*electronics*

*Article*

# Editable and Verifiable Anonymous Authentication Incorporating Blockchain in the Internet of Energy

**Qiaolian Zhang [1,2], Fenhua Bai [1,2], Zhuo Yu [3], Yingli Liu [1,2], Tao Shen [1,2,*], Anke Xie [4] and Lin Huang [5]**

[1] Faculty of Information Engineering and Automation, Kunming University of Science and Technology, Kunming 650093, China; zhangqiaolian@stu.kust.edu.cn (Q.Z.); bofenhua@stu.kust.edu.cn (F.B.); lyl@kust.edu.cn (Y.L.)
[2] Yunnan Key Laboratory of Computer Technologies Application, Kunming University of Science and Technology, Kunming 650500, China
[3] Beijing Zhongdian Puhua Information Technology Company, Ltd., Beijing 100192, China; yuzhuo@sgitg.sgcc.com.cn
[4] Yunnan Key Laboratory of Blockchain Application Technology, Kunming 650233, China; anke@bhynii.com
[5] Yunnan Provincial Academy of Science and Technology, Kunming 650051, China; yilinhuanglin1@gmail.com
* Correspondence: shentao@kust.edu.cn

**Abstract:** With the continuous development of the Internet of Energy, the access of a large number of distributed renewable energy has caused difficulties in energy management. The traditional energy management mode cannot meet the needs of existing energy management and trading. Therefore, this paper proposes an integrated energy management platform based on blockchain, which allows multiple decentralized energy management systems to conduct unified identity authentication. At the same time, an editable and verifiable anonymous authentication (EVAA) scheme integrating blockchain in the Internet of Energy is designed, which combines the idea of chameleon hash (CH) and the algorithm of elliptic curve encryption (ECC) to realize the dual identity authentication of user information. Finally, the generated certificate is stored in the chain through blockchain consensus. The scheme is mainly constructed using multiple secure cryptographic algorithms, which combine the advantages of blockchain for information authentication. Thus, it can accomplish user cross-system authentication and transaction, and achieve more secure editable anonymous identity authentication through the algorithm performance test, compared with the existing similar schemes under the unified test standard. This paper not only ensures the operation efficiency, but also reflects the obvious advantage of realizing higher intensity security performance.

**Keywords:** Internet of Energy; blockchain; anonymous authentication; editable; verification

check for updates

**Citation:** Zhang, Q.; Bai, F.; Yu, Z.; Liu, Y.; Shen, T.; Xie, A.; Huang, L. Editable and Verifiable Anonymous Authentication Incorporating Blockchain in the Internet of Energy. *Electronics* **2022**, *11*, 1992. https://doi.org/10.3390/electronics11131992

Academic Editor: Martin Reisslein

Received: 31 May 2022
Accepted: 23 June 2022
Published: 25 June 2022

## 1. Introduction

In recent years, with the awakening of people's awareness of low-carbon environmental protection and the growing demand for electricity resources, renewable energy, such as wind power, solar power, and other green energy sources, has attracted widespread attention around the world. For their ability to alleviate the fossil fuel crisis and reduce greenhouse gas emissions, it is recyclable and cost-effective [1]. The development of modern Internet technology has made it possible for individual users to store, sell, and transmit energy [2,3]. The existing energy trading system relies on a centralized architecture, and the whole process is controlled by a central organization. Access to a large number of distributed energy has brought great challenges to this kind of centralized energy transaction [4]. At present, P2P (Peer to Peer) energy trading schemes based on various information and communication technologies [5–7] can solve the problem of the two-way flow of information and power among distributed energy in the process of distributed energy trading. However, the centralized intermediary used to manage P2P energy transactions among distributed energy may lead to security problems, such as privacy leakage and single point of failure. Therefore, distributed P2P energy transactions will become the mainstream way of energy transactions in the future [8].

Due to the conceptual similarity between blockchain technology and distributed energy trading, energy trading based on blockchain has become a research hotspot for many scholars. In recent years, blockchain technology has been widely used in P2P energy trading systems for its decentralized, tamper-evident, and traceability features. Many researchers have proposed blockchain-based P2P energy trading schemes [9–18]. Huang et al. [9] proposed a multi-blockchain-based energy trading framework to ensure the security and privacy of energy transactions. In [10], the authors put forward a secure and efficient energy trading scheme that enables green computing while ensuring privacy security. Abdella et al. [11] introduced a P2P energy trading framework based on permissioned blockchain to integrate three different types of energy trading systems to achieve a unified form of energy trading and settlement. In [17], a blockchain-based multi-microgrid two-layer energy trading framework is proposed to provide decentralized trading, information transparency, and a mutual trust system for each node in the trading market. Although the above energy trading schemes based on the blockchain can solve some security problems in the centralized energy trading system, they do not solve the problem of user privacy. If the privacy problem is not solved, users with additional energy may not be willing to join the P2P energy trading system for energy trading.

Therefore, some scholars have carried out a series of research on the privacy and security of P2P energy transactions based on blockchain. Li et al. [13] used an access control mechanism and anonymous authentication technology to protect user privacy. Aitzhan et al. [14] proposed a multi-signature and anonymous message technology to protect the privacy of users. In [18], the dynamic account allocation method and differential privacy based on noise are combined to protect user privacy. Gai et al. [19] proposed to hide the user privacy information by using the account mapping algorithm based on blockchain to realize privacy protection. Zhao et al. [20] proposed a differential privacy scheme based on noise, which protects users' privacy by utilizing the privacy parameter to limit the relevant information of the data set with noise output leakage. In [21], a supervised anonymous authentication scheme suitable for blockchain systems is realized by combining anonymous authentication technology, zero-knowledge proof, and group signature. However, most of the existing schemes only realize a semi-decentralized energy system, only a few certified third-party nodes can manage and verify the transaction, and the prosumers in the energy transaction have no right to manage and verify the transaction. In addition, once the user's private information is uploaded to the blockchain, the user cannot update the uploaded information due to the tamper-proof characteristics of the blockchain.

In order to make up for the shortcomings of blockchain, Ateniese et al. [22] proposed the concept of "Redactable blockchain", which rewrites the blockchain history by using chameleon hash (CH) [23]. Huang et al. [24] proposed a new threshold chameleon hash (TCH) and accountable-and-sanitizable chameleon signature (ASCS) schemes to build a reconfigurable blockchain. Wei et al. [25] proposed a rewritable blockchain for secure federated learning based on a novel chameleon hash scheme with a changeable trapdoor (CHCT). The above schemes use the improved chameleon hash function to replace the original hash algorithm (such as SHA256) to build a reconfigurable blockchain. In the above solutions, rewritable roles should be selected for the setting of the rewriting function. Once the selected roles are attacked, the security of the whole system will be threatened [26].

In view of the above problems, this paper proposes an integrated energy management platform based on blockchain. The platform allows access to multiple decentralized energy management systems and carries out unified identity authentication for users so as to realize that one authentication can respond to different systems, support users to conduct cross-system transactions, and accomplish the interconnection of multiple energy management systems. At the same time, in order to achieve a high degree of autonomy and anonymous authentication of user identity information, a user-editable and verifiable anonymous authentication scheme integrating blockchain in the Internet of Energy is proposed. Combined with the idea of CH and the algorithm of ECC (elliptic curve encryption) with the shorter key to achieving higher security, the dual identity authentication of user information is realized, and the hash value generated by the chameleon hash signature is further authenticated to generate a certificate. When there is a need to modify data, it is necessary to provide correct trapdoor and certificate at the same time to modify. Finally, the certificate is stored in the chain through blockchain consensus. The scheme is mainly constructed using multiple secure cryptographic algorithms, which combine the advantages of blockchain for information authentication so as to achieve the effect of one-time registration and multiple uses. Users can authorize multiple different energy management systems to conduct energy transactions.

The specific contributions of this paper include the following three points:

(1) We propose an integrated energy management platform based on blockchain, which mainly carries out unified authentication for the identity of energy prosumers. Users can authorize multiple different energy management systems according to their own needs only through one-time authentication on our platform, and realize cross-system energy transactions;

(2) We come up with an editable and verifiable anonymous authentication (EVAA) scheme integrating blockchain in the Internet of Energy, which combines the idea of CH and the algorithm of ECC to realize the dual identity authentication of user information;

(3) Through experimental verification, the scheme proposed in this paper improves the efficiency of the user authentication process on the premise of ensuring the security of user identity. Meanwhile, the integrated energy management platform based on blockchain proposed in this paper can not only ensure the privacy and security of users, but also expand the scope of energy transactions, which is convenient for users to conduct cross-system energy transactions.

The remainder of the paper is organized as follows. The second section introduces the related work of the paper, and the third section introduces the overall system architecture, the scheme structure in detail about EVAA. Section 4 analyzes security analysis of EVAA and compares the efficiency and function of the scheme. Finally, the conclusions are given in Section 5.

## 2. Related Works

Recently, blockchain technology is considered to be one of the most influential technologies. It provides an effective solution to the security problems in current energy management and trading process. This part mainly introduces the related work from the following two aspects: identity authentication and preparatory knowledge.

### *2.1. Identity Authentication*

Identity authentication is a process to confirm whether a claimed identity is real and effective which is widely used in many fields, such as finance, communication, and social networking. Through identity authentication, it can be determined whether the user has access and use rights to certain resources [21]. The commonly used identity authentication methods mainly rely on the online digital certificate issuer to provide online identity proof, which requires the issuer to be online at all times, increasing the burden of the system; another typical way is that the user obtains the digital certificate in advance through the offline certificate authority (CA) and directly presents the digital certificate to the verifier when authentication is required. The whole process does not need the participation of CA [21].

The current standard of digital certificate is X.509 standard formulated by International Telecommunication Union (ITU-T) [27]. Under the X.509 standard, the user first generates a public-private key pair, sends the public key and other information to be authenticated to the CA, then CA issues a public key certificate for the user and maintains the public key and certificate in the database of CA. Certificates can be selectively revoked or renewed through the database. When verification is required, the user sends the certificate to the verifier, and the verifier can use the CA public key for verification. Under the X.509 digital certificate standard, functions such as data integrity, identity certainty, non-repudiation, and tamper resistance can be realized.

However, most identity authentication schemes do not consider the privacy protection of authentication, and users are easy to be exposed during authentication. Therefore, how to ensure the anonymity of identity authentication has become a hot issue of privacy protection [21]. Zero-knowledge succinct non-interactive argument of knowledge (ZK-SNARKs) and Camenisch–Lysyanskaya signature (CL-Signature) based zero-knowledge proof (ZKP) are representative schemes that provide strong anonymity in the process of identity authentication. ZK-SNARKs [28] can generate concise proofs that can be efficiently verified. CL-Signature [29] can verify the integrity of the verification information provided by the certifier without disclosing the original information. RA [28] et al. proposed verifiable anonymous identity management for human-centric security and privacy in IoT based on ZK-SNARKs. In order to realize the user's supervision, combined with anonymous authentication technology, zero-knowledge proof, and group signature, a supervised anonymous authentication scheme suitable for blockchain system is proposed [21]. Although the existing anonymous authentication schemes have been able to ensure the privacy and security of users, they do not take into account the autonomy of users to personal identity information.

## *2.2. Preparatory Knowledge*

### 2.2.1. Bilinear Pairing

The bilinear pairing was first used in cryptographic analysis, the reduction of discrete logarithm problems on elliptic curves. For example, the well-known Menezes–Okamoto-Vanstone (MOV) reduction based on Weil pairing and Frey-Ruck (FR) reduction based on Tate pairing reduce the discrete logarithm problem on the elliptic curve to the discrete logarithm problem on the corresponding finite field, which makes it easy to solve. In recent years, with the proposal of various identity-based encryption and signature schemes, the bilinear pairings have also been proved to be used to construct low-bandwidth and provably secure signature, encryption and key agreement schemes. The following is the mathematical definition of bilinear pairing.

Assume that $G_1, G_2,$ and $G_T$ are cyclic groups of order $p$; $Z_p$ is an integer group of order p; $g_1$ is the generator of $G_1$ and $g_2$ is the generator of $G_2$; and e is said to be a bilinear pair if there exists a computable mapping $e$: $G_1 \times G_2 \rightarrow G_T$ satisfying the following properties:

Bilinear: For $\forall \mu_1 \in G_1$, $\forall \mu_2 \in G_2$, $\forall a,\ b \in Z_p$, there is $e\left(\mu_1^a, \mu_2^b\right) = e(\mu_1, \mu_2)^{ab}$.

Non-degenerate: $e(g_1, g_2) \neq 1$, that is, $e(g_1, g_2)$ is generator of $G_T$.

Computability: For $\forall a,\ b \epsilon G_1$, there is an efficient algorithm to compute $e(a, b)$.

Generally speaking, when $G_1 \neq G_2$ is called $e$ asymmetric bilinear pair, and when $G_1 = G_2$ is called $e$ a symmetric bilinear pair.

### 2.2.2. Chameleon Hash

The chameleon hash function is a special anti-collision function. Each chameleon hash function can be considered to set a trapdoor. If you master the trapdoor, you can easily find collisions. Otherwise, it still meets the collision resistance.

The chameleon hash includes the following four algorithms:

***Setup***$(\boldsymbol{\lambda})$: Given a security parameter $\lambda$, output public key $pp$ of chameleon hash;

***KeyGen***$(\boldsymbol{pp})$: Enter the public parameters and output the corresponding public-private key pair $(pk,\ sk)$, where $pk$ is the public key, and $sk$ is the private key and trapdoor.

***Hash***$(\boldsymbol{pk},\ \boldsymbol{m},\ \boldsymbol{r})$: Enter public key $pk$, message $m$ and a random number $r$, the encrypted chameleon hash $ch$ can be obtained.

***Forge***$(\boldsymbol{pk},\ \boldsymbol{m},\ \boldsymbol{r},\ \boldsymbol{m'})$: Enter private key $sk$, message $m$, random $r$ and new message $m'$, output a new random number $r'$ and it can meet $ch = Hash(pk, m, r) = Hash(pk, m', r')$.

### 2.2.3. ECC

Neal Koblitz and Victor Miller introduced the concept of ECC in 1985, which can be used for digital signature, encryption, key exchange, and key negotiation schemes in blockchain-based IoT implementations. The main benefit of using ECC is to reduce the key size and thus increase the speed of key generation, signing, and verification. 256-bit ECC public keys and 3072-bit RSA public key ensures almost the same level of security [30]. The security of the algorithm is mainly based on the difficulty of the discrete logarithm problem on elliptic curves, and there is no polynomial-time algorithm to solve the discrete logarithm problem on elliptic curves.

## 3. System Model

We have proposed an integrated energy management platform based on blockchain. First, the blockchain provides verifiable public trust and offers trusted identity certificates of corresponding users for multiple different energy management systems. Secondly, the security in identity certificate's generating process is mainly guaranteed by EVAA. EVAA has the characteristics of CH and ECC, which ensures that the user will not disclose the user's own information but can only get the processed results when presenting the certificate or verifying the certificate, and realizes the strong anonymity of the user's information. At the same time, users only need to show their certificates when conducting transactions. In this section, we first introduce the overall operation process of the platform in detail, just as shown in the overall architecture diagram in Figure 1. Finally, the whole process of the proposed the scheme of EVAA is described in more detail.

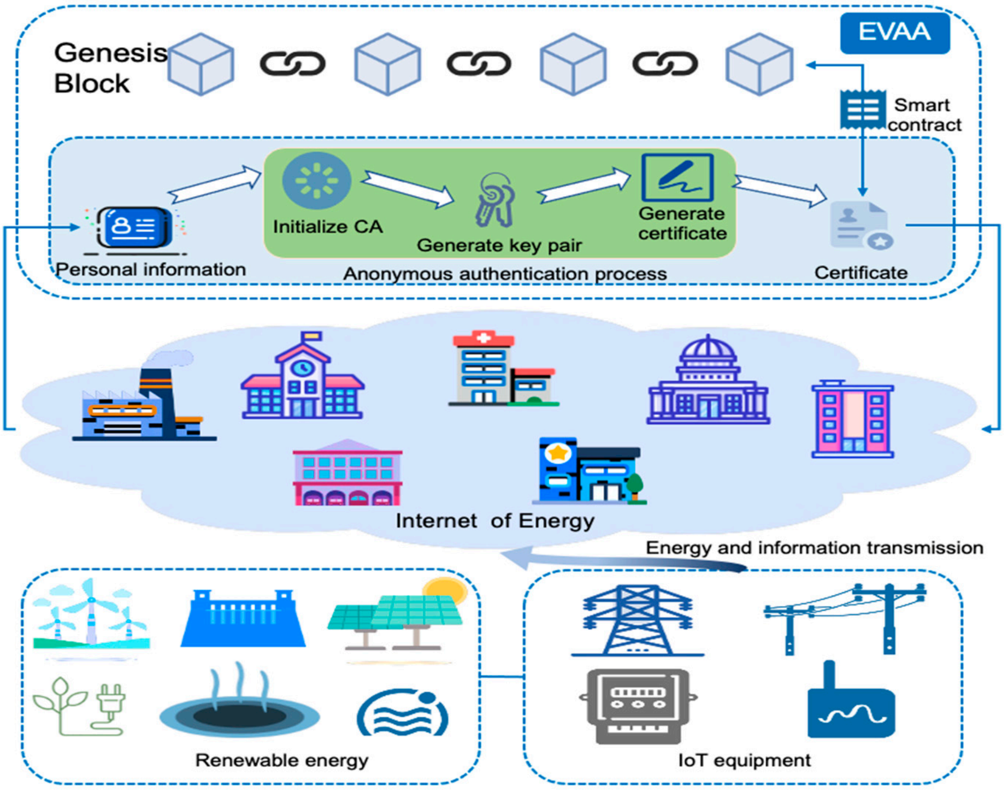


**Figure 1.** System architecture diagram.

### *3.1. Overall Architecture*

The framework of the blockchain-based integrated energy management platform proposed in this paper is shown in Figure 1, where users can collect the generated energy through IoT devices. At the same time, users can share, buy, sell, or transmit energy with each other. When a user has excess energy to sell or buy, the user can authenticate anonymously through the blockchain-based integrated energy management platform and generate proof of identity to be stored in the blockchain through smart contracts for storage. Since several different energy management systems are connected to the platform, users can use any of the systems connected to the platform to buy and sell energy through the generated identity the proof, allowing buyers and sellers to check each other's identity in the process of the transaction; in the process of identity checking, only the result of checking is returned, and no specific information is returned to ensure the safety of users' identity. Meanwhile, through the improved authentication technology based on the CH idea, a high degree of autonomy of user information is realized, and personal information can be legally modified without amending the identity proof on the chain. To avoid the problem of slow system operation caused by multiple authentication or modification in the blockchain, the verification process of generating identity proofs and revising personal information is placed off-chain for calculation, and only the generated identity proofs are consensus, verified, and stored on the chain.

### *3.2. Editable and Verifiable Anonymous Authentication Incorporating Blockchain on Internet of Energy (EVAA)*

The symbolic variables and meanings mainly involved in the scheme of this paper are shown in Table 1.

**Table 1.** Symbolic variables and meanings in this paper.

| Variable Symbol | Meanings |
|---|---|
| $pk$ | Hash public key |
| $pk_{ca}$ | $CA$ public key |
| $m$ | User information |
| $m'$ | User new information |
| $r_0$ | User-entered trapdoor |
| $r_2$ | Trapdoor from personal information library |
| $sk$ | Hash private key(trapdoor) |
| $sk_{ca}$ | $CA$ private key |
| $CH(m)$ | Encrypted hash value |
| $certification_0$ | User's identity proof |
| $certification_1$ | Certificate from certificate library |
| $proof$ | User-showed certificate |
| $certification_2$ | Certificate from blockchain |

The scheme of EVAA incorporating blockchain constructed in this paper combines the CH idea and ECC technology; the scheme model is mainly composed of the following parts: user, verifier, $CA$ center and blockchain. The program flow is shown in Figure 2:

User: The role of the user in the whole process is to provide personal information, which is processed by the platform to generate data for user identity authentication and store the data in the off-chain (information library) and the blockchain respectively.

Verifier: The staple function of the verifier is to verify the user's identity.

$CA$ center: This part is used in distributing key pairs, generating certificates, and verifying certificates.

Blockchain: In our scheme we mainly make use of the decentralized and tamper-proof characteristics of blockchain to store the generated identity certificate on the chain. Since different energy management systems are connected to the blockchain, the users can use the identity certificate in the blockchain to publish and execute transactions in each energy management system when they need to conduct energy transactions.

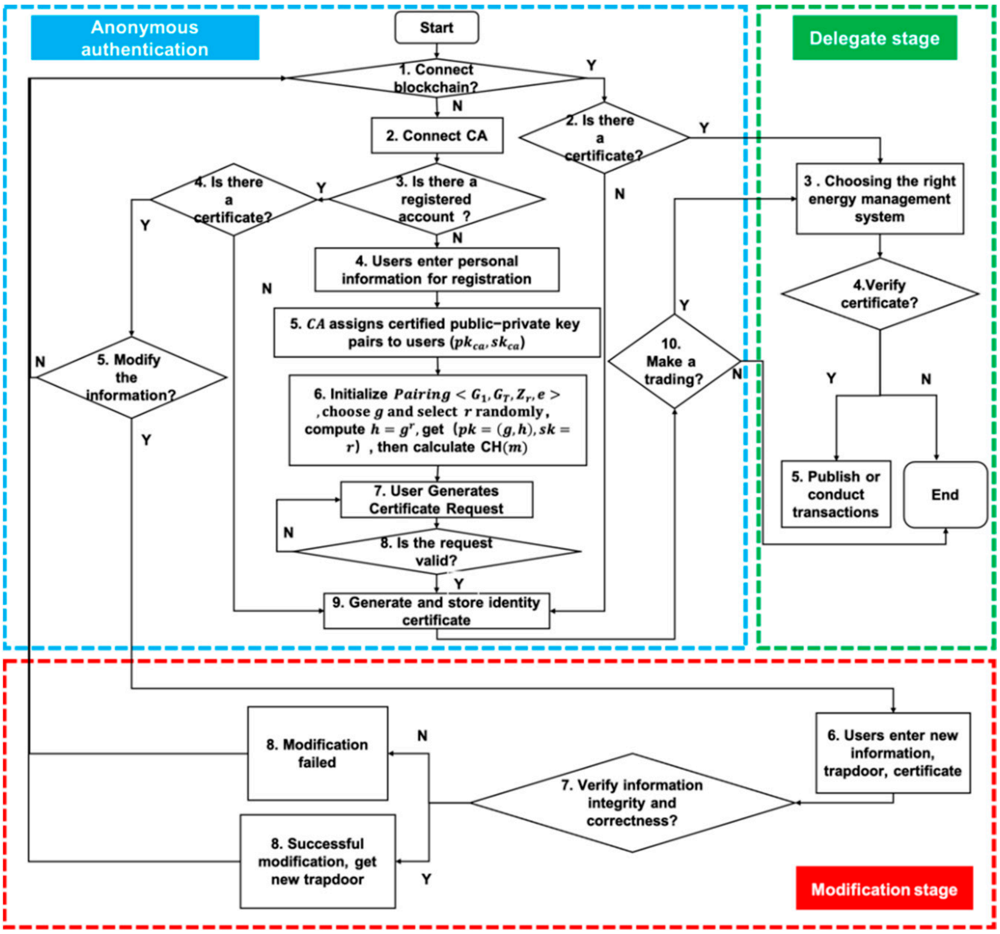

Anonymous authentication
Start
1. Connect blockchain?
N
Y
2. Connect CA
2. Is there a certificate?
Y
N
3. Is there a registered account ?
N
Y
4. Is there a certificate?
Y
N
4. Users enter personal information for registration
5. CA assigns certified public–private key pairs to users $(pk_{ca}, sk_{ca})$
6. Initialize $Pairing < G_1, G_T, Z_r, e >$ ,choose $g$ and select $r$ randomly, compute $h = g^r$, get $(pk = (g, h), sk = r)$ , then calculate CH($m$)
7. User Generates Certificate Request
N
8. Is the request valid?
Y
9. Generate and store identity certificate
5. Modify the information?
N
Y
10. Make a trading?
Y
N
Delegate stage
3 . Choosing the right energy management system
4.Verify certificate?
Y
N
5. Publish or conduct transactions
End
6. Users enter new information, trapdoor, certificate
7. Verify information integrity and correctness?
N
Y
8. Modification failed
8. Successful modification, get new trapdoor
Modification stage

**Figure 2.** Overall flow chart.

After the platform is established, firstly initialize and generate the $CA$ center. Then the user provides personal information $m$, and the system initializes the parameters $Paring\langle G_1, G_T, Z_r, e\rangle$ required to generate the CH signature, where $G_1$ and $G_T$ are the cyclic groups of order $p$, and $Z_r$ is the integer group of order $p$. The generating element $g$ of the $G_1$ group is selected, and $e$ is the corresponding bilinear pairing. Randomly select an exponent $r$, and calculate $h = g^r$, where $r$ is the user's private key $sk$ and trapdoor information, and the public key $pk = (g, h)$. It can be calculated that $CH(m) = ChameleonHash(pk, m, r)$. Then the $CH(m)$ is provided to the $CA$ center for authentication to obtain the identity certificate. The $CA$ center generates the authentication public and private keys for the user, encrypts the $CH(m)$ with its own public key $pk_{ca}$, and creates the user's digital certificate $certification$. When the user needs to modify the information due to the information update, the user's private key $sk$ and $certification$ must be displayed at the same time, and the information can be modified only after the verification of both is successful. When users need to authenticate, they can present their own $certification$. The verifier can verify the presented $certification$. If the verification is passed, the certificate is valid and the user identity authentication is successful; otherwise, the presented $certification$ is invalid; at this time, the verifier can send the certificate information to the $CA$ center for arbitration. After receiving the certificate information of the verifier, the $CA$ center can obtain the real identity of the user according to the multi-database information comparison and return the verification result to the verifier.

The scheme of EVAA incorporating blockchain in the Internet of Energy consists of the following processes:

Step 1: Establish a $CA$ center: The $CA$ center is generated by running the Equation (1), which is mainly used to distribute public-private key pairs, generate and verify digital certificates.

$$CA \leftarrow createCA() \tag{1}$$

Step 2: Initialize the generation curve equation and generate user key pairs: Input parameters $rBits$ , $qBits$, and then run the Equation (2) to generate the parameters of the Equation (3), where $G_1, G_T$ is the cyclic group of order $p$, and $Z_r$ is the integer group of order $p$, and $e$ is the corresponding bilinear pairing. Then select the generation element g of $G_1$ group, an index $r$ randomly on the integer group $Z_r$ to calculate $h = g^r$, where $r$ is the user's private key $sk$, also is trapdoor information, and public key is $pk = (g, h)$.

$$((pk,\ sk) \leftarrow E) \leftarrow Setup(rbits,\ qbits) \tag{2}$$

$$Pairing(G_1, G_T,\ Z_r,\ e) \tag{3}$$

Step 3: User registration: User inputs personal information $m$, then runs the Equation (4) in combination with $pk$ and $r$ generated in the previous step, and outputs $CH(m)$.

$$CH\ (m) \leftarrow ChameleonHash(pk,\ m,\ r) \tag{4}$$

Step 4: Storage parameters: The generated hash value $CH(m)$ is written to the blockchain through the smart contract; at the same time, the hash value $CH(m)$, public key $pk$, and curve parameter $g$ are written to the personal information library of the user outside the chain.

Step 5: Generate $CA$ issuance key: Run the Equation (5) and output the $CA$-assigned key pair $(pk_{ca}, sk_{ca})$, which is used to generate and verify the user digital certificate.

$$(pk_{ca}, sk_{ca}) \leftarrow getGenerateKey() \tag{5}$$

Step 6: Certificate request: Input the secret value $CH(m)$, combine it with the $pk$ generated by step 2, run the Equation (6) and generate the certificate request $certificationRequest$.

$$(certificationRequest) \leftarrow CR(pk,\ CH(m).toBytes()) \tag{6}$$

Step 7: Certificate request validation: Input certificate request $certificationRequest$, combined with $pk_{ca}$ and then run the Equation (7). If verification passed, set $result = 1$ and generate the certificate for the user.

$$(certificationRequest) \leftarrow CR(pk,\ CH(m).toBytes()) \tag{7}$$

Step 8: Generate certificate: Input secret value $CH(m)$,combine it with $pk_{ca}$ and run the Equation (8), generate $certification$ and send it to user for audit.

$$(certification) \leftarrow eccEncrypt(pk_{ca},\ CH(m).toBytes()) \tag{8}$$

Step 9: Store parameters: $CA$ retains and stores generated $(pk_{ca}, sk_{ca})$, and generated certificates are stored separately in the personal information library and certificate library.

Step 10: Information modification: Input new message $m'$, secret value $CH(m)$, private key of user $r$ and certificate $proof$. By getting $CH(m)$, $certification_2$ from the blockchain, getting $CH(m),\ r,\ certification_0$ values from the information library, comparing the values of $CH(m), r, certification$ obtained from multiple parties to see if they are consistent, if it is consistent then recovering $h$ through the curve parameter $g$,then to run the Equation (9) for get $CH(m')$ and $r'$. By judging whether $CH(m).equal(CH(m'))$ is true, if it is consistent, it will pass the verification and modify the data, and update the $r$ value in the personal information database to the new $r'$.

$$r',\ CH(m')) \leftarrow forge(m',\ CH(m),\ r,\ proof) \tag{9}$$

Step 11: Display certificate: Input user private key $r$,user information $m$, and $pk_{ca}$, then run the Equation (10) and output $proof$.

$$proof \leftarrow showCertification(r,\ m, pk_{ca}) \tag{10}$$

Step 12: Certificate verification: User present $proof$, $pk_{ca}$ and $CH(m)$, and then run $vertify(proof, pk_{ca}, CH(m))$ algorithm in the Equation (11). Compare with the certificate in the information library and certificate library, and at the same time find the corresponding $sk_{ca}$ according to $pk_{ca}$ and run $eccDecrypt(proof, sk_{ca})$ in the Equation (11) to compare the calculation result with $CH(m)$, if they are consistent then $result = 1$, indicating that the presented certificate is valid, and return the verification result; otherwise, the verification fails, showing that the certificate is invalid.

$$result \leftarrow vertify(proof, pk_{ca},\ CH(m))\&\&eccDecrypt(proof, sk_{ca}) \tag{11}$$

## 4. Experiments and Results Analysis

### 4.1. Security analysis of EVAA

To test the reliability and validity of the editable and verifiable anonymous authentication incorporating blockchain in the Internet of Energy, the following is a brief security proof of the authentication scheme in terms of both computational security and algorithm design.

#### 4.1.1. Proof of Computational Security

The CH is implemented by a bilinear mapping; the group $G_1$ generates the curve parameter $g$, the user public key $pk = (g, h)$, and the integer group $Zr$ generates the user trapdoor the $sk = r$; and the signature $CH(m)$ is generated using $pk$ and $sk$. The difficulty for an attacker to derive $r$ and $m$ using $CH(m)$ and $pk$ is equivalent to solving the discrete logarithm problems on an elliptic curve. Similarly, the difficulty of trying to derive $CH(m)$ from a digital certificate implemented by ECC is comparable to that of trying to derive $CH(m)$ from a certificate. Therefore, the security assumptions of the discrete logarithm puzzle and the ECC digital certificate guarantee the computational security of the scheme.

$$CH(m) = g^m \times h^r = eccDecrypt(certification, sk_{ca}) \tag{12}$$

#### 4.1.2. Proof of Algorithmic Security

In the scheme described in this paper, the modification right is always in the hands of the user himself, and the reasonable legality of the modification right needs to verify whether the $r_0$ input by the user is consistent with the value $r_2$ of the corresponding hash signature in the information library, and whether the certificate information $proof$ input by the user is consistent with the certificate $certification_2$ of the corresponding hash in the blockchain and that the $certification_1$ in the certificate base of $CA$ is consistent. If all the above information is consistent, the data can be modified. When the verifier disagrees with the digital certificate presented by the user, the digital certificate can be sent to $CA$ for verification. In the verified process when, and only when, the entered $proof$ is consistent with the $certification_2$ stored in the blockchain and $certification_1$ from the certificate library and the calculation result of $eccDecrypt(proof, sk_{ca})$ is the same as $CH(m)$, the verification is successful. The whole process of user's modification, verifying data by the verifier do not contain the original message $m$, which also ensures the privacy of the message $m$.

$$r = r_2 \tag{13}$$

$$\begin{cases} proof = certification_1 = certification_2 \\ CH(m) = eccDecrypt(proof, sk_{ca}) \end{cases} \tag{14}$$

#### 4.1.3. Proof of Anonymous Security

In the scheme of EVAA, the identities of all users in the energy Internet are encrypted when they communicate and transact with each other. Neither of the other users can confirm the true identities of the user because a secret private key only exists between the $CA$ and the user.

(1) Other users: During transactions between users, the identity of the other party will be verified. In the verification process, the results of $CA$ decryption will be compared with the relevant information queried in the blockchain. Only the verification results can be returned without disclosing any other information, thus ensuring the anonymity and authenticity of the user's identity.

(2) $CA$: $CA$ has strong physical properties and is not easy to be broken. $CA$ and users generate certificates by running the Equation (15). If the user's private key and real identity are not known, it is difficult to associate a user with the certificate.

$$eccEncrypt(pk_{ca}, CH(m).toBytes()) \tag{15}$$

(3) Blockchain: Blockchain is a distributed public ledger, and all its transactions are jointly supervised by all users. Unless the attacker has mastered 51% of the computing power, the blockchain is absolutely safe.

(4) User's public key: Due to the use of double encryption to generate certificates, it is almost impossible to obtain users' information by cracking a separate public key. This is because in the EVAA, the substantive problem of public key cracking is to solve the problem of discrete logarithm on two elliptic curves, which is a recognized mathematical problem that is almost impossible to solve.

### *4.2. Performance Analysis*

Aiming at the scheme proposed in this paper, this part analyzes and compares these with other propositions from the two aspects of function and efficiency. The blockchain system combined in this paper is the FISCO BCOS, into which we store identity information through smart contracts.

#### 4.2.1. Functional Analysis

Compared with the supervised anonymous authentication scheme [21], the scheme in this paper adds an editable function and improves the anonymity. When users edit information, they need to present both the relevant certificate and trapdoor for dual authentication, and information modification can only be done after the authentication is passed. Meanwhile, when verifying the validity of the certificate, the correctness of the user's anonymous identity information can also be verified. The scheme proposed in this paper can modify the user's personal information under the condition of ensuring the user's anonymity, but the user's identity can only be verified and cannot be traced back to the original information, which ensures the security of the user's private information.

#### 4.2.2. Efficiency Analysis

This paper improves the anonymity of user information and adds editable functions in the supervised anonymous authentication scheme. The following experiments compare the efficiency of the original scheme.

The experimental environment of this paper is mainly based on windows10 64-bit, Intel(R) Core(TM) i5-9400@2.90 GHz, and 16 G RAM and macOS Monterey Intel Core i5@2.7 GHz, and 8 G RAM. The blockchain platform FISCO BCOS involved in the experiment is deployed in the macOS environment. The development tool used in the development of FISCO-SDK is IDEA 2021, main development languages are Java and

Solidity, and main java toolkit used is JPBC (http://gas.dia.unisa.it/projects/jpbc, accessed on1 May 2022). The efficiency comparison is shown in the figure below.

Compared with the ZK-SNARKs [28] and CL signatures [29] mentioned in the existing VAIM scheme, the results given by this scheme are shown in Figure 3. ZK-SNARKs [28], CL signatures [29], and the CH signature verification time based on the proposed scheme will all increase with the increase of the number of users. However, it is more obvious that the signature time of ZK-SNARKs [28] and CL signatures [29] change the fastest when the number of users increases from 1 to 5, and increases slowly from 5 to 20. The signature verification time of the proposed scheme in this paper is relatively stable with the growth of the number of users. Compared with other schemes, the efficiency of the proposed scheme is higher and the signature verification time is shorter.

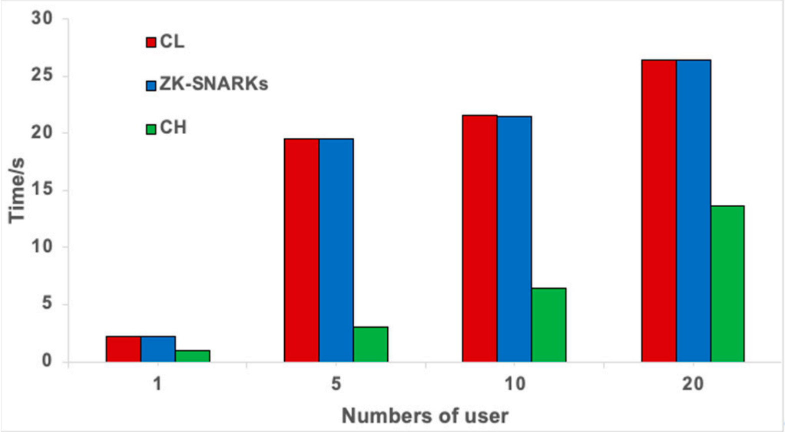
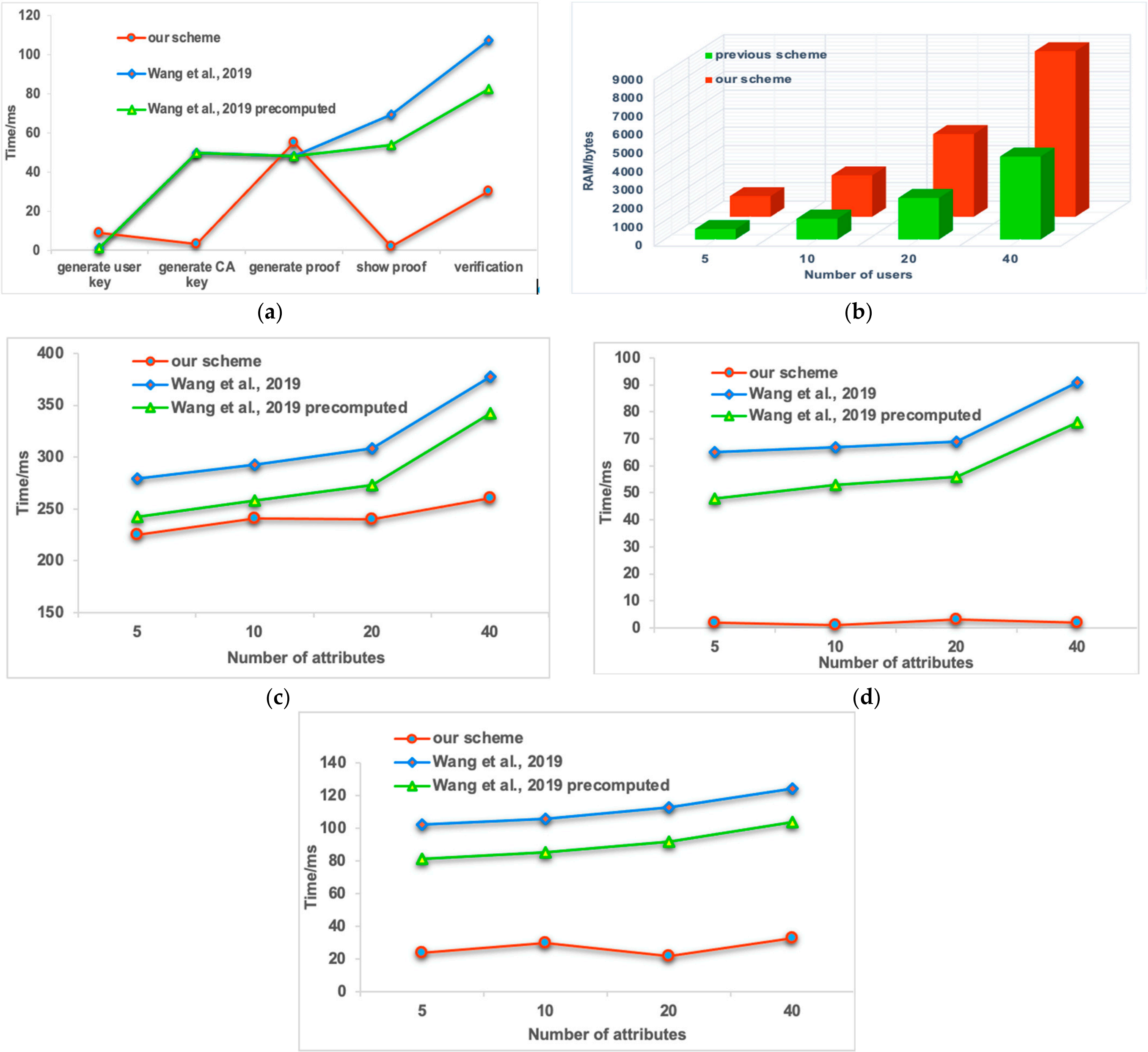


**Figure 3.** Comparison of signature verification time between CL, ZK-SNARKs, and CH.

Figure 4a shows the comparison of the computational efficiency of this scheme, the supervised anonymous authentication scheme [21] and its precomputing scheme at different stages. As can be seen from the figure, in the two stages of generating the user key and certificate, this scheme takes slightly longer than the other two schemes, but the time is relatively shorter in the stages of generating $CA$ key, presenting the certificate, and displaying the certificate. The main reason for this is that multiple curve parameters need to be generated in the stage of generating the user key; in the stage of generating $CA$ key, due to the short length of ECC key, the generation cost is low and the time is relatively short; in the certificate generation stage, the encryption speed of ECC is relatively slow; and in the certificate presentation and verification stage, the generated certificate is directly stored in the certificate library of the certificate center. When it is necessary to verify the user's certificate, the certificate in the certificate library, the corresponding certificate of the blockchain, and the certificate held by the user can be directly compared to verify the authenticity. On the whole, this scheme can ensure the improvement of efficiency while ensuring security, which has great advantages.

Figure 4b shows the comparison of certificate storage space under the different number of users. In addition to the certificate library provided by the certificate center, certificates are also stored in the blockchain. When certificates need to be presented, they can be obtained directly through the blockchain. When certificates need to be verified, the user identity can be determined directly through the comparison and verification of multi-party pre-stored certificates. That is, the strategy of space for time is adopted for certificates storage, which can be directly accessed when needed, eliminating the process of real-time calculation. Therefore, when presenting and verifying the certificate in Figure 4a, it takes the least time and has the highest efficiency compared with other schemes.



(**a**) (**b**)

(**c**) (**d**)

(**e**)

**Figure 4.** Analysis of scheme efficiency [21]. (**a**) Comparison of calculation efficiency; (**b**) comparison of certificate storage space; (**c**) multi attribute efficiency comparison; (**d**) efficiency comparison of certificate presentation; and (**e**) verify the efficiency of the certificate.

Figure 4c shows the comparison of the efficiency of this paper's scheme, the supervisory anonymous authentication scheme [21], and its precomputed scheme under different attributes. From the figure, it can be seen that both the supervisory anonymous authentication scheme [21] and its precomputed scheme gradually decrease in efficiency as the value of attributes increases. However, the efficiency of the proposed scheme is not related to the number of attribute values, and the efficiency of the proposed scheme varies slightly within a certain range regardless of the number of attribute values and does not have a significant impact; moreover, the efficiency of the proposed scheme is higher compared with the supervised anonymous authentication scheme [21] and its precomputed scheme.

Figure 4d,e, respectively, show the comparison of the efficiency of this scheme, supervised anonymous authentication scheme [21] and its precomputing scheme in presenting and verifying certificates under different attributes. From the figures, it can be seen that the time in both the supervisory anonymous authentication scheme [21] and its precomputation scheme decreases with the increase of attribute values, and the time to present and verify the certificate increases; however, in the scheme proposed in this paper, the efficiency in this paper is also not affected by the attribute values at this stage.

Figure 5 shows the performance analysis of certificates and their public key in storing on-chain by utilizing smart contract in this scheme. The above results are obtained by performing tests 1, 5, 10, and 20 times on different numbers of users N = 1, 5, 10, 20 and taking their average values. From the figure, we can see that when the number of users N is 1, 5, 10, and 20, respectively, the time of certificate and its public key storage fluctuates within a certain range, indicating that the time of storage on-chain is not much affected by the number of users. In the scheme proposed in this paper, we support multi-users authentication and unified certificate storage. When verification is required, the corresponding part can be queried separately without disclosing other information. While ensuring security, it also ensures the efficiency of storage.

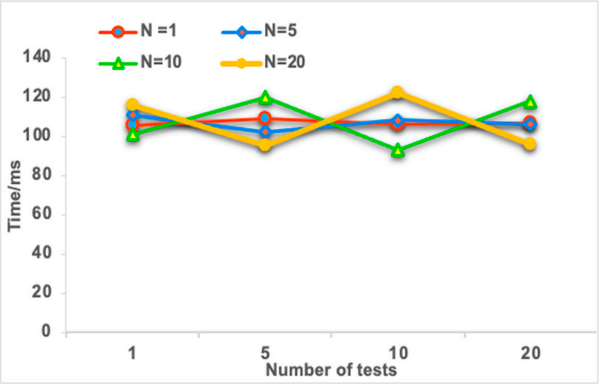


**Figure 5.** Analysis of on-chain certificate storage performance.

Figure 6 shows the performance analysis of the blockchain authentication certificate. The performance tests were conducted 1, 5, 10, and 20 times for different numbers of users N = 1, 5, 10, 20, respectively, and their average values were taken to derive the above results. From the figure, it can be seen that when the number of users N is 1, 5, 10, and 20, the time to obtain the corresponding certificate from the blockchain swings within a certain range and has small increasing trend, and the average time when the number of users N is 5 is shorter than the average time when the number of users N is 1, which indicates that the time to obtain the certificate from the blockchain is weakly affected by the number of users. At the same time, multiple users suffer from large network delays when acquiring evidence, resulting in unstable data. However, the impact of this situation is not much significant. Therefore, in the scheme proposed in this paper, the performance of obtaining certificates from the blockchain for authentication is stable and efficient.

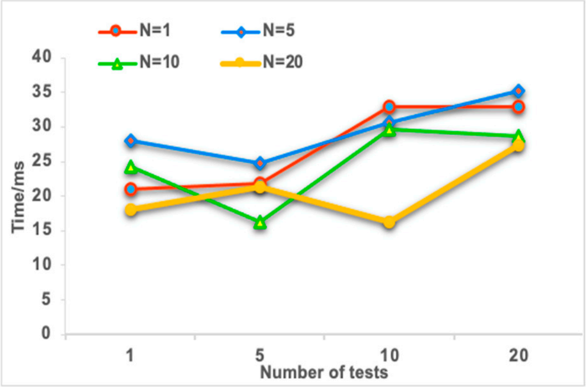


**Figure 6.** Analysis of verify certificate performance from blockchain.

## 5. Conclusions

The current continuous growth of renewable energy demand has led to a major challenge in distributed renewable energy management. To solve the current energy management dilemma, this paper proposes an editable and verifiable anonymous authentication scheme incorporating blockchain for renewable energy users in the Internet of Energy. Combined with the idea of the CH, ECC, and blockchain, the scheme introduces the editing function into the existing distributed energy management system so that users can modify and update their identity information without affecting the use of certificates. Anonymous authentication technology is used to protect users' identity privacy and complete identity authentication without disclosing their identity information; users can register at one time to meet the energy transactions of one or more systems, and blockchain technology is used to store certificates on the chain. When users need to conduct energy transactions, multi-party authentication is carried out through personal information, certificate information stored on the blockchain and in the certificate library. This scheme solves the problem that the current authentication technology cannot be edited. It aims to update the user's identity through editable technology, facilitate the user's high autonomy of their identity, reduce system redundancy, and improve the operation efficiency of the system. The proposal of this scheme will be beneficial to the security of users' privacy in the process of users' transactions in the energy Internet, and will be of great benefit to the development of the energy industry and the information technology industry in the future. In future studies, we plan to specifically analyze how to further improve the efficiency of the proposed scheme while ensuring security and consider the key security. This paper shows sufficient advantages in authentication and anonymous security. However, in order to improve the verification efficiency, some space efficiency needs to be sacrificed. In the future, while improving the verification efficiency, more consideration should be given to the utilization of storage space. In addition, a more feasible and secure solution is also needed for user key management.

**Author Contributions:** Conceptualization, Q.Z.; methodology, Q.Z.; software, Q.Z.; validation, Q.Z., Z.Y., A.X. and L.H.; formal analysis, Q.Z.; investigation, Q.Z.; resources, Q.Z.; data curation, Q.Z.; writing—original draft preparation, Q.Z.; writing—review and editing, Q.Z., F.B., Y.L. and T.S.; visualization, Q.Z.; supervision, F.B.; project administration, T.S. All authors have read and agreed to the published version of the manuscript.

**Funding:** The authors thank the Major Scientific and Technological Projects in Yunnan Province (no. 202002AB080001-8),Yunnan Key Laboratory of Blockchain Application Technology (funding no. 202105AG070005, and open project no.YNB202109 and no.YNB202115), the National Natural Science Foundation of China (No. 61971208), Yunnan Reserve Talents of Young and Middle-aged Academic and Technical Leaders (Shen Tao, 2019HB005), and Yunnan Young Top Talents of Ten Thousands Plan (Shen Tao, Zhu Yan, Yunren Social Development No. 2018 73), for their support.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Baig, M.J.A.; Igbal, M.T.; Jamil, M.; Khan, J. Iot and blockchain based peer to peer energy trading pilot platform. In Proceedings of the 2020 11th IEEE Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON), Vancouver, BC, Canada, 4–7 November 2020; IEEE: Piscataway, NJ, USA, 2020.
2. Zhang, Y.; Yu, R.; Xie, S.; Yao, W.; Xiao, Y.; Guizani, M. Home M2M networks: Architectures, standards, and QoS improvement. *IEEE Commun. Mag.* **2011**, *49*, 44–52. [CrossRef]
3. Maharjan, S.; Zhu, Q.; Zhang, Y.; Gjessing, S.; Basar, T. Dependable demand response management in the smart grid: A Stackelberg game approach. *IEEE Trans. Smart Grid* **2013**, *4*, 120–132. [CrossRef]
4. Pilz, M.; Al-Fagih, L. Recent advances in local energy trading in the smart grid based on game-theoretic approaches. *IEEE Trans. Smart Grid* **2017**, *10*, 1363–1371. [CrossRef]
5. Gregoratti, D.; Matamoros, J. Distributed energy trading: The multiple-microgrid case. *IEEE Trans. Ind. Electron.* **2014**, *62*, 2551–2559. [CrossRef]
6. Paudel, A.; Chaudhari, K.; Long, C.; Gooi, H.B. Peer-to-peer energy trading in a prosumer-based community microgrid: A game-theoretic model. *IEEE Trans. Ind. Electron.* **2018**, *66*, 6087–6097. [CrossRef]

7. Mandala, D.; Dai, F.; Du, X.; You, C. Load balance and energy efficient data gathering in wireless sensor networks. *Wirel. Commun. Mob. Comput.* **2008**, *8*, 645–659. [CrossRef]
8. Yang, W.; Guan, Z.; Wu, L.; Du, X.; Lv, Z.; Guizani, M. Autonomous and Privacy-preserving Energy Trading Based on Redactable Blockchain in Smart Grid. In Proceedings of the GLOBECOM 2020-2020 IEEE Global Communications Conference, Taipei, Taiwan, 7–11 December 2020; IEEE: Piscataway, NJ, USA, 2020.
9. Huang, X.; Zhang, Y.; Li, D.; Han, L. A Solution for Bi-layer Energy Trading Management in Microgrids Using Multi-Blockchain. *IEEE Internet Things J.* **2022**. [CrossRef]
10. Lu, X.; Guan, Z.; Zhou, X.; Du, X.; Wu, L.; Guizani, M. A secure and efficient renewable energy trading scheme based on blockchain in smart grid. In Proceedings of the 2019 IEEE 21st International Conference on High Performance Computing and Communications; IEEE 17th International Conference on Smart City; IEEE 5th International Conference on Data Science and Systems (HPCC/SmartCity/DSS), Zhangjiaje, China, 10–12 August 2019; IEEE: Piscataway, NJ, USA, 2019.
11. Abdella, J.; Tari, Z.; Anwar, A.; Mahmood, A.; Han, F. An architecture and performance evaluation of blockchain-based peer-to-peer energy trading. *IEEE Trans. Smart Grid* **2021**, *12*, 3364–3378. [CrossRef]
12. AlAshery, M.K.; Yi, Z.; Shi, D.; Lu, X.; Xu, C.; Wang, Z.; Qiao, W. A blockchain-enabled multi-settlement quasi-ideal peer-to-peer trading framework. *IEEE Trans. Smart Grid* **2020**, *12*, 885–896. [CrossRef]
13. Li, M.; Hu, D.; Lal, C.; Conti, M.; Zhang, Z. Blockchain-enabled secure energy trading with verifiable fairness in industrial Internet of Things. *IEEE Trans. Ind. Inform.* **2020**, *16*, 6564–6574. [CrossRef]
14. Aitzhan, Z.N.; Svetinovic, D. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Trans. Dependable Secur. Comput.* **2016**, *15*, 840–852. [CrossRef]
15. Li, Z.; Kang, J.; Yu, R.; Ye, D.; Deng, Q.; Zhang, Y. Consortium blockchain for secure energy trading in industrial internet of things. *IEEE Trans. Ind. Inform.* **2017**, *14*, 3690–3700. [CrossRef]
16. Jamil, F.; Iqbal, N.; Imran; Ahmad, S.; Kim, D. Peer-to-peer energy trading mechanism based on blockchain and machine learning for sustainable electrical power supply in smart grid. *IEEE Access* **2021**, *9*, 39193–39217. [CrossRef]
17. Zhao, Z.; Guo, J.; Luo, X.; Xue, J.; Lai, C.S.; Xu, Z.; Lai, L.L. Energy transaction for multi-microgrids and internal microgrid based on blockchain. *IEEE Access* **2020**, *8*, 144362–144372. [CrossRef]
18. Zhang, X.; Jiang, S.; Liu, Y.; Jiang, T.; Zhou, Y. Privacy-Preserving Scheme with Account-Mapping and Noise-Adding for Energy Trading Based on Consortium Blockchain. *IEEE Trans. Netw. Serv. Manag.* **2021**, *19*, 569–581. [CrossRef]
19. Gai, K.; Wu, Y.; Zhu, L.; Qiu, M.; Shen, M. Privacy-preserving energy trading using consortium blockchain in smart grid. *IEEE Trans. Ind. Inform.* **2019**, *15*, 3548–3558. [CrossRef]
20. Zhao, Y.; Zhao, J.; Kang, J.; Zhang, Z.; Niyato, D.; Shi, S.; Lam, K.-Y. A blockchain-based approach for saving and tracking differential-privacy cost. *IEEE Internet Things J.* **2021**, *8*, 8865–8882. [CrossRef]
21. Wang, Z.; Fan, J.; Cheng, L.; An, H.-Z.; Zheng, H.-B.; Niu, J.-X. Supervised Anonymous Authentication Scheme. *J. Softw.* **2019**, *30*, 1705–1720.
22. Ateniese, G.; Magri, B.; Venturi, D.; Andrade, E. Redactable blockchain–or–Rewriting history in bitcoin and friends. In Proceedings of the 2017 IEEE European Symposium on Security and Privacy (EuroS&P), Paris, France, 26–28 April 2017; IEEE: Piscataway, NJ, USA, 2017.
23. Krawczyk, M.H.; Rabin, T.D. Chameleon Hashing and Signatures. U.S. Patent 6108783A, 22 August 2000.
24. Huang, K.; Zhang, X.; Mu, Y.; Wang, X.; Yang, G.; Du, X.; Rezaeibagha, F.; Xia, Q.; Guizani, M. Building redactable consortium blockchain for industrial Internet-of-Things. *IEEE Trans. Ind. Inform.* **2019**, *15*, 3670–3679. [CrossRef]
25. Wei, J.; Zhu, Q.; Li, Q.; Nie, L.; Shen, Z.; Choo, K.R.; Yu, K. A Redactable Blockchain Framework for Secure Federated Learning in Industrial Internet-of-Things. *IEEE Internet Things J.* **2022**. [CrossRef]
26. Brown, J.; Du, X. Detection of selective forwarding attacks in heterogeneous sensor networks. In Proceedings of the 2008 IEEE International Conference on Communications, Beijing, China, 19–23 May 2008; IEEE: Piscataway, NJ, USA, 2008.
27. I'Anson, C.; Mitchell, C. Security defects in CCITT recommendation X. 509: The directory authentication framework. *ACM SIGCOMM Comput. Commun. Rev.* **1990**, *20*, 30–34. [CrossRef]
28. Ra, G.; Kim, T.; Lee, I. VAIM: Verifiable Anonymous Identity Management for Human-Centric Security and Privacy in the Internet of Things. *IEEE Access* **2021**, *9*, 75945–75960. [CrossRef]
29. Camenisch, J.; Lysyanskaya, A. A signature scheme with efficient protocols. In Proceedings of the International Conference on Security in Communication Networks, Amalfi, Italy, 11–13 September 2002; Springer: Berlin/Heidelberg, Germany, 2002.
30. Yadav, A.K. Significance of Elliptic Curve Cryptography in Blockchain IoT with Comparative Analysis of RSA Algorithm. In Proceedings of the 2021 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), Greater Noida, India, 19–20 February 2021; IEEE: Piscataway, NJ, USA, 2021.