Computers, Materials & Continua

Tech Science Press

DOI: 10.32604/cmc.2023.034668
Article

A Secure Energy Internet Scheme for IoV Based on Post-Quantum Blockchain

Jiansheng Zhang[1], Yang Xin[1,*], Yuyan Wang[2], Xiaohui Lei[2] and Yixian Yang[1]

[1]Information Security Center, State Key Laboratory of Networking and Switching Technology, Beijing University of Posts and Telecommunications, Beijing, 100876, China
[2]Beijing Everyone Crowdsourcing Technology Company Ltd., Beijing 100018, China
*Corresponding Author: Yang Xin. Email: yangxin@bupt.edu.cn
Received: 23 July 2022; Accepted: 26 October 2022

Abstract: With the increasing use of distributed electric vehicles (EV), energy management in the Internet of vehicles (IoV) has attracted more attention, especially demand response (DR) management to achieve efficient energy management in IoV. Therefore, it is a tendency to introduce distributed energy such as renewable energy into the existing supply system. For optimizing the energy internet (EI) for IoV, in this paper, we introduce blockchain into energy internet and propose a secure EI scheme for IoV based on post-quantum blockchain, which provides the new information services and an incentive cooperation mechanism for the current energy IoV system. Firstly, based on the principles of constructing a short lattice basis and preimage sampling, a lattice signature scheme is proposed and used in blockchain for authentication, which provides anti-quantum security. Secondly, we design the EI based on the post-quantum blockchain model. Lastly, based on this model, we design a secure EI scheme for IoV based on post-quantum blockchain. Through our analysis and experiment, this new scheme can increase the efficiency of energy utilization and enrich EI's application in IoV. In particular, we further illustrate and analyze its performance. It is shown that EI based on post-quantum blockchain is more secure and efficient in information communications and energy trading.

Keywords: EI; blockchain; IoV; information security; anti-quantum

1 Introduction

With the development of the economy and population growth, the energy demand has become increasingly urgent. However, traditional fossil energy consumption leads to the energy crisis and severe pollution. Consequently, some new green renewable energy sources have been used. And how to access and control these various types of intermittent energy is faced with new challenges. Namely, these energy sources require a better energy system as a support to make them be used more reasonably [1]. Therefore, the energy internet (EI) emerges as the times require.

EI is a new energy ecosystem which integrates information flow, energy flow and control flow. It can guarantee the energy use become more reliable, economical and convenient [2]. In addition, it

supports intelligent supply and energy sharing. Obviously, it also provides innovative concepts and envisions to enhance the capability of power grids [3], such as smart grids [4,5], distributed energy and microgrids [6,7].

Through network technology and intelligent management technology, a lot of distributed energy collection devices and various types of network nodes can be interconnected by the EI [8]. In other words, the EI implements a real-time information acquisition and control strategy. And multiple energy sources interact with each other to achieve energy sharing. Therefore, EI has a very positive effect on our environment and economy [9,10,11]. More importantly, the development of the energy internet is fundamentally changing the dependence on the traditional energy consumption model, which is a fundamental revolution of human social life. As Rifkin pointed out, combining the Internet with renewable energy, energy internet is a sign of the third industrial revolution [12]. At the same time, Because of the advantages of environmental protection and low cost, EV is regarded as an essential development direction of the automotive industry in the future, which has received significant attention from academics and industries. In addition, with the deployment of charging piles, IoV and EI are more closely related.

On the other side, with the development of distributed network technology and cryptography, Nakamoto designed a peer-to-peer electronic cash system and described the blockchain for the first time in 2008 [13]. Blockchain is a distributed data structure which is replicated and shared among members through a distributed network. Furthermore, blockchain 2.0 has been presented, which includes hyperledger and smart contract technology [14–16]. Smart contract technology provides blockchain with a built-in fledged Turing-complete programming language that can create contracts. In other words, by programming, these created contracts are used to encode arbitrary state transition functions, allowing users to create systems [17]. In addition, blockchain integrated the cryptographic algorithm, hash algorithm and distributed network technology together [18].

At present, blockchain has been widely concerned and researched, such as consensus mechanisms [19,20], smart contracts [21] and post-quantum blockchain [22]. However, blockchain is still mainly used in the financial field now. It has changed the traditional currency system, which needs to rely on a credit institution as the third party. And some cryptocurrencies are also designed using the blockchain, such as Bitcoin, Litecoin and Ether. Meanwhile, due to the transparency and security of information on the blockchain, we also find that its application is continuously expanded, such as voting [23], medical treatment and copyright protection [24]. In 2020, a novel peer-to-peer EMR data management and trading system called health chain was proposed based on consortium blockchain [25]. Aiming at the security threat of quantum computing attacks on blockchain technology, in 2021, a lattice-based blind signature for blockchain-enabled systems was proposed [26]. In 2022, Li proposed a secure keyword searchable attribute-based encryption scheme, which is efficient and more secure [27]. Similarly, we consider that blockchain technology can be introduced into the energy internet to promote the collaboration of the energy and participants. In this way, with the anonymity and security of blockchain technology, EI based on post-quantum blockchain can be more powerful and secure.

With the continuous development of EV, the application of IoV technology is gradually widespread, and the privacy leakage and security problems in IoV are becoming more serious. Additionally, as far as we know, the research on blockchain-based EI applied in IoV is still relatively less. In this paper, we design an incentive mechanism for energy production and information services, which is of forward-looking significance for the EI in IoV.

The remainder of this paper is organized as follows. In Section 2, we make a brief introduction to blockchain and EI. In Section 3, we summarize the common characteristics between blockchain

and EI. Afterward, EI based on the post-quantum blockchain model is designed. Its advantages are also analyzed and provided. In Section 4, we propose a secure EI scheme based on post-quantum blockchain for IoV. In Section 5, we further illustrate and analyze its performance. Some concluding remarks are presented in Section 6.

2 Preliminary

In this section, we start with the introduction of blockchain. Then, we describe the research status and development trend of EI. In addition, we further introduce some current applications of EI with blockchain.

2.1 Blockchain

Blockchain is a distributed super-ledger system that relies on the maintenance of all users, and the transactions can not be forged and altered intuitively. As shown in Fig. 1, each block has a hash value and references the hash of its previous block, respectively. Therefore, in this way, a link is established between these blocks, and it creates a blockchain.

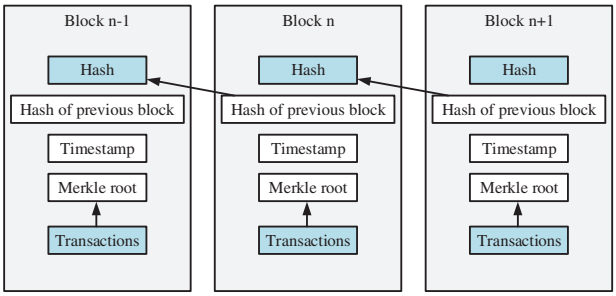

Figure 1: Organization structure of blockchain

Due to this design of chain structure and decentralization, the transactions are stored in a distributed ledger on the blockchain, and it has the advantages of transparency and traceability. At the same time, it also ensures that the date will not be tampered with or deleted. In particular, through the smart contract, some blockchain operations can be smart and automated [28,29]. We can use it to change the previous traditional model, which relies on third-party assistance and greatly facilitates the use of blockchain technology in practical applications.

2.2 Energy Internet

The notion of EI was presented in 2004. It transforms the traditional electricity grid into a smart and responsive digital network. Afterward, its application was widely concerned and studied. In 2008, a new energy system was built in Germany. Then, European Union constructed a new Internet for energy in 2011. And the global energy backbone grid was proposed during the 2018 Global Energy Interconnection Conference. As we see, this is a growing trend of global interconnection by EI now [30,31].

At present, some novel based-blockchain energy internet applications have been realized successively. The Energy company LO3 cooperated with ConsenSys to build an interactive grid platform based on blockchain. It is a community energy market that enables members to trade energy with each other [32]. The US company Filament set up the "Taps" detection devices on the grid nodes

and established corresponding communication mechanisms for these detection devices based on blockchain. Then, the government, grid company and users can share information [33,34]. It illustrates that the application research of energy internet based on blockchain is getting closer to our daily life.

3 EI Based on Post-Quantum Blockchain

By using sensing devices and actuators with vehicle ad-hoc networks and computing abilities, IoV provides interconnection and intelligence to the current intelligent transportation system. At the same time, with the anonymity and security of blockchain technology, blockchain is more intelligent and secure. In this section, firstly, we summarize and analyze five common characteristics of blockchain and the energy internet. Subsequently, based on analysis, we design an EI based on the post-quantum blockchain model.

3.1 Common Characteristics

Comparing them, we find that blockchain has five characteristics in common with the energy internet. These following common characteristics provide conditions and foundations for us to combine blockchain with EI.

(1) **Decentralized.** Decentralized is one of the most important features of blockchain. There is no centralized database and managers, and each node has equal rights that can jointly protect information on the blockchain. In addition, information is transmitted and verified by all nodes in the distributed network through the consensus mechanism. In EI, distributed energy is equally shared and used energy between individuals. Both blockchain and EI are self-management open frameworks.

(2) **Self-management.** The blockchain system is executed, maintained and managed by all nodes in the distributed network. And blockchain is a novel intelligent industrial ecosystem. In energy internet, energy is automatically coordinated and controlled with many protocols. Both blockchain and EI are self-management open frameworks.

(3) **Flexible.** By programming, these created contracts are used to encode arbitrary state transition functions in IoT. In addition, through this smart contract technology, blockchain can automatically trigger the executions of these contracts. Similarly, in the energy internet, many intelligent energy devices are used for energy transmission, utilization and storage. Thus, a series of smart contracts are adopted in the energy internet.

(4) **Industrial application.** Energy internet is mainly adopted in industry and plays a significant role in energy production and utilization. Besides, blockchain can be applied to industry, which ensures data security and reliability. Both the energy internet and blockchain make a positive contribution to modern industry applications.

(5) **Commercial.** All kinds of new energy can be regarded as commodities in EI. And energy commercialization is a typical feature of the energy internet. Through the power grid, energy is transmitted and traded to realize the mode of the energy market, so as to make full use of energy and improve its value. Likewise, by using blockchain technology, blockchain can provide a trading platform for the transactive applications. Both energy internet and blockchain have the value of commercial application.

3.2 Lattice Signature Cryptography Scheme

However, with the in-depth study of the quantum computer, the security of the Elliptic curve digital signature algorithm (ECDSA) is greatly threatened. Quantum computer has powerful parallel

computing capabilities, which can break the ECDSA and threaten the security of current blockchain. In 2008, Gentry et al. proposed a trapdoor design cryptosystem based on a preimage sampleable function.

Based on the principles of the short lattice basis generation [35] and preimage sampleable function [36], a lattice signature scheme is proposed. In this scheme, for the integers $q = ploy(n)$ and $m \geq 2n\log^2 q$, there is a $(\mathbf{A}, \mathbf{S})$ which can be obtained in the polynomial time. $\mathbf{A} \in Z_q^{m\times n}$ obeys the random uniform distribution and $\mathbf{S} \in Z^{m\times n}$ is a corresponding short lattice basis of $\mathbf{L}^{\perp}(\mathbf{A}) = \{x \in Z^m \,|x\mathbf{A} = 0 \bmod q\}$. And $\mathbf{SA} = 0 \bmod q$ and $\|\mathbf{S}\| = O\left(m^{0.5}\right)$ are also satisfied. Thus, $\mathbf{A}$ is the user's public key and $\mathbf{S}$ is the user's private key.

Suppose that Alice generates her own public key pk_a and private key sk_a according to the above method. Thus, the signing algorithm is shown as follows.

Algorithm 1: Signing algorithm

Input: Message M, Alice's pk_a and sk_a.
Output: Signature $(\mathbf{e}, M)$
Step 1: $t \leftarrow D = \{t \in R \,|\|t\| \geq 1/s\}$
Step 2: $\mathbf{u} \leftarrow SampleD(pk_a, s)$
Step 3: $\boldsymbol{\mu} = t\sum_{i=1}^{d}(-1)^{M[i]}\mathbf{C_i} + pk_a\mathbf{u}$
Step 4: $\mathbf{e}' \leftarrow SamplePre(pk_a, sk_a, \boldsymbol{\mu}, s)$
Step 5: $\mathbf{e} = t^{-1}(\mathbf{e}' - \mathbf{u})$

The verification algorithm is shown as follows.

Algorithm 2: Verification algorithm

Input: Message M, Alice's pk_a, integer m and the signature $\mathbf{e}$
Output: "Accept" or "Reject"
Step 1: $\|\mathbf{e}\| \leq 2s^2\sqrt{m} \wedge \mathbf{e} \neq \mathbf{0}$
Step 2: $pk_a\mathbf{e} = \sum_{i=1}^{d}(-1)^{M[i]}\mathbf{C}_i$

3.3 Security Proof

(1) **Correctness**

Theorem 1: This lattice signature scheme satisfies the correctness.

Proof: The signature $\mathbf{e} = t^{-1}(\mathbf{e}' - \mathbf{u})$ and $\|\mathbf{e}\| = \left\|t^{-1}(\mathbf{e}' - \mathbf{u})\right\|$. According to the preimage sampling trapdoor algorithm, we have $\|\mathbf{u}\| \leq s\sqrt{m}$ and $\|\mathbf{e}'\| \leq s\sqrt{m}$. Thus, $\|t\|^{-1} \leq s$, so we have $\|\mathbf{e}\| \leq \|t\|^{-1}(\|\mathbf{e}'\| + \|\mathbf{u}\|) \leq 2s^2\sqrt{m}$.

Due to the output $\mathbf{e}' \leftarrow SamplePre(pk_a, sk_a, \boldsymbol{\mu}, s)$ satisfies $pk_a\mathbf{e}' = \boldsymbol{\mu}$.

Thus, we can have $\boldsymbol{\mu} = t\sum_{i=1}^{d}(-1)^{M[i]}\mathbf{C}_i + pk_a\mathbf{u}$ and $pk_a\mathbf{e} = t^{-1}(\boldsymbol{\mu} - pk_a\mathbf{u})$. So

$$\begin{aligned} pk_a\mathbf{e} &= pk_a\left(t^{-1}\left(\mathbf{e}'-\mathbf{u}\right)\right) = t^{-1}\left(\boldsymbol{\mu}-pk_a\mathbf{u}\right) \\ &= t^{-1}\left(t\sum_{i=1}^{d}(-1)^{M[\mathrm{i}]}\mathbf{C}_i + pk_a\mathbf{u}\right) - t^{-1}pk_a\mathbf{u} \\ &= \sum_{i=1}^{d}(-1)^{M[\mathrm{i}]}\mathbf{C}_i. \end{aligned} \tag{1}$$

Through the above analysis, this lattice signature scheme satisfies the correctness, and Alice can not deny her signature.

(2) **Unforgeability**

Theorem 2: Based on the SIS assumption from lattice cryptography, our proposed scheme is unforgeable.

Proof: Suppose there is a probability polynomial, and the adversary wins the game with probability e. The goal is to build a random instance $\mathbf{B} \in Z_q^{m\times n}$ that challenges the SIS problem and outputs a nonzero vector $\mathbf{u}$ satisfying $\mathbf{Bu} = \mathbf{0} \bmod q$.

For the integers $q = ploy(n)$ and $m \geq 2n\log^2 q$, the challenger obtains a $(\mathbf{A}, \mathbf{S})$ in the polynomial time. $\mathbf{A} \in Z_q^{m\times n}$obeys the random uniform distribution and $\mathbf{S} \in Z^{m\times n}$is a corresponding short lattice basis of $\mathbf{L}^{\perp}(\mathbf{A}) = \{x \in Z^m | x\mathbf{A} = 0 \bmod q\}$. Thus, $\mathbf{A}$ is the user's public key, and $\mathbf{S}$ is the user's private key.

The adversary adaptively conducts polynomial queries. For the first inquiry, the adversary selects k files which are represented by $\mathbf{v}_1, \mathbf{v}_2, \cdots, \mathbf{v}_k$. Then the challenger performs the following steps:

1. Randomly select an identifier id_i from $\{0,1\}^n$.
2. Run signing algorithm to output $(\mathbf{e}', M)$.
3. Output the signature set and send it to the adversary.

It can be seen from the above simulation process that the output of the challenger is statistically indistinguishable from the output of this scheme. In our scheme, the public key is generated by the sampling algorithm TrapGen. It can be seen from TrapGen that the distribution of the public key pair is statistically indistinguishable in a simulation game from that in our scheme. In addition, since all signatures are obtained by executing the preimage sampling algorithm using the short basis of the lattice, the signature distribution of our scheme and the simulated game is statistically indistinguishable.

If the adversary outputs a valid forged signature $\mathbf{e}_1$ for the identifier id', the challenger can solve a random instance of the SIS problem. The opponent's solution process can be as follows:

For all inquiries, the id satisfies $id \neq id'$, the adversary has not inquired for any message from the identifier id. Because signature $\mathbf{e}_1$ is a valid signature, and $pk_a\mathbf{e}_1 = t^{-1}\left(\boldsymbol{\mu} - pk_a\mathbf{u}\right)$. Thus, we can have $pk_a\mathbf{e} - \sum_{i=1}^{d}(-1)^{M[\mathrm{i}]}\mathbf{C}_i = \mathbf{0}\mathrm{mod}q$.

According to the previous sampling algorithm TrapGen, this equation can not be established with an overwhelming probability. Adversary forges a valid signature of the message with negligible probability, and this scheme satisfies unforgeability under the lattice SIS assumption.

3.4 Scheme Model

In the new EI based on the post-quantum blockchain model, we introduce the above lattice signature cryptography scheme into the blockchain.

In the traditional blockchain, data security and reliability are guaranteed using cryptography algorithms, such as Hash 256 and ECDSA. Especially in ECDSA, the signature verification of this algorithm is used in the transaction system to ensure the correctness and reliability of the transaction. Unfortunately, under the attack of quantum computing, the ECDSA is no longer secure. This problem undoubtedly poses a fatal threat to blockchain technology. Different from the traditional blockchain, we use the above lattice signature scheme to generate the user's public key and private key. As mentioned above, the lattice signature scheme satisfies correctness. And Alice can not deny her signature. It can provide a security guarantee for the transactions and be applied to the blockchain. More importantly, compared with before, this new blockchain is more secure by using this lattice signature scheme.

Afterward, to improve the efficient utilization of energy and realize energy trading, we design the EI based on post-quantum blockchain, which is the integration of blockchain and EI system. As shown in Fig. 2, three energy modules are under the control of EI based on post-quantum blockchain. They are energy production, energy storage and energy usage.

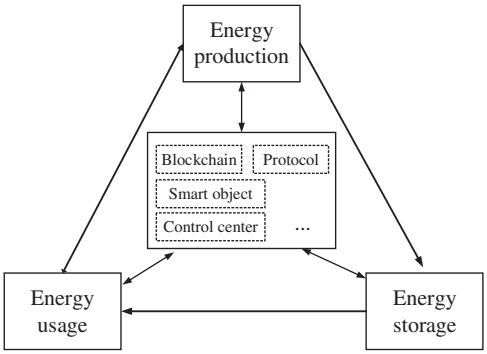

Figure 2: EI based on post-quantum blockchain model

In the core of EI based on the post-quantum blockchain model, there should be many modules, including blockchain, control center, a series of protocols, smart object, etc. They are in charge of dispatching and managing energy. At the same time, they need to fuse information and energy for energy sharing and trading, and smart objects are used to collect massive ambient data. These collected data are uploaded on the blockchain. In these modules, blockchain is beneficial and essential. It is like a distributed sharing database, and the stored data on the blockchain are secure. Namely, blockchain is very suitable for optimizing traditional application, which needs to rely on third-party authentication and guarantee. The information transmitted on the EI based on post-quantum blockchain can not be tampered with or deleted. Besides, we can quickly create contracts by programming. These contracts can be used to encode arbitrary state transition functions, which makes EI dispatch and control energy in time. In particular, EI based on post-quantum blockchain also can provide new information services and incentive mechanisms for energy production. More importantly, it can provide a good platform for energy coordination and trading in IoV. To sum up, EI based on post-quantum blockchain can increase the efficiency of energy utilization and enrich EI's application in IoV.

3.5 Advantages

In this subsection, the advantages of EI based on the post-quantum blockchain model are also analyzed and provided as follows.

(1) **Smart.** Smart contract technology provides blockchain with a built-in fledged Turing-complete programming language which can create contracts. In other words, by programming, these created contracts are used to encode arbitrary state transition functions. Through programming to create a contract, in this model, a smart contract can be triggered automatically to execute the command in time. It also makes it easier to expand its functions in the applications of EI based on post-quantum blockchain. Therefore, EI based on post-quantum blockchain becomes smarter and more powerful.

(2) **Secure.** Blockchain is like a distributed super-ledger system that relies on the maintenance of all nodes. Since this design of chain structure and decentralization, EI based on post-quantum blockchain provides a secure way for these nodes in the energy internet that record in a secure and verifiable manner. Therefore, blockchain is very safe and trusty with cryptography and the data can not be tampered with or deleted. Any change in the distributed data will be verified by these nodes. In particular, it has the advantages of transparency and traceability. More importantly, by introducing the lattice signature cryptography scheme in Subsection 3.2, the security of this model is greatly enhanced.

(3) **High efficiency.** The transformation from a centralized to distributed generation patterns naturally calls for robust, effective, and secure cyber infrastructures to support these complex communications interactions by using many distributed energy objects. The blockchain data can be distributed across the distributed network in minutes and will be processed at any time. Blockchain keeps a high efficiency in its applications.

(4) **Low cost.** Compared with traditional EI, blockchain does not need high infrastructure and maintenance costs associated with architecture. And it also does not require large server farms and networking equipment. Therefore, blockchain can reduce costs in EI.

(5) **Data integrity.** These data on the blockchain are distributed and stored in each device. Namely, every node in this distributed network has a copy of the same data. Therefore, even though some devices are broken, the data can still be stored completely. In particular, with the consensus mechanism, these data are also consistent and reliable. It shows that blockchain maintains a high degree of data integrity and consistency.

4 Post-quantum Blockchain-based EI applied in IoV

Combined with the EV charging network and IoV platform, we design a post-quantum blockchain-based EI scheme. This scheme mainly includes a data service system, blockchain-based IoV trading platform, renewable energy, charging station and EV as follows.

(1) **Data service system.** Value added based on data information can provide more innovative services, including capacity, the number of users and the frequency of the acquisition cycle. And data is transmitted and shared on this standardized IoV platform.

(2) **Blockchain-based IoV trading platform.** With the improvement of the power market, the technology and business model of interaction between various EVs and power grids are gradually maturing. Therefore, it can better realize the information and energy transmission between EV and EI. And this platform participates in centralized power trading and auxiliary services in the power market. In the era of mobile Internet, it provides users with fast information services and energy services, which increases user viscosity.

(3) **Renewable energy.** Energy mainly comes from renewable energy sources, including electric energy, wind energy and solar energy. Based on the adjustability of the EV charging load, it can absorb the electricity converted from the above green energy to charge the EV, which can promote the consumption of clean energy and reduce the power cost of the EV.

(4) **Charging station.** The charging station has the functions of energy storage and fast charging, which can meet the urgent and fast charging demand for EVs. At the same time, the intermittent high-power load of EV rapid charging can be stabilized through the energy storage system in this station, which can effectively reduce the impact of EV rapid charging on access to the local power grid. Besides, a charging station usually sets up multiple charging piles, which can meet the charging demand of multiple electric vehicles at the same time. More importantly, it can intelligently adjust the charging power and time. In this way, it can also optimize the configuration of charging resources and reasonably arrange the orderly charging of electric vehicles. Based on meeting the electric energy demand for EV users, the efficient interaction between EV and EI can be achieved through regulating orderly charging and discharging.

(5) **EV.** EVs can obtain online or offline services through the IoV trading platform, such as charging services and car rental services. At the same time, they can release the energy storage of electric vehicles and participate in auxiliary services to obtain corresponding benefits.

In this new scheme, we regard a unit of energy as an energy coin. Thus, each energy coin is defined as a cryptocurrency. Energy providers can be divided into power plants and personal energy producers (see Fig. 3), and the former is the main energy provider. Firstly, the energy storage center obtains new energy from the energy provider. Secondly, through the energy internet and blockchain trading center, a new transaction is established, and the system rewards him with corresponding energy coins. At last, transactions are stored in each node. On the contrary, if you want to consume energy, you can use energy coins to buy energy from others. Similarly, the users can also regard the energy coins as cryptocurrency to use in their daily life.

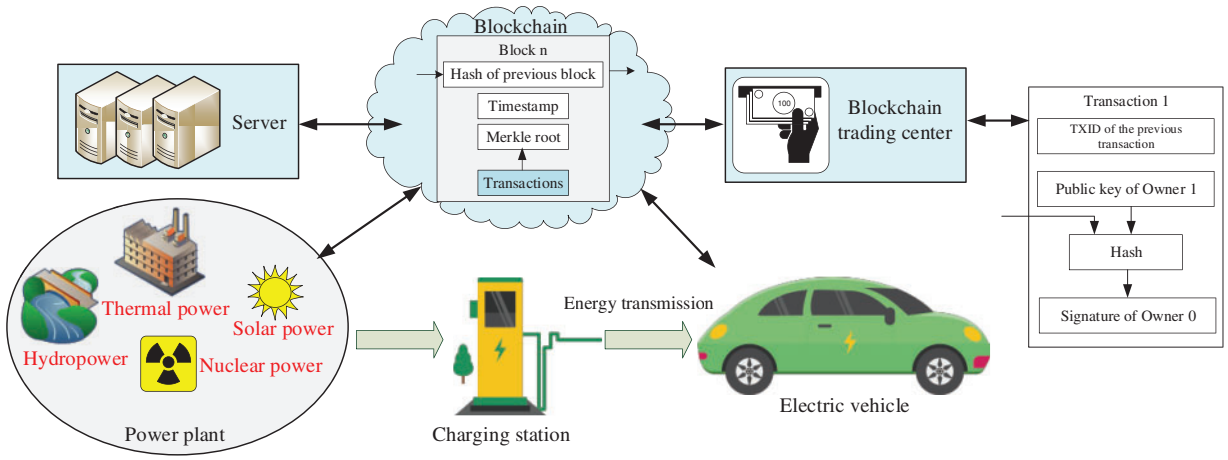

Figure 3: EI based on post-quantum blockchain

Generally speaking, EI aims at achieving coordination and comprehensive utilization of renewable energy, such as wind energy, hydropower and solar energy. By balancing the power supply of the energy Internet and the load of the charging station, this scheme can reduce the investment in power system expansion required to construct the charging station. At the same time, combined with energy storage, it can effectively reduce the impact of centralized charging of electric vehicles on the power grid. With the decline in power generation cost, the integrated storage and charging station can effectively reduce the power purchase cost of the charging station and improve the overall benefit of the EV charging station. As an energy trading platform, because its price is open and transparent, blockchain can encourage energy providers to bid with each other and sell to registered EV users at a preferential price.

5 Performance Comparison

In this scheme, the secret key and signature sizes are essential to its performance in practical application. Suppose that the parameters (n, m, q, σ) in our scheme corresponds to the parameters in other schemes. Compared with the same type of signature algorithms in [37–39], the results are shown in Table 1 below. To sum up, using the principles of constructing a short lattice basis and preimage sampling, the sizes of the public key, private key and signature in other schemes are larger than those in our signature scheme. In addition, the security of the signature algorithm in this paper depends on the lattice SIS problem. As is known to all, the lattice SIS problem in the average case can be reduced to the Shortest Independent Vector Problem (SIVP) in the worst case in polynomial time. It has been proved in [36] that it has the advantage of resisting quantum computation attacks. And according to the proofs in [35] and [36], under the assumption of lattice SIS problem, this proposed signature scheme satisfies unforgeability. Therefore, our scheme is more secure.

Table 1: Comparison with similar schemes

Scheme	Public key size	Private key size	Signature size
[37]	$mn\log q$	$m^2\log q$	$(dm/2 + m)\log(12\sigma)$
[38]	$nmlogq$	$nm(log2d) + n\ \log q$	$nm(\log 2d) + n\ \log q$
[39]	$2mn\log q$	$m^2\log 2q$	$mlog(12\sigma) + d(\log n + 1)$
Our work	$mn\log q$	$m^2\log q$	$m\log(12\sigma)$

Next, we will analyze the scheme's efficiency in this subsection from the perspective of the experiment, specifically comparing the number of elements in the public key and the number of integers in the signature. More concretely, the influences of the security parameter n on the public key and signature size in these schemes are considered. According to the actual requirements in these schemes, under reasonable parameters $d = \lceil \log n \rceil$, $q = 2^{10}$, $m = 6n\log q$, $\sigma = 2^{30}$, take the range of security parameter n to increase from 10 to 160. The public key size and private size of our proposed scheme and those in [37–39] are compared, respectively. As shown in Figs. 4 and 5, with security parameter n's increases, the public key size and signature size in our lattice-based scheme are significantly shorter than other schemes, which can improve the operation's efficiency in our proposed scheme.

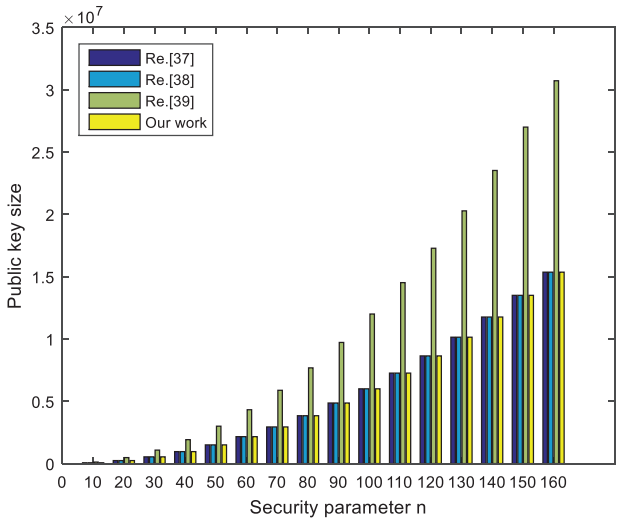

Figure 4: The public key size comparison

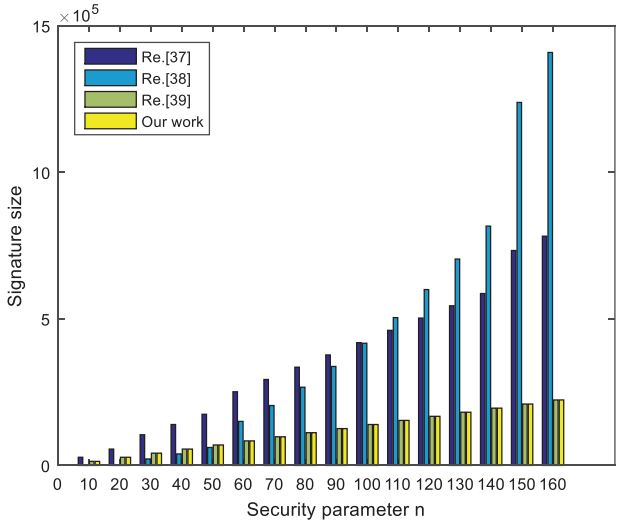

Figure 5: The signature size comparison

6 Conclusions

Our work provides a new reference for the research and application of EI based on blockchain. In this paper, we design a secure EI scheme based on post-quantum blockchain for IoV and analyze its performance. Through our analyses, it can improve renewable energy efficiency and achieve a coordinated supply of multiple energy sources. Furthermore, it can reduce some environmental problems caused by industrial pollution. More importantly, we propose a more efficient and secure signature scheme, which is introduced into the blockchain-based IoV trading platform. This new scheme can increase the efficiency of energy production and utilization, and we also further illustrate and analyze its performance. It is shown that EI based on post-quantum blockchain is more secure in information communications and energy trading.

Acknowledgement: The authors are grateful to the financial supports from the National Key R&D Program of China, Major Scientific and Technological Special Project of Guizhou Province, and the Foundation of Guizhou Provincial Key Laboratory of Public Big Data.

Funding Statement: This work is supported by National Key R&D Program of China (Grant No. 2020YFB1805403), Major Scientific and Technological Special Project of Guizhou Province (Grant No. 20183001), Foundation of Guizhou Provincial Key Laboratory of Public Big Data (Grant Nos. 2018BDKFJJ021, 2018BDKFJJ020, 2017BDKFJJ015, 2018BDKFJJ008), the Fundamental Research Funds for the Central Universities (CUC22GZ012), Beijing Municipal Natural Science Foundation (M22002, 4212019), National Natural Science Foundation of China (62172005).

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

References

[1] F. F. Wu, P. P. Varaiya and R. S. Hui, "Smart grids with intelligent periphery: An architecture for the energy internet," *Engineering*, vol. 1, no. 4, pp. 436–446, 2015.
[2] M. Gao, K. Wang and L. He, "Probabilistic model checking and scheduling implementation of an energy router system in energy internet for green cities," *IEEE Transactions on Industrial Informatics*, vol. 14, no. 4, pp. 1501–1510, 2018.
[3] X. Fang, S. Misra, G. Xue and D. Yang, "Smart grid—The new and improved power grid: A survey," *IEEE Communications Surveys & Tutorials*, vol. 14, no. 4, pp. 944–980, 2012.
[4] H. Farhangi, "The path of the smart grid," *IEEE Power and Energy Magazine*, vol. 8, no. 1, pp. 18–28, 2010.
[5] V. C. Gungor, B. Lu and G. P. Hancke, "Opportunities and challenges of wireless sensor networks in smart grid," *IEEE Transactions on Industrial Electronics*, vol. 57, no. 10, pp. 3557–3564, 2010.
[6] M. J. Davison, T. J. Summers and C. D. Townsend, "A review of the distributed generation landscape, key limitations of traditional microgrid concept & possible solution using an enhanced microgrid architecture," in *2017 IEEE Southern Power Electronics Conf. (SPEC)*, Puerto Varas, Chile, pp. 1–6, 2018.
[7] J. M. Guerrero, J. C. Vasquez, J. Matas, M. Castilla and L. G. Vicuna, "Control strategy for flexible microgrid based on parallel line-interactive ups systems," *IEEE Transactions on Industrial Electronics*, vol. 56, no. 3, pp. 726–736, 2009.
[8] A. Quelhas, E. Gil, J. D. McCalley and S. M. Ryan, "A multiperiod generalized network flow model of the US integrated energy system: Part I—model description," *IEEE Transactions on Power Systems*, vol. 22, no. 2, pp. 829–836, 2007.
[9] N. Bui, A. P. Castellani, P. Casari and M. Zorzi, "The internet of energy: A web-enabled smart grid system," *IEEE Network*, vol. 26, no. 4, pp. 39–45, 2012.
[10] S. Lanzisera, A. R. Weber, A. Liao, D. Pajak and A. K. Meier, "Communicating power supplies: Bringing the internet to the ubiquitous energy gateways of electronic devices," *IEEE Internet of Things Journal*, vol. 1, no. 2, pp. 153–160, 2014.
[11] R. Bolla, R. Bruschi, F. Davoli and F. Cucchietti, "Energy efficiency in the future internet: A survey of existing approaches and trends in energy-aware fixed network infrastructures," *IEEE Communications Surveys & Tutorials*, vol. 13, no. 2, pp. 223–244, 2011.
[12] J. Rifkin, "The third industrial revolution: How lateral power is transforming energy, the economy, and the world," *Survival*, vol. 2, no. 2, pp. 67–68, 2011.
[13] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," *Decentralized Business Review*, 2008. [Online]. Available: https://bitcoin.org/bitcoin.pdf
[14] P. Giungato, R. Rana, A. Tarabella and C. Tricase, "Current trends in sustainability of bitcoins and related blockchain technology," *Sustainability*, vol. 9, no. 12, pp. 2214, 2017.

[15] C. Decker and R. Wattenhofer, "Information propagation in the bitcoin network," in *IEEE P2P 2013 Proc.*, Trento, Italy, pp. 1–10, 2013.
[16] G. Zyskind and O. Nathan, "Decentralizing privacy: Using blockchain to protect personal data," in *IEEE Security and Privacy Workshops*, San Jose, CA, USA, pp. 180–184, 2015.
[17] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the Internet of Things," *IEEE Access*, vol. 4, pp. 2292–2303, 2016.
[18] I. Eyal, "Blockchain technology: Transforming libertarian cryptocurrency dreams to finance and banking realities," *Computer*, vol. 50, no. 9, pp. 38–49, 2017.
[19] D. Kraft, "Difficulty control for blockchain-based consensus systems," *Peer-to-Peer Networking and Applications*, vol. 9, no. 2, pp. 397–413, 2016.
[20] M. Milutinovic, W. He, H. Wu and M. Kanwal, "Proof of luck: An efficient blockchain consensus protocol," in *Proc. of the 1st Workshop on System Software for Trusted Execution*, New York, USA, pp. 1–6, 2016.
[21] A. Kosba, A. Miller, E. Shi, Z. Wen, C. Papamanthou *et al.,* "Hawk: The blockchain model of cryptography and privacy-preserving smart contracts," in *2016 IEEE Symp. on Security and Privacy*, San Jose, CA, USA, pp. 839–858, 2016.
[22] Y. Gao, X. Chen, Y. Sun, X. Niu and Y. Yang, "A secure cryptocurrency scheme based on post-quantum blockchain," *IEEE Access*, vol. 6, pp. 27205–27213, 2018.
[23] X. Yang, X. Yi, S. Nepal, A. Kelarev and F. Han, "Blockchain voting: Publicly verifiable online voting protocol without trusted tallying authorities," *Future Generation Computer Systems*, vol. 112, no. 2, pp. 859–874, 2020.
[24] Y. Gao, X. Chen, G. Xu, W. Liu, M. Dong *et al.,* "A new blockchain-based personal privacy protection scheme," *Multimedia Tools and Applications*, vol. 80, no. 20, pp. 30677–30690, 2021.
[25] C. Li, M. Dong, J. Li, G. Xu, X. Chen *et al.,* "Healthchain: Secure EMRs management and trading in distributed healthcare service system," *IEEE Internet of Things Journal*, vol. 8, no. 9, pp. 7192–7202, 2021.
[26] C. Li, Y. Tian, X. Chen and J. Li, "An efficient anti-quantum lattice-based blind signature for blockchain-enabled systems," *Information Sciences*, vol. 546, no. 2, pp. 253–264, 2021.
[27] C. Li, M. Dong, J. Li, G. Xu, X. Chen *et al.,* "Efficient medical big data management with keyword-searchable encryption in healthchain," *IEEE Systems Journal*, vol. 16, no. 4, pp. 5521–5532, 2022.
[28] A. Anjum, M. Sporny and A. Sill, "Blockchain standards for compliance and trust," *IEEE Cloud Computing*, vol. 4, no. 4, pp. 84–90, 2017.
[29] K. Gai, Y. Wu, L. Zhu, M. Qiu and M. Shen, "Privacy-preserving energy trading using consortium blockchain in smart grid," *IEEE Transactions on Industrial Informatics*, vol. 15, no. 6, pp. 3548–3558, 2019.
[30] K. Wang, J. Yu, Y. Yu, Y. Qian, D. Zeng *et al.,* "A survey on energy internet: Architecture approach and emerging technologies," *IEEE Systems Journal*, vol. 99, pp. 1–14, 2017.
[31] K. Zhou, S. Yang and Z. Shao, "Energy internet: The business perspective," *Applied Energy*, vol. 178, no. 23, pp. 212–222, 2016.
[32] C. Zhang, J. Wu, C. Long and M. Cheng, "Review of existing peer-to-peer energy trading projects," *Energy Procedia*, vol. 105, pp. 2563–2568, 2017.
[33] A. Tapscott and D. Tapscott, "How blockchain technology can reinvent the power grid," Fortune, Internet of Things, 2016. [Online]. Available: http://fortune.com/2016/05/15/blockchain-reinvents-power-grid/
[34] W. Gu, Z. Wu, R. Bo, W. Liu, G. Zhou *et al.,* "Modeling, planning and optimal energy management of combined cooling, heating and power microgrid: A review," *International Journal of Electrical Power & Energy Systems*, vol. 54, no. 1, pp. 26–37, 2014.
[35] J. Alwen and C. Peikert, "Generating shorter bases for hard random lattices," *Theory of Computing Systems*, vol. 48, no. 3, pp. 535–553, 2011.
[36] C. Gentry, C. Peikert and V. Vaikuntanathan, "Trapdoors for hard lattices and new cryptographic constructions," in *Proc. of the 40th Annual ACM Symp. on Theory of Computing*, Victoria, British Columbia, Canada, pp. 17–20, 2008.

[37] C. Y. Li, X. B. Chen, Y. L. Chen, Y. Y. Hou and J. Li, "A new lattice-based signature scheme in post-quantum blockchain network," *IEEE Access*, vol. 7, pp. 2026–2033, 2018.

[38] J. Chen, Y. Hu, H. Liang and W. Gao, "Novel efficient identity-based signature on lattices," *Frontiers of Information Technology and Electronic Engineering*, vol. 22, no. 2, pp. 244–250, 2021.

[39] L. Wang, C. Huang and H. Cheng, "Quantum attack-resistant signature scheme from lattice cryptography for WFH," in *IEEE 2nd Int. Conf. on Big Data, Artificial Intelligence and Internet of Things Engineering (ICBAIE)*, Nanchang, China, pp. 868–871, 2021.