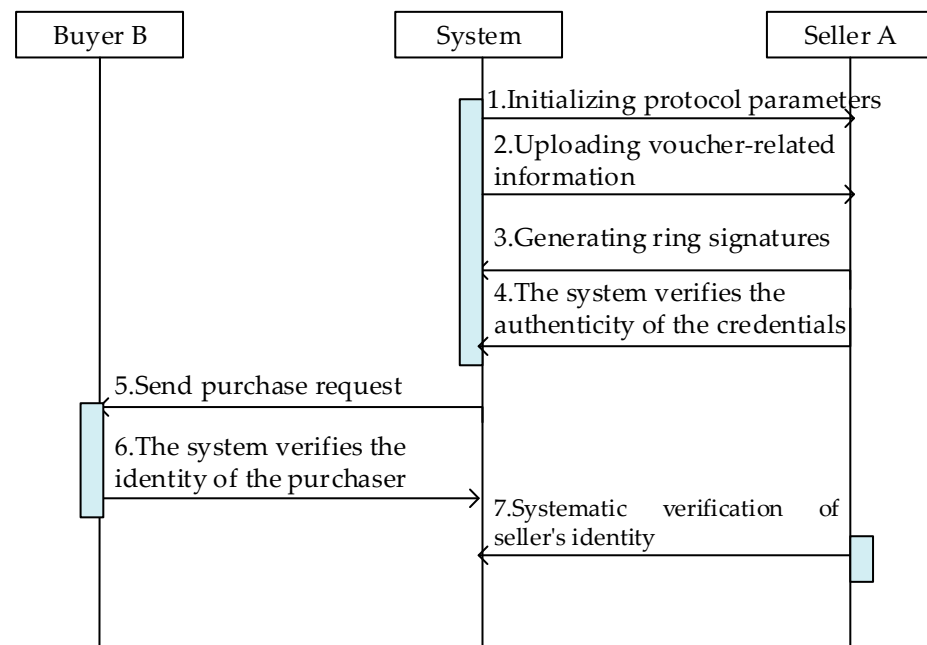


Figure 3. Purchase protocol interaction diagram.

In Equation (1), $\text{KeyGen}()$ represents the private key space initialization function; key_length represents the length of the key; PK represents the public key space; SK represents the private key space; $\text{Hashfunctionsetup}()$ represents hash function initialization; H represents the hash function generated by the hash function; $\text{SystemSetup}()$ represents the system initialization function; C_{id} represents the deposit certificate number; T_{id} represents the transaction number; Status represents the certificate status; and owner_{id} represents the credential owner.

Seller A will upload the credential information to the system and perform hash operations on it to generate a unique hash value for subsequent data integrity verification and tamper detection:

$$\begin{aligned} \{\text{C}_{\text{id}}, \text{id}_A, \text{C}_{\text{period}}, \text{E}_{\text{Amount}}, \text{E}_{\text{Type}}, \text{T}^*\} &\rightarrow G \\ H(G) &\rightarrow h_G \end{aligned} \quad (2)$$

In Equation (2), C_{id} represents the deposit number of the certificate; id_A represents the identity number of user A; C_{period} represents green energy consumption and supply cycles

in the certificate; E_{Amount} represents the total energy in the certificate; E_{Type} represents the energy type; T^* represents the timestamp generated when the voucher information was uploaded; G represents the uploaded voucher information; and h_G represents the hash of green card information.

The system checks the validity of the uploaded certificate information, especially the verification of the deposit certificate number. After successful verification, the system updates the ownership record of that credential on the blockchain and checks the on-chain record to prevent duplicate transactions. If the credential number does not exist, the system marks the credential status as not allocated:

$$\begin{aligned} \text{Check}() = \text{true} &\rightarrow \text{owner}_{id} = id_A \\ \text{QueryBlockchain}(C_{id}) = \text{null} &\rightarrow \text{status}(\text{null}) \end{aligned} \quad (3)$$

In Equation (3), $\text{Check}()$ represents the validation function; true represents obtaining true when validation passes; owner_{id} represents the credential owner; id_A represents the identity number of user A; $\text{QueryBlockchain}(C_{id})$ represents the verification of the existence of the certificate of deposit number in the voucher information; null represents that the certificate's deposit number (C_{id}) does not exist; and $\text{status}(\text{null})$ represents the emptying of the certificate status corresponding to the certificate number.

The blockchain record contains the certificate number, credential ownership, and status fields, which are uniformly stored in the Record structure on the chain. In addition, credential details are added to the Global Credential Registry (GCR) array to facilitate cross-node data synchronization and querying:

$$\begin{aligned} \text{Associate}(\text{Status}, \text{owner}_{id}, C_{id}) &\rightarrow \text{record} \\ \text{GCR} &= \{G, h_G\} \end{aligned} \quad (4)$$

In Equation (4), $\text{Associate}()$ represents parameter association functions; Status represents the certificate status; owner_{id} represents the credential owner; C_{id} represents the deposit number of the certificate; record represents the records generated by correlating Status , owner_{id} , and C_{id} ; G represents the uploaded voucher information; h_G represents the hash of green card information; and GCR represents the credential information.

(2) Ring signature authentication: The seller uses a ring signature mechanism to achieve anonymity and enhance transaction security. By choosing multiple ring members to sign, the certificate authenticity verification is enhanced. The system also records the public keys and timestamps of ring members to ensure follow-up audit traceability.

Seller A uses a cryptographic hash algorithm to generate a digital digest of the credentials, ensuring the integrity and immutability of its data:

$$H_{GCR_1} = H(\text{GCR}) \quad (5)$$

In Equation (5), H_{GCR_1} represents the voucher summary and $H(\text{GCR}[\cdot])$ represents the array of credential information (GCR).

Seller A implements a ring signature and selects at least two users as ring members. By combining the signature sequences of these members and applying XOR operation to construct the final ring signature, the parallel locking mechanism is implemented to enhance the anonymity and security of the transaction:

$$\begin{aligned} S_1 &= E_{sk_1}(E_{sk_2}(E_{sk_A}(H_{GCR_1}, T_A), T_2), T_1) \\ S_2 &= E_{sk_1}(E_{sk_A}(E_{sk_2}(H_{GCR_1}, T_2), T_A), T_1) \\ S_3 &= E_{sk_2}(E_{sk_1}(E_{sk_A}(H_{GCR_1}, T_A), T_1), T_2) \\ S_4 &= E_{sk_2}(E_{sk_A}(E_{sk_1}(H_{GCR_1}, T_1), T_A), T_2) \\ S_5 &= E_{sk_A}(E_{sk_2}(E_{sk_1}(H_{GCR_1}, T_1), T_2), T_A) \\ S_6 &= E_{sk_A}(E_{sk_1}(E_{sk_2}(H_{GCR_1}, T_2), T_1), T_A) \\ S_{\text{final}} &= S_1 \oplus S_2 \oplus S_3 \oplus S_4 \oplus S_5 \oplus S_6 \end{aligned} \quad (6)$$

In Equation (6), H_{GCR1} represents the voucher summary; S_i represents the signature of the i th signature order ($i = 1, 2, 3, 4, 5, 6$); S_1 indicates the order (A, 2, 1); T_j represents the Timestamp generated when user j signs ($j = A, 1, 2$); E_{sk_j} represents the private key cryptographic function for user j ; and S_{final} represents the final ring signature.

After receiving the timestamp and public key, the system constructs a signature verification matrix. Then, seller A creates and sends a unified credential array $UGCR[]$ to the system for verification by combining the ring signature and credential information GCR:

$$\begin{aligned} PK_T &= \{(T_1, pk_1), (T_2, pk_2), (T_A, pk_A)\} \\ UGCR &= \{H_{GCR1}, S_{final}\} \end{aligned} \quad (7)$$

In Equation (7), PK_T represents the array of signer public keys and timestamps involved in the signature; pk_j represents the public key for user j ; T_j represents the Timestamp generated when user j signs ($j = A, 1, 2$); H_{GCR1} represents the voucher summary; S_{final} represents the final ring signature; and $UGCR$ represents the voucher with ring signature.

(3) On-chain verification of credentials: The system performs hash and timestamp verification on signed certificates to ensure their validity and data consistency. After successful verification, the certificate will be encrypted and uploaded to the blockchain, ensuring its security and immutability:

The system uses the signature verification matrix to decrypt the credentials by the timestamp private key of each member in the user list $\{x, y, z\}$. These users correspond directly to the ring signature members $\{1, 2, A\}$, which ensures the integrity and security of the verification process:

$$\begin{aligned} D_{pk_x}(D_{pk_y}(D_{pk_z}(GCR, T_z), T_y), T_x) &\rightarrow H_{GCR2} \\ H_{GCR1} &= H_{GCR2} \end{aligned} \quad (8)$$

In Equation (8), T_j represents the verification of timestamps in the array when user j signs ($j = x, y, z$); D_{pk_j} represents the public key decryption function for user j ($j = x, y, z$), when z takes the value 1 of $\{1, 2, A\}$, $T_z = T_1$; pk_j represents the public key for user j ; H_{GCR2} represents the hash value obtained after decryption; and H_{GCR1} represents the voucher summary.

The system uses the signature verification matrix to check the timestamp and compare the current timestamp with the timestamp when the certificate was uploaded to verify the timeliness of the certificate and prevent its illegal use:

$$T_y > T^* \& T_y > T^* \& T_z > T^* \quad (9)$$

In Equation (9), T_j represents the verification of timestamps in the array when user j signs ($j = x, y, z$) and T^* represents the timestamp generated when the voucher information was uploaded.

(4) Encrypted purchase request submission: The buyer initiates a certificate purchase request on the trading platform, and the system ensures the security of the transaction by verifying the credential status and the buyer's signature. This mechanism can effectively resist double-spending attacks while maintaining the anonymity of transactions.

After receiving the uniform credential array $UGCR[]$, the buyer initiates the encrypted purchase request M , which contains encrypted identification and the buyer's private key to ensure security and maintain anonymity during the transaction:

$$\begin{aligned} M_{B1} &= E_{pk_A}(id_B, T_{id}, pk_B) \\ S_B &= E_{sk_B}(M_{B1}) \\ M &= \{M_{B1}, S_B\} \end{aligned} \quad (10)$$

In Equation (10), M_{B1} represents a message containing the identity of buyer B; id_B represents the identity number of buyer B; T_{id} represents the transaction number; pk_B represents the public key of buyer B; E_{sk_B} represents buyer B's private key encryption

function; S_B represents the signature of buyer B; and M represents the purchase request message signed by buyer B.

Upon receiving a credential purchase request from buyer B, the system first performs credential status verification to ensure its tradability. After verification, the request is forwarded to vendor A. After receiving the request, the seller uses blockchain technology to verify the anonymous identity of buyer B and the integrity of the signature. In this process, the system ensures the anonymity of the identities of the transaction parties, while only the basic transaction information of the certificate is processed.

$$\begin{aligned} D_{pk_A}(M) &\rightarrow \{id_B, T_{id}, pk_B\} \rightarrow \text{Check}(id_B) \\ M_{B1} &= E_{sk_B}(S_B) \end{aligned} \tag{11}$$

In Equation (11), D_{pk_A} represents the public key decryption function for seller A; T_{id} represents the transaction number; pk_B represents the public key of buyer B; E_{sk_B} represents buyer B's private key encryption function; S_B represents the signature of buyer B; M_{B1} represents a message containing the identity of buyer B; id_B represents the identity number of buyer B; and M represents the purchase request message signed by buyer B.

The system performs two-factor verification: first, it checks the transaction status of the certificate to confirm that it has not been traded, and second, it checks the holder's identity ID hash to ensure the consistency and authenticity of the owner:

$$\text{Check } H(\text{owner}_{id}) = H(id_A) \tag{12}$$

In Equation (12), Check represents the validation function; id_A represents the identity number of user A; H represents the hash function generated by the hash function; and ownerid represents the credential owner.

3.2. Payment Protocol

The payment protocol goes through three key stages in turn: triggering the payment protocol, performing on-chain funds settlement, and certificate delivery, shown as in Figure 4.

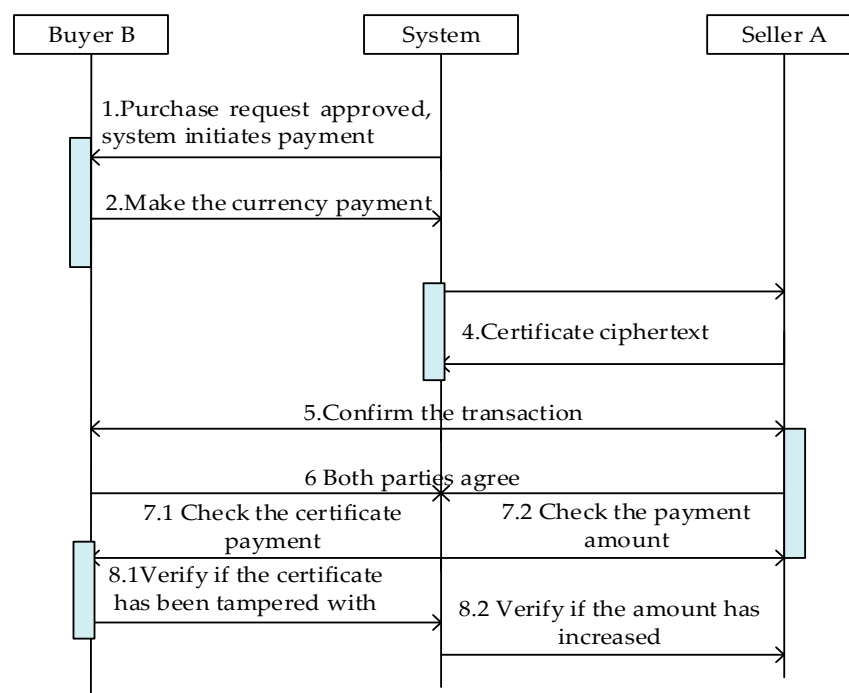


Figure 4. Payment protocol interaction diagram.

- (1) Trigger the payment protocol: The system initiates the transaction execution to buyer B and automatically processes the payment operation through the smart contract.
- (2) Perform on-chain fund settlement: After buyer B completes the transfer of funds on the blockchain platform, the smart contract will be automatically executed, and the system will only settle the transaction after both parties confirm that the transaction is correct:

$$\text{Balance}_B - \text{PaymentAmount} \rightarrow \text{Balance}_B' \quad (13)$$

In Equation (13), Balance_B represents the balance of buyer B; PaymentAmount represents the amount of voucher payment; and $\text{Balance}_B'$ represents the balance after the purchase of certificates by buyer B.

- (3) Certificate Delivery:

The system first passes buyer B's anonymous credentials to seller A:

$$D_{pk_A}(M) \rightarrow \{id_B, T_{id}, pk_B\} \quad (14)$$

In Equation (14), D_{pk_A} represents the public key decryption function for seller A; id_B represents the identity number of buyer B; T_{id} represents the transaction number; pk_B represents the public key of buyer B; and M represents the purchase request message signed by buyer B.

Seller A uses buyer B's public key and trusted timestamp to encrypt the global credential registry array $GCR[]$ and upload it to the blockchain:

$$\begin{aligned} C_{B1} &= E_{sk_B}(T_B) \\ C_{B2} &= E_{sk_B}(GCR, T_B) \end{aligned} \quad (15)$$

In Equation (15), C_{B1} represents the timestamp ciphertext; C_{B2} represents the voucher ciphertext; T_B represents the signature of buyer B; E_{sk_B} represents buyer B's private key cryptographic function; and GCR represents the credential information.

After the system encryption certificate verification, the smart contract coordinates the two parties to establish a transaction. After confirmation, the system decrypts the certificate and passes it to seller B, and triggers the smart contract to automatically settle the funds to buyer A. Both parties verify the integrity of the certificate, the funds arrive, and the transaction is completed after the consistency verification:

$$\begin{aligned} D_{pk_B}(C_{B1}) &\rightarrow T_B \\ D_{pk_B}(C_{B2}, T_B) &\rightarrow \{GCR, T_B\} \rightarrow G \\ \text{CheckH}(G) &= h_G? \\ \text{CheckBalance}_A + \text{PaymentAmount} &\stackrel{?}{=} \text{Balance}_A' \end{aligned} \quad (16)$$

In Equation (16), D_{pk_B} represents the public key decryption function for buyer B; C_{B1} represents the timestamp ciphertext; C_{B2} represents the voucher ciphertext; T_B represents the signature of buyer B; GCR represents the credential information; Check represents the validation function; H represents the hash function generated by the hash function; h_G represents the hash of green card information; G represents the uploaded voucher information; Balance_A represents the balance of seller A; PaymentAmount represents the amount of voucher payment; and $\text{Balance}_A'$ represents the balance after purchase of certificates by seller A.

3.3. Non-Transferable Protocol

The non-transferable protocol goes through two key stages in turn: updating blockchain records and the verification of credential transaction status, as shown in Figure 5.

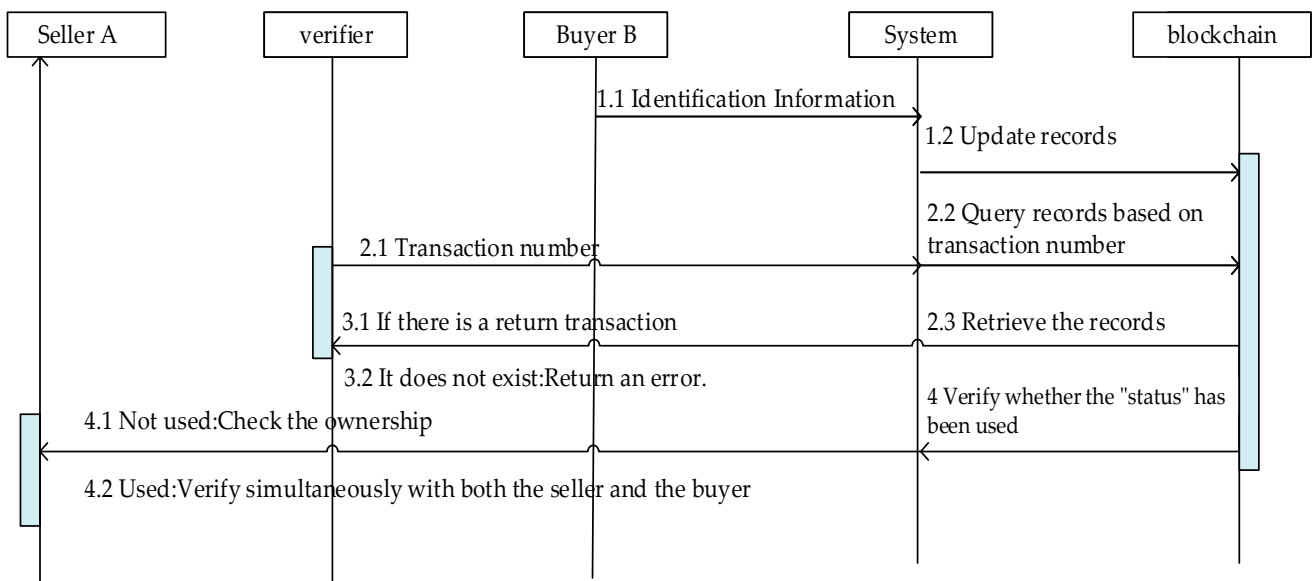


Figure 5. Non-transferable protocol interaction diagram.

(1) Update of chain records:

Once the transaction is closed, the system broadcasts the transaction details to the blockchain, which triggers an update of the record on the chain, which involves a state change, ownership transfer, and binding the certificate entry to the transaction number:

$$\begin{aligned}
 & \text{status}(\text{null}) \rightarrow \text{status}(\text{used}) \\
 & \text{owner}_{id}(\text{id}_A) \rightarrow \text{owner}_{id}(\text{id}_B) \\
 & \text{Associate}(\text{status}, \text{owner}_{id}, C_{id}, T_{id})
 \end{aligned} \tag{17}$$

In Equation (17), Status represents the certificate status; status(null) represents the empty certificate status corresponding to the certificate number; status(used) represents that the certificate number corresponding to the certificate status has been traded; $\text{owner}_{id}(\text{id}_A) \rightarrow \text{owner}_{id}(\text{id}_B)$ means ownership changed from seller A to buyer B; Associate (status, owner_{id} , C_{id} , T_{id}) represents the association between the certificate's deposit number and the certificate status, owner code, and transaction number attributes.

(2) Verification of voucher transaction status:

The credential transaction status is reviewed by an authorized verifier on the blockchain by issuing a query request. The system responds to the request by retrieving the transaction records of the relevant credentials in the blockchain. If there is a transaction, the system will verify the correctness of the certificate owner id. An id mismatch will return a query error. The correct id and idle credential status indicate that no transaction occurred, and the system flags 'certificate not traded' and notifies the verifier. If the credential status is 'used', indicating that the transaction has been completed, the system will report the 'certificate has been traded' and carry out a further verification process:

$$\text{Check owner}_{id} = \text{id}_A \rightarrow \text{id}_B? \tag{18}$$

In Equation (18), Check represents the validation function; owner_{id} represents the credential owner; id_A represents the identity number of user A; and id_B represents the identity number of buyer B.

4. Experimental Analysis

4.1. Security Analysis

The protocol discussed in this paper ensures anonymity and privacy through the use of ring signatures and encryption, which differs from the traceable anonymity of RingCT 2.0 of Protocol [9] and Protocol [12]. To defend against man-in-the-middle attacks, this protocol combines authentication, encryption, and consensus mechanisms, effectively preventing data interception and tampering, unlike the decentralization approach of Protocol [11]. To combat double-spend attacks, this protocol leverages blockchain immutability and unique identifiers to ensure that only unused credentials are processed, in contrast to the privacy enhancement of Protocol [9] and the decentralization of Protocol [11]. In preventing transaction rollback attacks, this protocol uses blockchain immutability to ensure that transactions cannot be modified or revoked once completed, in contrast to Protocol [12]’s public traceability verification. Finally, this protocol avoids duplicate transactions by verifying electronic certificate records before processing, ensuring that transactions are final and unrepeatable, unlike Protocol [12]’s traceability verification to prevent transaction replays. The security comparison is listed in Table 1.

Table 1. Security comparison.

Security Performance	This Paper	Reference [9]	Reference [11]	Reference [12]
User privacy	✓	✓	×	✓
Man-in-the-middle attacks	✓	×	✓	×
Double spending attacks	✓	✓	✓	✓
Transaction rollback attacks	✓	×	×	✓
Transaction replay attacks	✓	×	×	✓

Based on the above analysis, in order to show the advantages of this paper in preventing secondary transactions more clearly, we use AHP (hierarchical analysis) to score each scheme. Security indicators such as user privacy and transaction rollback attacks are taken as the criterion layer, and the several schemes compared in Table 1 are taken as the measure layer. The results obtained are shown in Table 2. The detailed hierarchical model is shown in Figure 6.

Table 2. Program-level judgment matrix summary results.

	This Paper	Reference [9]	Reference [11]	Reference [12]	Weights	Consistency Check
Double spending attacks	1	5	1	3	33.284	pass
Transaction rollback attacks	0.2	1	0.2	0.333	5.262	pass
Transaction replay attacks	1	5	1	3	36.864	pass
Man-in-the-middle attacks	0.333	3	0.2	0.333	9.044	pass
User privacy	0.3	0.3	0.1	0	15.545	pass

Transaction replay attacks (36.864%) and double payment attacks (33.284%) are considered the most critical risk factors in the system security assessment, so prioritizing protection against these attacks is critical. User privacy (15.545%) and man-in-the-middle attacks (9.044%) also had an impact. Transaction rollback attacks (5.262%) are considered the least threatening in the current analysis.

Based on the above results, the scores of the schemes are shown in Figure 7. It can be seen that the scheme of this paper has obvious advantages in transaction security and the prevention of secondary transactions.

This paper’s green certificate transaction protocol demonstrates a strong defense against a wide range of cyber-security threats prevalent in digital transactions. It uniquely combines user privacy with traceability, provides strong defenses against man-in-the-middle, and ensures that transactions are irreversible and immune to replay attacks. While other protocols, such as PBT and TRCT, also provide important protections, particularly in the areas of privacy and traceability, this protocol’s integrated approach to verifying

transaction legitimacy and certificate status provides a strong defense against double spending and fraudulent activity in the area of green certificate trading.

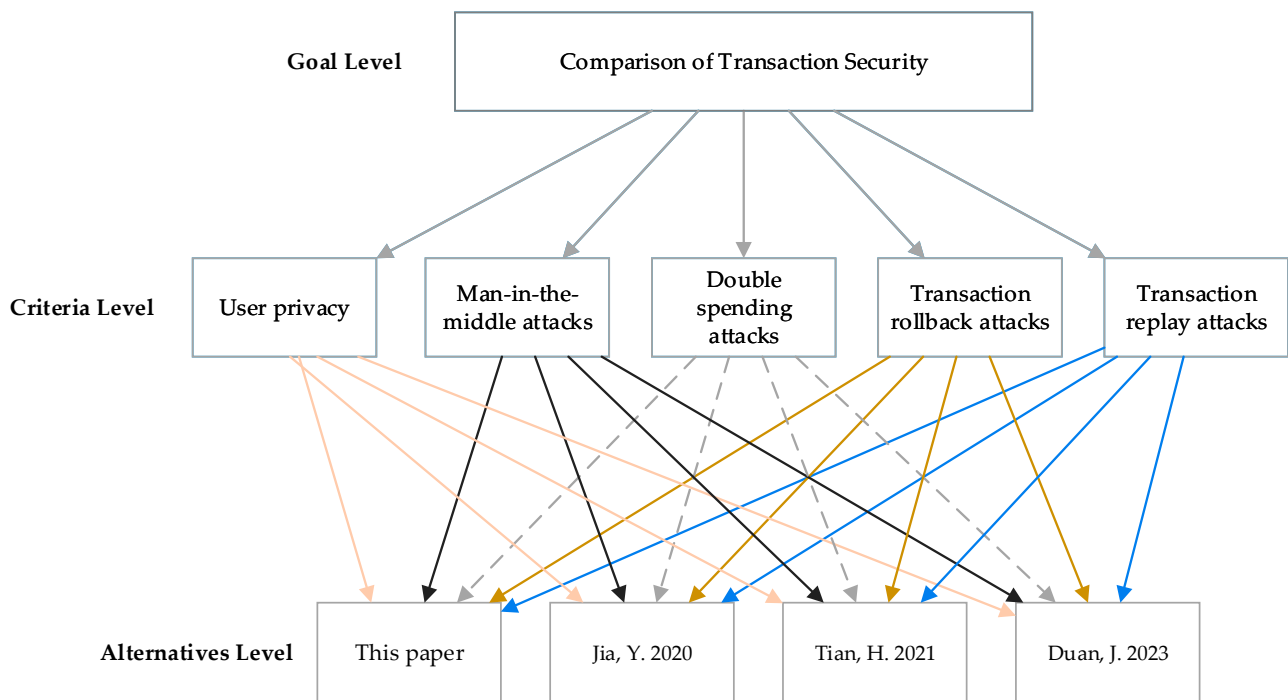


Figure 6. Comparison of Traditional Protocols [9,11,12] and Integrated Protocols.

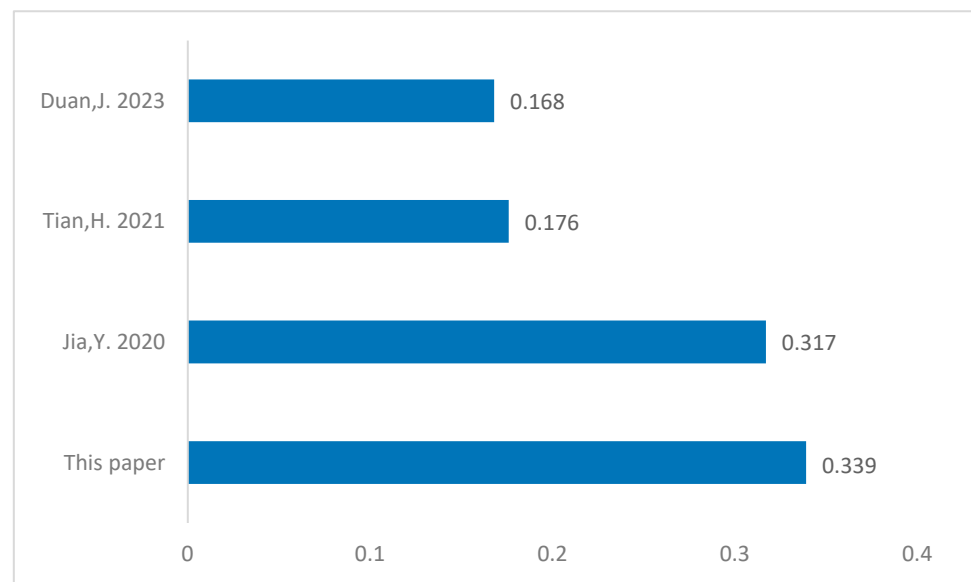
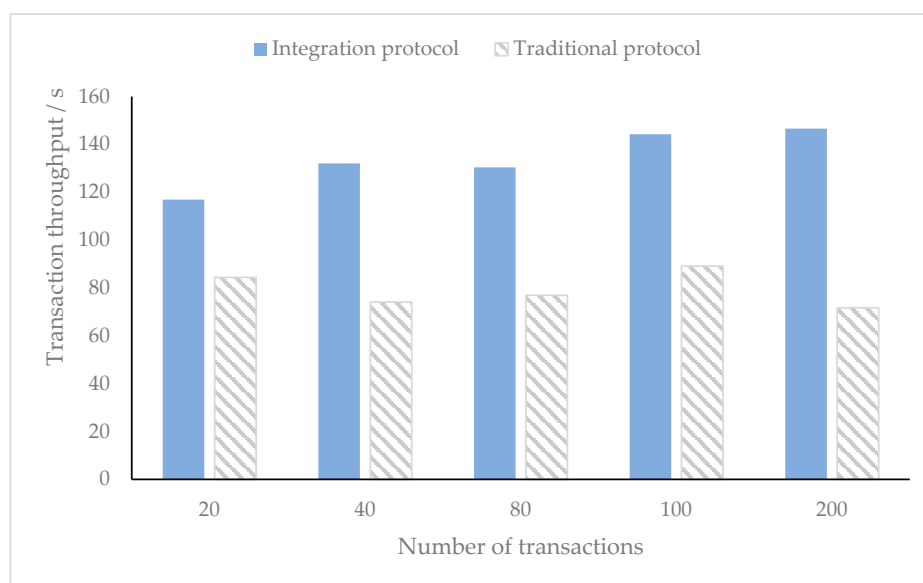


Figure 7. Scheme score from [9,11,12] compared with the Proposed Scheme.

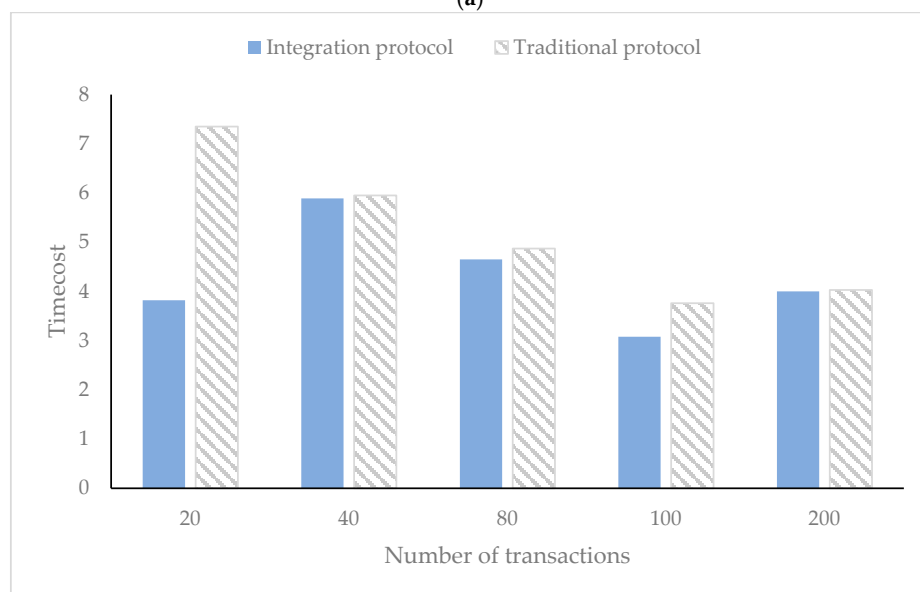
4.2. Performance Testing

Traditional transaction models often involve separate, cumbersome processes for purchase and payment. In contrast, the scheme proposed in this paper integrates these protocols into a seamless process, automatically transitioning from purchase to payment without manual intervention. This integration simplifies operations and accelerates transactions. Additionally, a non-transferable agreement phase ensures green certificates are valid only once, providing complete traceability and effectively preventing secondary trading, thereby enhancing transaction security and reliability.

To compare the performance of the integration protocol and the traditional protocol, this study analyzes two key performance metrics: average transaction latency and transaction throughput. In Figure 8a, as the number of transactions increases from 20 to 200, the transaction throughput of the integration protocol is consistently higher than that of the traditional protocol, and the difference in throughput between the two continues to grow, from about 40 initially to 80. This indicates that the integrated protocol is able to more effectively increase the transaction processing capability when dealing with a larger number of trading accounts, which in turn increases the security of the transaction and prevents the effect of secondary transactions. In Figure 8b, the traditional protocol incurs higher time costs compared to the integrated protocol. These delays can negatively affect double-spending prevention and overall system security, as slower processing may lead to transaction validation delays and increased opportunities for fraud. Additionally, the decreased responsiveness and efficiency of the traditional protocol make it harder to maintain strong security and promptly address threats.



(a)



(b)

Figure 8. Comparison of traditional and integrated protocols. (a) Comparison of transaction throughput. (b) Comparison of Timecost.

Figure 9 shows the transaction throughput for the non-transferable, payment, and purchase protocols running independently, as well as the transaction throughput for the integrated protocol that combines all three. As the transaction volume increases, the purchase protocol grows from 62.5 to 94.61, the payment protocol grows from 52.22 to 92.21, the non-transferable protocol grows from 74.07 to 88.38, and the integrated protocol grows from 116.85 to 146.56. While all four protocols show growth, the integrated protocol consistently provides higher throughput compared to the other three protocols. This indicates that the integrated protocol has a significant advantage in processing efficiency and can efficiently process more transactions as the transaction volume increases.

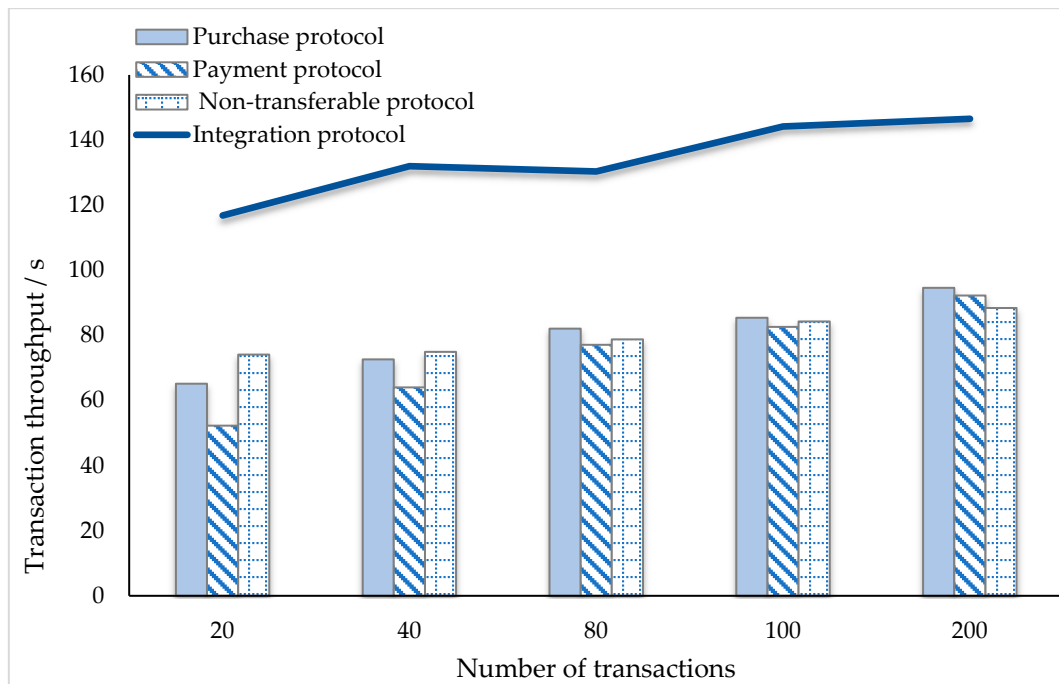


Figure 9. Throughput comparison of transaction.

5. Conclusions

This paper presents a blockchain-based green certificate trading protocol designed to ensure the security and uniqueness of transactions throughout the entire process. The primary contributions and value of this work are as follows:

- (1) **Integration of purchase, payment, and tracking:** Unlike traditional green certificate systems, which often operate in isolated phases, our protocol integrates purchase, payment, and tracking into a unified system. This integration ensures transaction consistency and completeness, addressing the shortcomings of previous systems.
- (2) **Enhanced privacy and fraud prevention:** To safeguard participant anonymity and prevent intermediary fraud, the protocol employs ring signatures. This method protects participant identities while enabling third-party verification, enhancing the security of transactions.
- (3) **Mechanism to prevent double spending:** To tackle the issue of multiple claims on a single green certificate, our protocol introduces a mechanism that prevents duplicate transactions. This ensures that each certificate's green attributes are recognized only once, preventing the inflation of renewable energy contributions and maintaining the credibility of the green certificate system.
- (4) **Improved data security through blockchain integration:** By incorporating blockchain technology, including cryptographic methods and smart contract automation, the protocol strengthens data integrity and transaction security. Despite these advancements, challenges such as high energy consumption and blockchain implementation

complexity remain. Future research will focus on improving transaction performance, evaluating system time cost effectiveness, and exploring cross-chain interoperability to address these limitations and expand the applicability of the protocol.

Based on the performance results and AHP scoring for attack prevention, the protocol in this paper demonstrates significant advantages:

- (1) Good transaction throughput: As shown in the results, the integrated protocol consistently outperforms traditional models in transaction throughput, highlighting its efficiency in handling increased transaction volumes.
- (2) Effective prevention of attacks: The protocol's design addresses key security concerns effectively. It excels in preventing double spending, mitigating man-in-the-middle attacks, and ensuring transaction immutability and traceability. The high AHP scores for these security aspects underscore its robust defense mechanisms against various attacks.

In conclusion, the proposed blockchain-based green certificate trading protocol offers a comprehensive solution to enhance the security, traceability, and credibility of green certificate transactions. It addresses critical issues such as double spending, credibility, and traceability.

Author Contributions: Conceptualization: Y.L., M.Y. and S.X.; data curation: X.L.; formal analysis: M.J., M.Y. and S.X.; funding acquisition: Y.L.; investigation: X.L. and S.P.; methodology: Y.L., M.J., M.Y. and S.X.; project administration: Y.L. and S.X.; resources: X.L. and J.Z.; software: S.Z.; supervision: M.Y. and J.Z.; validation: M.J., M.Y., S.X. and Z.G.; writing—original draft: M.J.; writing—review and editing: M.J. and S.X. All authors have read and agreed to the published version of the manuscript.

Funding: This work received financial support from the Project of Yichang Power Supply Company, State Grid Hubei Electric Power Co., Ltd. (B715H023001N).

Data Availability Statement: The original contributions presented in the study are included in the article.

Conflicts of Interest: Authors Yang Li, Xiaojun Liu, Jia Zhu, Shurui Peng and Zhongming Gu were employed by the Yichang Power Supply Company of State Grid Hubei Electric Power Co., Ltd. The authors declare that this study received funding from Yichang Power Supply Company of State Grid Hubei Electric Power Co., Ltd. The funder was not involved in the study design, collection, analysis, interpretation of data, the writing of this article or the decision to submit it for publication. The remaining authors declare that the research was conducted in the absence of any commercial or financial relationships that could be construed as a potential conflict of interest.

References

1. Guo, H.; Chen, Q. Modeling strategic behaviors of renewable energy with joint consideration on energy and tradable green certificate markets. *IEEE Trans. Power Syst.* **2019**, *35*, 1898–1910. [[CrossRef](#)]
2. Wang, T.; Gong, Y. A review on promoting share of renewable energy by green-trading mechanisms in power system. *Renew. Sus. Energy Rev.* **2014**, *40*, 923–929. [[CrossRef](#)]
3. Dong, C.; Zhou, R. Rushing for subsidies: The impact of feed-in tariffs on solar photovoltaic capacity development in China. *Appl. Energy* **2021**, *281*, 116007. [[CrossRef](#)]
4. Zhou, D.; Hu, F. Regional allocation of renewable energy quota in China under the policy of renewable portfolio standards. *Resour. Conserv. Recycl.* **2022**, *176*, 105904. [[CrossRef](#)]
5. Dimitriadis, C.; Tsimopoulos, E. Optimal bidding strategy of a gas-fired power plant in interdependent low-carbon electricity and natural gas markets. *Energy* **2023**, *277*, 127710. [[CrossRef](#)]
6. Zhang, S.; Hu, W. Low-carbon optimal operation of distributed energy systems in the context of electricity supply restriction and carbon tax policy: A fully decentralized energy dispatch strategy. *J. Clean. Prod.* **2023**, *396*, 136511. [[CrossRef](#)]
7. Shen, J.; Zhou, T. Block design-based key agreement for group data sharing in cloud computing. *IEEE Trans. Dependable Secur. Comput.* **2017**, *16*, 996–1010. [[CrossRef](#)]
8. Xiao, R.; Ren, W. A Mixing Scheme Using a Decentralized Signature Protocol for Privacy Protection in Bitcoin Blockchain. *IEEE Trans. Dependable Secur. Comput.* **2019**, *18*, 1793–1803. [[CrossRef](#)]
9. Jia, Y.; Sun, S. PBT: A New Privacy-Preserving Payment Protocol for Blockchain Transactions. *IEEE Trans. Dependable Secur. Comput.* **2020**, *19*, 647–662. [[CrossRef](#)]
10. Zhang, J.; Cheng, Y. A Reputation-Based Mechanism for Transaction Processing in Blockchain Systems. *IEEE Trans. Comput.* **2021**, *71*, 2423–2434. [[CrossRef](#)]

11. Tian, H.; Xue, K. Enabling cross-chain transactions: A decentralized cryptocurrency exchange protocol. *IEEE Trans. Inf. Forensics Secur.* **2021**, *16*, 3928–3941. [[CrossRef](#)]
12. Duan, J.; Wang, L. TRCT: A Traceable Anonymous Transaction Protocol for Blockchain. *IEEE Trans. Inf. Forensics Secur.* **2023**, *18*, 4391–4405. [[CrossRef](#)]
13. Jie, W.; Qiu, W. A Secure and Flexible Blockchain-Based Offline Payment Protocol. *IEEE Trans. Comput.* **2023**, *73*, 408–421. [[CrossRef](#)]
14. Zhou, H.; Zhang, Z. Joint Optimization of Computing Offloading and Service Caching in Edge Computing-Based Smart Grid. *IEEE Trans. Cloud Comput.* **2022**, *11*, 1122–1132. [[CrossRef](#)]
15. Zhou, H.; Wang, Z. UAV-Aided Computation Offloading in Mobile-Edge Computing Networks: A Stackelberg Game Approach. *IEEE Internet Things* **2023**, *10*, 6622–6633. [[CrossRef](#)]
16. Kumar, P.; Gurtov, A. Lightweight Authentication and Key Agreement for Smart Metering in Smart Energy Networks. *IEEE Trans. Smart Grid* **2018**, *10*, 4349–4359. [[CrossRef](#)]
17. Yu, Y.; Guo, Y. Trusted transactions in micro-grid based on blockchain. *Energies* **2019**, *12*, 1952. [[CrossRef](#)]
18. Gajić, D.B.; Petrović, V.B. A Distributed Ledger-Based Automated Marketplace for the Decentralized Trading of Renewable Energy in Smart Grids. *Energies* **2022**, *15*, 2121. [[CrossRef](#)]
19. Tsao, Y.; Thanh, V. Toward Blockchain-Based Renewable Energy Microgrid Design Considering Default Risk And Demand Uncertainty. *Renew. Energy* **2021**, *163*, 870–881. [[CrossRef](#)]
20. Juszczyk, O.; Shahzad, K. Blockchain technology for renewable energy: Principles, applications and prospects. *Energies* **2022**, *15*, 4603. [[CrossRef](#)]
21. Xie, L.; Wu, J. Automatic Generation Control Strategy for Integrated Energy System Based on Ubiquitous Power Internet of Things. *IEEE Internet Things* **2022**, *10*, 7645–7654. [[CrossRef](#)]
22. Zhang, W.; Zeadally, S. Joint Service Quality Control and Resource Allocation for Service Reliability Maximization in Edge Computing. *IEEE Trans. Commun.* **2022**, *71*, 935–948. [[CrossRef](#)]
23. Yun, J.; Jiang, D. Grasping detection of dual manipulators based on Markov decision process with neural network. *Neural Netw.* **2023**, *169*, 778–792. [[CrossRef](#)] [[PubMed](#)]
24. Huang, Z.; Weng, S. Ranking Method of Intuitionistic Fuzzy Numbers and Multiple Attribute Decision Making Based on the Probabilistic Dominance Relationship. *Symmetry* **2023**, *15*, 1001. [[CrossRef](#)]
25. Zhong, J.; Chen, T. Face expression recognition based on NGO-BILSTM model. *Front. Neurobot.* **2023**, *17*, 1155038. [[CrossRef](#)]
26. Wan, S.; Tang, B. A writing style-based multi-task model with the hierarchical attention for rumor detection. *Int. J. Mach. Learn. Cyber.* **2023**, *14*, 3993–4008. [[CrossRef](#)]
27. Zhou, H.; Li, M. Accelerating Deep Learning Inference via Model Parallelism and Partial Computation Offloading. *IEEE Trans. Parallel Distrib. Syst.* **2022**, *34*, 475–488. [[CrossRef](#)]
28. Sun, H.; Li, B. Multi-level Feature Interaction and Efficient Non-Local Information Enhanced Channel Attention for image dehazing. *Neural Netw.* **2023**, *163*, 10–27. [[CrossRef](#)]
29. Zhang, H.; Huang, M. Capacity Maximization in RIS-UAV Networks: A DDQN-Based Trajectory and Phase Shift Optimization Approach. *IEEE Trans. Wirel. Commun.* **2023**, *22*, 2583–2591. [[CrossRef](#)]

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.