applied sciences

Article

Proxy Signature-Based Management Model of Sharing Energy Storage in Blockchain Environment

Yiting Wang [1], Weiqiang Qiu [2,*], Ling Dong [1], Wei Zhou [1], You Pei [2], Li Yang [2], Heng Nian [2] and Zhenzhi Lin [2]

[1] State Grid Qinghai Electric Power Company, Xining 810001, China; wangyiting1436@163.com (Y.W.); dongling1436@163.com (L.D.); tempt520@163.com (W.Z.)

[2] College of Electrical Engineering, Zhejiang University, Hangzhou 310027, China; peiyou@zju.edu.cn (Y.P.); eeyangli@zju.edu.cn (L.Y.); nianheng@zju.edu.cn (H.N.); linzhenzhi@zju.edu.cn (Z.L.)

* Correspondence: qwqelectricity@zju.edu.cn

Received: 16 September 2020; Accepted: 23 October 2020; Published: 26 October 2020

Abstract: Sharing energy storage (SES) is a novel business model in order to increase the profits and improve the utilization rate of idle energy storage facilities. On the other hand, blockchains can be competently applied in the transaction and operation of SES because of distributed network architecture, traceability and tamper proof. In this paper, a management model of SES based on proxy signatures in the blockchain environment is proposed. Many management models including the principal-agent model are analyzed for SES in terms of benefit, cost, resources, and so on. Moreover, a blockchain framework and a typical transaction process of SES is presented. Finally, a proxy signature mechanism based on the ElGamal algorithm is proposed in order to address the problem that the signature power of nodes cannot be transferred on blockchains. Simulation results show that the proposed proxy signature mechanism can achieve the delegation of digital signature power under the premise of security and reliability, which is suitable for the management model of SES on blockchains.

Keywords: sharing energy storage (SES); blockchain; proxy signature; management model; principal-agent model

1. Introduction

With the increase in renewable energy sources (RESs) such as wind turbines and photovoltaic generation, massive amounts of clean energy are supplied to users all over the country, reducing carbon dioxide emissions and slowing down fossil energy consumption significantly [1]. However, the security and stability of power systems are worsening because of the intermittent, highly erratic and weather-dependent characteristics of RESs [2,3]. On the other hand, China has put forward rigid requirements for the consumption rate of RESs in each province in order to accelerate the energy transformation and stimulate the development of RESs' industry chain [4]. To address the above problems, energy storage systems are employed to provide a reliable solution [5,6]. By the end of 2019, the total installed capacity of China's energy storage projects reached 32.4GW, of which the installed capacity of electrochemical energy storage was 1706.9 MW, with a year-on-year increase of 59.4%.

Although the development of energy storage technology and related projects is extremely rapid, the return on investment in energy storage projects is not optimistic because of the smaller price difference of peak and valley electricity, the developing and incomplete electricity ancillary service market and the lower utilization rate. In this situation, sharing energy storage (SES) will be a novel business model in the energy storage field, improving the utilization rate of idle energy storage resources and making profits in a competitive market. In [7], based on a sharing economy, a new business model of battery energy storage systems is proposed. The study demonstrates that SES can bring additional profits for the owners of energy storage facilities and will attract investors. An investment decision model of SES is proposed in [8], which is a non-convex storage investment game admitting a unique Nash equilibrium. Cooperative game theory is applied in the modeling of participants (i.e., suppliers and demanders of energy storage resources), and the cooperative benefits in SES can be proved [9]. In [10], a concept of cloud energy storage (CES), where demanders can gain on-demand access to a sharing pool of grid-scale energy storage resources, is proposed. The energy storage facility of CES is large-scale and centrally controlled by the CES operator.

Although the feasibility and economy of SES have been verified, its further operation and promotion still have a few problems such as the lack of a sharing transaction platform, difficulties in information disclosure and sharing, and the high construction costs of the credit system. In past few years, blockchains have been applied in many fields including energy [11–13], transportation [14] and the Internet of Things (IoT) [15] due to the characteristics of decentralization, tamper proof and data traceability [11–16]. In [17], a large number of projects of blockchains in the energy sector are reviewed and summarized. For example, the Brooklyn Microgrid project set up a blockchain platform called Exergy, and the producers and consumers of clean energy could sell and purchase electricity on it [18]. Energo Labs, a Chinese startup company, utilizes blockchain solutions for community energy projects comprising prosumers, consumers, energy storage and smart grid devices to enable peer-to-peer (P2P) energy sharing [19]. In [20], a blockchain-based smart contract architecture for decentralized energy trading and management is presented, where a three-step peer-to-peer (P2P) energy trading mechanism adopts the double auction principle to enhance market vitality. In [21], an optimization model and blockchain-based architecture to manage the operation of crowdsourced energy systems with P2P energy trading transactions is proposed, allowing the system operator to manage the network users to seamlessly trade energy. In a localized consortium blockchain, a P2P electricity trading pricing model among prosumers with game theory is proposed, where the profit of sellers increases by 12.61% while the utility sacrifice of buyers decreases by 4.36% [22]. The P2P energy trading method based on blockchains is focused on the existing works and projects [17]. However, in order to reduce transaction and management costs, some small-scale owners may delegate a professional operator to trade their energy on the blockchain platform. Due to the lack of flexibility of the current blockchains [17], it is difficult to transfer the rights of nodes on the blockchain safely and reliably, and to be consistent with the off-line management model.

In a blockchain, the information security and ownership of nodes could be guaranteed by the digital signature mechanism based on asymmetric encryption [23,24]. The digital signature produced by a public-key system stands for the digital signature power of nodes on the blockchain, which could provide a proof of user identity and have the same legal effect as the traditional handwritten signature. The existing digital signature schemes (e.g., RSA [25], ElGamal [26] and elliptic curve cryptography (ECC) [27]) can be applied in blockchains. Besides, a special digital signature scheme, a proxy signature, is proposed in [28]. By the proxy signature, a node called the original signer can delegate the digital signature power to another node called the proxy signer, and then the proxy signer can issue information and sign contracts on behalf of the original signer.

The aim of this work is to select a management model for distributed SES resources in the blockchain environment and design a digital signature mechanism to make the digital signature power of nodes transfer flexibly on blockchains. The basic concept and characteristics of SES are described and several typical management models are analyzed in terms of benefit, cost, resources, and so on. Moreover, a blockchain framework and its transaction process of SES are presented. Furthermore, a proxy signature mechanism based on the ElGamal algorithm is designed for the SES blockchain considering the requirement of the principal-agent management model. The security, identification and distinguishability of the proxy signature mechanism will be analyzed and verified in the following sections.

2. SES and Its Management Model

2.1. Basic Concept and Characteristics of SES

SES is not a novel energy storage technology akin to superconducting the magnetic energy storage or Li-Ion batteries, but a business model based on a sharing economy for energy storage technology. Under this model, suppliers, owners of idle energy storage resources, could transfer the right to use the resources to demanders. The suppliers obtain the improved utilization rate of the idle resources and additional economic profits, and the demanders create greater value by using the energy storage resources. Consequently, total social welfare is improved.

There are three types of resources that can be shared as follows:

- Energy storage technologies and facilities: With the permission of policy and technology, the idle energy storage resources based on different kinds of technologies (mechanical storage, electrochemical storage or electrical storage) can all be shared and provide services to demanders.
- Energy storage application scenarios: According to the location and function of energy storage facilities, the application scenarios are classified into three types: power generation side, grid side and user side. The energy storage facilities in these scenarios can all be shared. For example, a wind farm can store electricity either in the SES facilities on the power generation side or the facilities on the user side, which depends on the cost of use. Moreover, the energy storage resources from different scenarios could be integrated as a whole to provide sharing services.
- Energy storage product form: Electric energy is the main product form for SES because energy storage facilities are shared to store or release electric energy. Otherwise, the service provided by energy storage is also a sharing product. For example, the peak regulation service of several RESs could be provided by an SES facility. Information is a by-product in the sharing process of energy storage resources.

A basic framework of SES is shown in Figure 1. It can be seen that the SES is made up of one or more energy storage facilities within a certain range. The electricity from centralized or distributed generation will be stored in SES facilities through the power network when wind and solar curtailment happens or power generation exceeds its planned output. Moreover, SES can also purchase electricity from power companies when electricity price is low. In the discharge mode, SES simultaneously releases the stored electricity to different users such as residential users, industrial users and power plants. For SES, the existing energy storage functions and profit models, such as peak–valley price arbitrage, smoothing generation curve and power auxiliary service, can be realized in a sharing way.

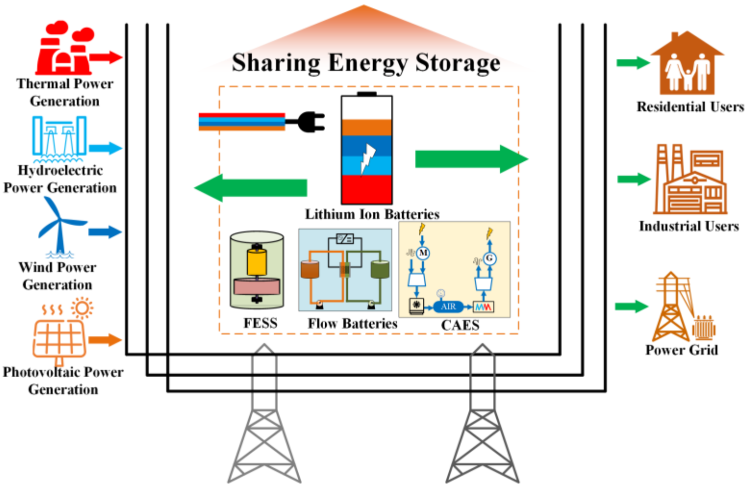

Figure 1. The basic framework of sharing energy storage (SES).

2.2. Management Model of SES

The essence of a sharing economy is the separation of ownership and use rights of goods, and temporary transfer of the use rights. Therefore, an SES market is necessary to provide a platform for matching, bidding and trading between supply and demand sides. Suppliers need to quantify and commercialize idle energy storage resources, which will be traded to demanders in the market. Demanders purchase the use rights of idle energy storage resources from the market and utilize the resources in real time or in a specified period of time. It is worth mentioning that the SES market can rely on the existing power market and its platform or build a special market where only the use rights of SES are traded.

All the owners of idle energy storage resources constitute the supply side of the SES market. According to the scale of resources, cost and management ability, the management model of SES can be classified into two categories: a self-operation model and principal-agent model.

- Self-operation model: In this model, the owners of idle energy storage resources directly participate in the market as an independent market entity. They are personally responsible for the market behaviors including bidding or pricing, credit behavior, signing and executing contracts, and so on. Moreover, the cost of labor and equipment, the obligations of market entities as well as the market risk are borne by the owners. Meanwhile, they will enjoy all the profits from the transactions of SES. Based on the above characteristics, this model is more suitable for the owners with large-scale energy storage facilities. Firstly, they possess sufficient technicians and information resources to maintain the competitiveness in the market. Moreover, the energy storage resources controlled by them can meet the market access conditions for energy storage according to the operating rules of the power market in China, which could obtain better profit prospects from it.
- Principal-agent model: In this model, the owners of energy storage resources delegate the agents to participate in the market on their behalf. The agents can exercise the rights of the principals in the market and complete the market behaviors. On the basis of the delegated scope, there are two types of principal-agent model—i.e., full delegation and partial delegation. The ownership of energy storage resources belongs to the owners, but the management rights, including operation, maintenance, personnel management and market transactions, are transferred to the agents in the full delegation relationship. In this paper, partial delegation only refers to the delegation of transaction rights to the agents. The full delegation model has been applied in some railway enterprises in China [29]; however, the partial delegation model is common in the financial field. On the other hand, the one-to-one model and many-to-one model are also two types of principal-agent model according to the number and relationship of principals and agents. The difference between these two models is that the resources controlled by an independent market entity from one owner or many owners.

For SES, the agents in the principal-agent model can be defined as sharing energy storage operators (SESOs). Compared with most of the owners, the advantages of SESOs include more professional and experienced market traders, superior information systems and more improved databases. Moreover, the small-scale idle energy storage resources can be aggregated by SESOs to meet the market access conditions. Through the agent of SESOs, the owners reduce expenditures on management, labor, equipment and transaction costs, and may obtain more profits from the market than independent operation. SESOs charge owners who delegate them a certain percentage of management fees. Based on the above characteristics, the principal-agent model is more suitable for the owners with small-scale energy storage facilities, as well as the owners who lack the experience and ability to trade in the market.

A flowchart for selecting the appropriate management model of SES is shown in Figure 2. The owners can select the right management model considering the energy storage scale, budget cost, profit expectation, management ability and market rules. As shown in Figure 2, firstly, the energy storage resources held by the owner are checked, and one or more target markets to participate in are chosen according to the scale and type of energy storage resources and the requirements of the owner. In addition, the budget cost and management capacity of human resources and facilities of the owner are evaluated to assist the decision-making of the management model. Moreover, the rules of energy storage facilities for the target markets are analyzed and the market access conditions for the given types of energy storage resources can be obtained. If the energy storage of the owner cannot meet the access conditions, the owner needs to participate in the markets jointly with other owners of small-scale energy storage resources under the aggregation of an SESO. The owner can delegate all the management rights to the SESO provided his budget cost and management capacity is insufficient—i.e., the many-to-one full delegation model is selected. Otherwise, the owner can select the many-to-one partial delegation model where only the transaction rights are delegated to the SESO. On the other hand, if the energy storage of the owner can meet the access conditions, the owner can participate in the markets as an independent market entity. Provided that the owner is a mature operator who has a sufficient budget, management capacity, market experience and information sources, the self-operation model is suitable for him due to the higher profit expectation. Otherwise, the one-to-one full delegation model and the one-to-one partial delegation model can be selected according to the evaluation of the above indexes for the owner.

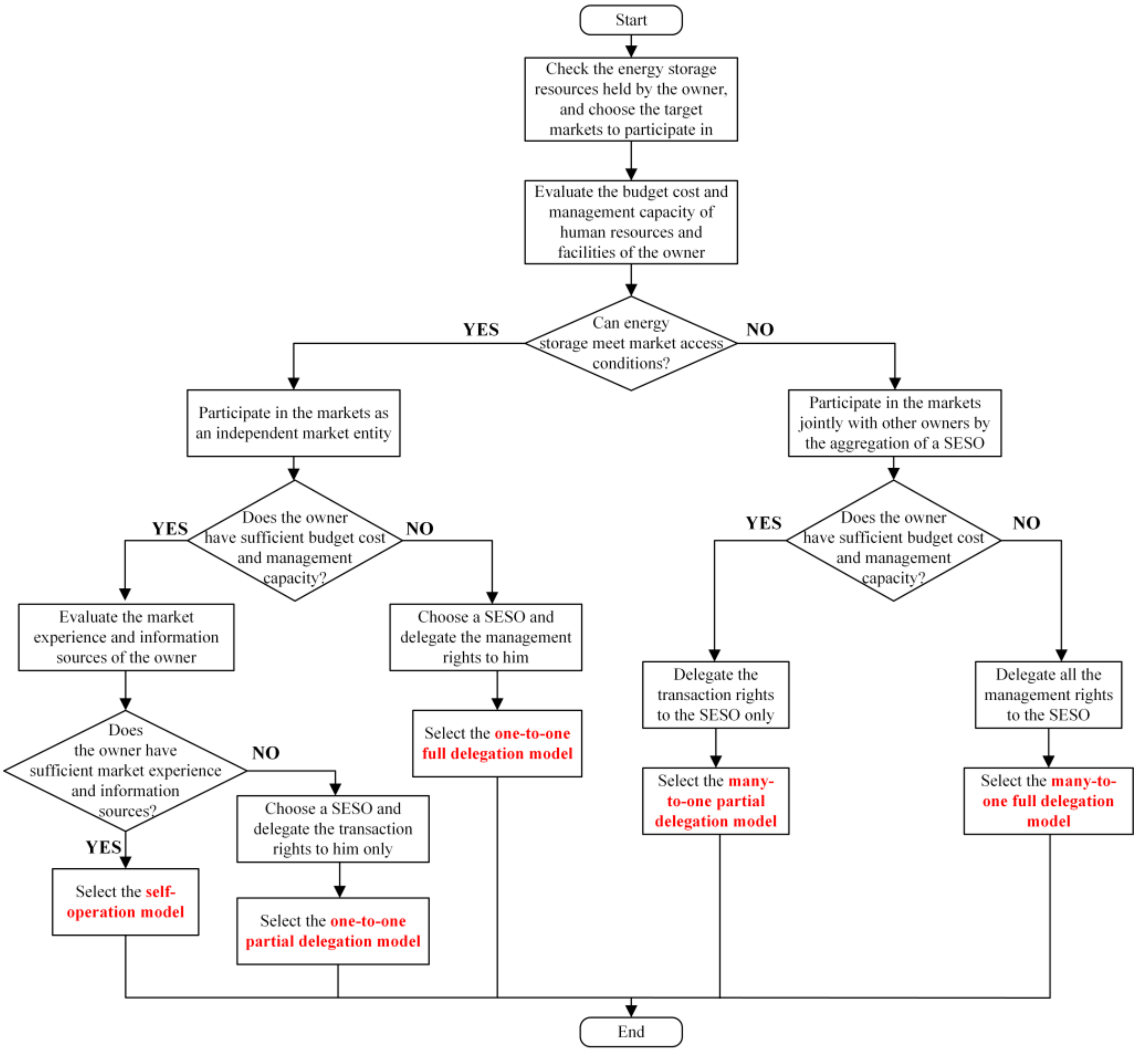
Start
Check the energy storage resources held by the owner, and choose the target markets to participate in
Evaluate the budget cost and management capacity of human resources and facilities of the owner
Can energy storage meet market access conditions?
YES
NO
Participate in the markets as an independent market entity
Participate in the markets jointly with other owners by the aggregation of a SESO
Does the owner have sufficient budget cost and management capacity?
YES
NO
Does the owner have sufficient budget cost and management capacity?
YES
NO
Evaluate the market experience and information sources of the owner
Choose a SESO and delegate the management rights to him
Delegate the transaction rights to the SESO only
Delegate all the management rights to the SESO
Does the owner have sufficient market experience and information sources?
NO
YES
Select the one-to-one full delegation model
Choose a SESO and delegate the transaction rights to him only
Select the many-to-one partial delegation model
Select the many-to-one full delegation model
Select the self-operation model
Select the one-to-one partial delegation model
End

Figure 2. The flowchart for selecting the appropriate management model of SES.

3. Blockchains and Authentication Technology

3.1. Blockchain Background

A blockchain is a decentralized and distributed database, which is maintained collectively by the nodes on the blockchain. A blockchain is a collection of many basic technologies, such as a blockchain data structure, distributed storage, consensus mechanism, cryptography and smart contracts. All affairs in a period of time are stored in a block, and these blocks are connected to a chain data structure in chronological order [14]. The hash of the previous block and Merkle root produced by cryptography, bytes version and time stamp constitute the header of the current block. The characteristics of tamper proof and traceability are determined by the blockchain data structure. Distributed storage means that the database is replicated and copied onto all the nodes of the blockchain, where the security and stability of the blockchain system is guaranteed even if a single point of failure occurs because of both technical failures and malicious attacks [14,17]. In addition, the nodes must reach an agreement on which the transactions and data are verified to guarantee that there will be no corrupt branches and divergences. Therefore, the uniformity of the distributed database is achieved by a consensus mechanism, providing a trustworthy system for decentralized nodes [15]. Asymmetric cryptography is the base of the encryption/decryption method and digital signature, bringing authentication, integrity and non-repudiation into blockchains [16]. Smart contracts are a kind of computer protocol which aims to spread, verify and execute contracts by means of information. With smart contracts, a contract can be automatically executed when the preset conditions are completed, reducing the transaction cost related to contracts [30].

3.2. Blockchain Framework of SES

As a novel information technology, blockchains are not a panacea that deal with all existing problems. The reason for applying blockchains in a scenario is that blockchains have more advantages and a lower cost in this scenario, compared with other technologies. Therefore, the compatibility between blockchains and SES is as follows.

First of all, the supply side and the demand side are, respectively, composed of energy storage resources and demanders with different locations, types and capacities. Therefore, SES is a distributed energy network, which is consistent with the distributed and decentralized characteristics of blockchains. In a blockchain, the participants of SES can act as a node to maintain the distributed database with other nodes. The distributed database is more fault-resistant and reliable than the centralized one, and every participant has a database backup locally.

Secondly, the demands of SES for fairness, equality and trust can be met by blockchains. According to organizational relation, the SES market is classified into two types: a center-dominated type and decentralized type. For example, the peak regulation market, where SES resources accommodate wind and solar power from different centralized power plants, is dominated by the power grid in China [31]. Under these circumstances, the power grid and other dominant institutions can issue a security statement by using blockchains. The security statement demonstrates that the market is fair and equal through the disclosure and sharing of key information on the blockchain. Although their power will be limited, the trust of the institutions from participants and regulators is improved. On the other hand, the SES market on the user side includes a large number of participants. The status and authority of these participants are equal, and therefore this market is decentralized. Blockchains realize the mutual balance and trust among the participants in a multiparty governance mode, even if the participants do not know each other or are even competitors.

Thirdly, the efficient, reliable and safe sharing process of energy storage can be achieved by blockchains. In a platform based on traditional information technologies, it is only a digital medium of the off-line trade. The signing, auditing and executing of contracts, a key step in transactions, still need tedious and time-consuming manual processing, which delays the time of completing a transaction and introduces many human factors that may affect fairness. However, smart contracts are utilized in blockchains to execute the procedure without human intervention. Moreover, blockchains can provide smart contracts with a reliable environment. The use of smart contracts improves the transaction efficiency and reduces the labor cost because the contracts execute automatically once the preset conditions are completed. Except for smart contracts, cryptography tools are another key element in the transaction process, protecting privacy while ensuring information can be verified.

A blockchain framework of SES is shown in Figure 3. It can be seen that the blockchain framework consists of a basis layer, core layer, service layer, user layer and cross-layer function. Moreover, a typical transaction process of SES is presented based on the user layer. The transaction process is composed of the following stages:

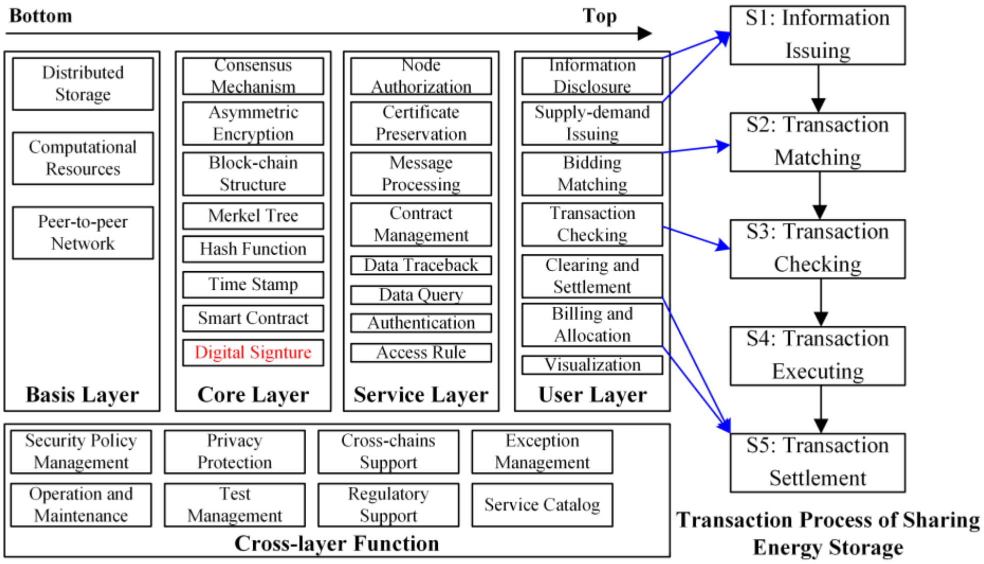

Figure 3. The blockchain framework of SES.

S1: Information issuing. In this stage, the participants issue the information about the SES transactions on blockchains. For example, suppliers or demanders can submit the number of the idle energy storage resources in the future and their price. Power grids can issue peak regulation information the next time to make participants understand the state of this market.

S2: Transaction matching. In this stage, the supplies and demands are matched based on the market rules and states. More factors, such as power loss, geographical location and facility performance, may be considered in the matching strategy compared to other types of power markets. The smart contract is applied in transaction matching to improve the matching efficiency and maintain the fairness of matching results. A matching result consists of the names of a supplier and a demander, the number and price of energy storage resources as well as the usage period.

S3: Transaction checking. In this stage, the matching results are submitted to the checking nodes which belong to a power dispatching organization or an exchange center. Security checking is completed by the nodes, which modify or cancel the matching results which violate line flow. The final matching results are recorded in electronic contracts. This stage can be integrated into the first two stages for a highly decentralized market.

S4: Transaction executing. In this stage, the transaction is executed by participants according to the matching results. The demanders remotely utilize the purchased energy storage resources within a prescribed period. Meanwhile, the suppliers provide the energy storage services that meet the demands. During execution, the power data of demanders and suppliers are submitted to the blockchain by smart meters, which is credible, tamper proof and traceable.

S5: Transaction settlement. In this stage, the transaction is settled in the light of the power data stored in the blockchain. The indicators for evaluating the service effect include the error between supply and demand curves, the average response time of the supplier for the instructions from demanders and the contract performance by participants. Finally, the settlement amount is computed and sent to participants by using smart contracts, representing the end of an SES transaction.

3.3. Digital Signature on Blockchains

On a blockchain, the off-line participants of SES are mapped as the nodes. Therefore, the operations of a node, such as information issuing, bidding, data querying and contract signing, have the same legal effect as that of the corresponding off-line participant in the market. In this case, it is crucial for a node to obtain the reliable on-line encrypted identity and authenticate the identity of the information received from other nodes. A digital signature is an important technology to identify information in the digital age and it is also applied in blockchains.

The basis of a digital signature is digital digest and asymmetric encryption. A message is transferred into a fixed length message digest by digital digest technology, and asymmetric encryption technology is used to encrypt the message digest. In fact, the digital digest technology is hash functions, transferring the information of any length into a fixed length message digest which is hard to restore to the original information. Due to the very low collision probability, it can be considered that the two pieces of original information should be the same if their message digests are the same. This feature can be used to compare the consistency of information. Therefore, information tampering is effectively prevented and the security is ensured.

Asymmetric encryption, also known as a two-key system, consists of a pair of keys—i.e., a public key and private key. A node has a private key firstly, and then a public key is generated by a function and the private key. The public key also includes the information of random variables except for the private key. Therefore, the private key cannot be obtained by cracking a public key though the public key is public to all. On the other hand, a pair of complementary algorithms is defined in the digital signature—i.e., encryption algorithm for the signature and decryption algorithm for verification. When one of the public or private keys is used to sign for the message digest by the encryption algorithm, the other one is used to verify the signed message by the decryption algorithm. In the process, the message that is not signed by the target node cannot be validated by the received node, and the integrity and reliability of the message can be confirmed.

According to the aforementioned principles, the basic characteristics of digital signatures are obtained easily. Firstly, the message cannot be modified after it has been signed. Secondly, all nodes receiving the message can confirm the signer's identity according to the digital signature because of the uniqueness and complementarity of the key pair. Thirdly, the signer cannot deny the message signed by him—i.e., the signature is undeniable. Finally, it is difficult for anyone else to forge the digital signature of the legal signer. In conclusion, digital signatures can replace the traditional handwritten signature and be sealed in the blockchain environment, representing recognition with a legal effect for messages. The key pair is the identity of nodes on blockchains.

4. Proxy Signature Method Based on ElGamal Algorithm

On a blockchain of the SES market, the participants orderly exercise their own rights through their digital signature. Unlike other participants, the rights of SESOs mainly come from the owners who delegate them, so SESOs need to use the corresponding digital signature to exercise the rights of an owner. However, the private key is the most important thing for nodes on blockchains because anyone who acquires the private key may abuse the rights of nodes. The private key is to the node as a password is to a bank account. Therefore, it is impossible for SESOs to directly utilize the digital signature of the node. In order to address the above problem, a proxy signature mechanism is proposed to achieve the delegation of digital signature power in a secure environment. By using a proxy signature mechanism, a node called the original signer can delegate its digital signature power to another node called the proxy signer. The proxy signer can generate the digital signature on behalf of the original signer—i.e., a proxy signature.

A basic protocol of proxy signatures is presented in [28], and the original signature scheme is kept unchanged. Therefore, a proxy signature mechanism based on the basic protocol and ElGamal algorithm is proposed in this paper, and its flowchart is shown in Figure 4. It can be seen that the proxy signature mechanism consists of the following four parts:

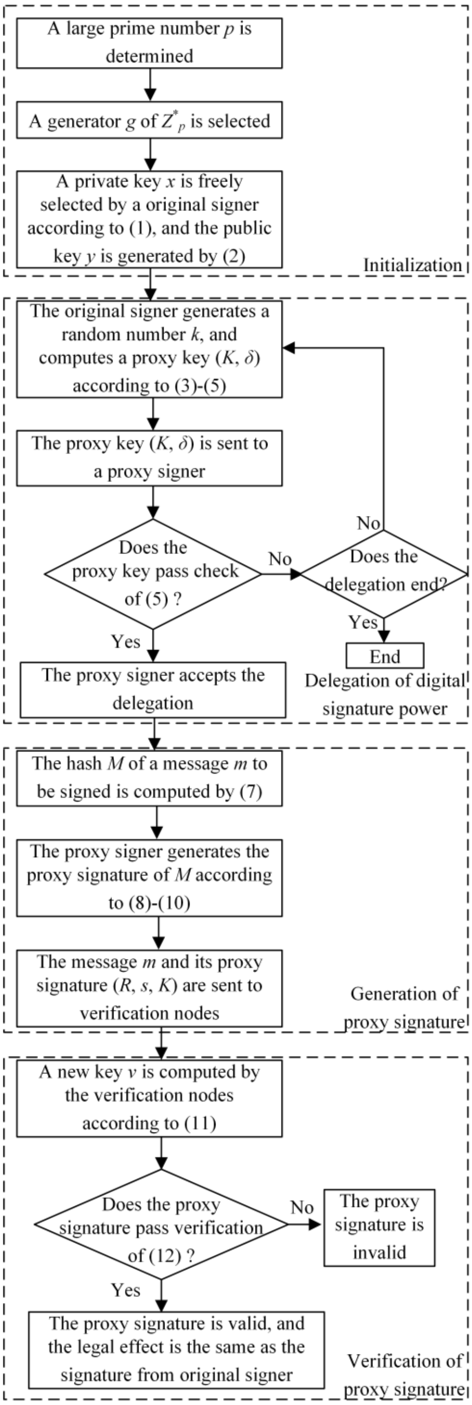
A large prime number p is determined
A generator g of Z^*_p is selected
A private key x is freely selected by a original signer according to (1), and the public key y is generated by (2)
Initialization
The original signer generates a random number k, and computes a proxy key (K, δ) according to (3)-(5)
The proxy key (K, δ) is sent to a proxy signer
Does the proxy key pass check of (5) ?
No
Does the delegation end?
No
Yes
End
Yes
The proxy signer accepts the delegation
Delegation of digital signature power
The hash M of a message m to be signed is computed by (7)
The proxy signer generates the proxy signature of M according to (8)-(10)
The message m and its proxy signature (R, s, K) are sent to verification nodes
Generation of proxy signature
A new key v is computed by the verification nodes according to (11)
Does the proxy signature pass verification of (12) ?
No
The proxy signature is invalid
Yes
The proxy signature is valid, and the legal effect is the same as the signature from original signer
Verification of proxy signature

Figure 4. The flowchart of the proxy signature mechanism.

1. Initialization. The parameters of the signature mechanism and the key pair of the node are determined in this stage.

The first parameter to be determined is p, a large prime number. The range of p can be selected by considering encryption bits. The ElGamal algorithm is based on the discrete logarithm problem over prime fields, which is not solved in polynomial time if p is a large enough prime number [32]. For example, if p is a prime number of 256 bits, the discrete logarithm based on the p needs more than 10^{19} operations to be solved by Pollard's rho algorithm, a recognized optimal algorithm, whose time complexity is $\mathrm{O}(p^{1/4})$, for computing discrete logarithms [33]. At present, the prime number p is 1024 bits or even 2048 bits in industrial applications, and therefore the solving time for the discrete logarithm is astronomical even if supercomputers are used.

The variable g less than p is a generator of Z_p^*. Z_p^* is a multiplicative group of integers modulo p and $Z_p^* = \{g \big| 1 \leq g \leq p-1, \gcd(g,p) = 1\}$, where gcd( ) is a function of computing the greatest common divisor between two numbers. For each b from 1 to p-1, there exist an a where $g^a \equiv b \ (\mathrm{mod}\ p)$. It is difficult for a large prime number to select generators. Therefore, a large safe prime p (p and $q= (p-1)/2$ are all the primes) is selected in order to obtain the generators easily because p-1 has only two factors—i.e., 2 and q. If $g^2(\mathrm{mod}\ p\big)$ and $g^q(\mathrm{mod}\ p)$ are not equal to 1, then g is a generator. p and g are the system parameters of the proxy signature mechanism.

Next, a private key x is freely selected as follows:

$$0 < x < p \quad x \in \mathbb{Z} \tag{1}$$

Then, the corresponding public key y can be obtained as follows:

$$y = g^x(\mathrm{mod}\ p) \tag{2}$$

The public key y, p and g constitute a group (y, p, g), which is public to all and used to verify that the owner of the public key has signed the message.

2. Delegation of digital signature power. In this stage, the digital signature power of the original signer is delegated to a proxy signer.

A random number k is generated by the original signer, and a proxy key is computed as follows:

$$0 < k < p \quad k \in \mathbb{Z} \tag{3}$$

$$K = g^k(\mathrm{mod}\ p\big) \tag{4}$$

$$\delta = x + \mathrm{kK}(\mathrm{mod}\ q) \tag{5}$$

where (K, δ) is the proxy key of the original signer. The original signer gives the proxy key (K, δ) to the proxy signer. Then, a congruence is checked by the proxy signer as follows:

$$g^\delta(\mathrm{mod}\ p) = yK^K(\mathrm{mod}\ p\big) \tag{6}$$

If (K, δ) passes the congruence equation, the proxy signer accepts it as a valid delegation. Otherwise, the proxy key is rejected, and a new proxy key generated by the original signer is sent to the proxy signer, or this protocol is stopped. Once the proxy signer accepts the delegation of original signer, the principal-agent relationship and K will be multicast to other nodes.

3. Generation of proxy signature. A proxy signature is generated by the proxy signer. The proxy signature represents the recognition of the original signer for the signed message.

Firstly, the hash of a message to be signed is computed by a specified hash function as follows:

$$M = H(m) \tag{7}$$

where m is the message to be signed; H denotes the hash function; M is the hash of m, and also the message digest. Moreover, a random number r is selected by the proxy signer, and the proxy signature for m is computed as follows:

$$0 < r < p \quad r \in \mathbb{Z} \tag{8}$$

$$R = g^r(\text{mod } p) \tag{9}$$

$$s = r^{-1}(M - \delta R)(\text{mod } p - 1) \tag{10}$$

where *R* and *s* are the part of the proxy signature, which constitute a complete proxy signature (*R*, *s*, *K*) with *K*. r^{-1} is the multiplicative inverse modulo of *r*, and it can be computed by an extended Euclidean algorithm. Finally, the proxy signature is sent to verification nodes with *m*.

4. Verification of proxy signature. The proxy signature is verified by the nodes which receive the message.

Once the nodes receive the message *m* and the proxy signature (*R*, *s*, *K*), a new key *v* corresponding to the proxy signature can be computed as follows:

$$v = yK^K(\text{mod } p\big) \tag{11}$$

The verification of the proxy signature is achieved by the following equation.

$$\text{Ver}(y,\ (R,\ s,\ K), m) = \begin{cases} \text{True} & g^{H(m)}(\text{mod } p) = v^R R^s(\text{mod } p\big) \\ \text{False} & g^{H(m)}(\text{mod } p\big) \neq v^R R^s(\text{mod } p\big) \end{cases} \tag{12}$$

where Ver(Public key, Digital signature, Message) is the verification function. When the received message and proxy signature can match with the public key of the original signer, the verification result is true. It means that the message is signed by the proxy signer on behalf of the original signer, and the message is not modified after signing. Otherwise, the verification is false, and the receivers do not admit the message.

Except for the basic characteristics of digital signatures, the proxy signature mechanism has some unique characteristics.

Unforgeability of proxy signatures: Except for the proxy signature, anyone including the original signer cannot generate valid proxy signature because of the confidentiality for *r*.

Distinguishability of proxy signatures: A proxy signature is different from an ordinary digital signature of the original signer because the proxy signature (*R*, *s*, *K*) adds *K*, a part of the proxy key, compared to the ordinary signature. In addition, the proxy signatures from several proxy signers are easy to be distinguished due to the difference of *K*.

Identifiability of proxy signer: An original signer can determine the identity of the corresponding proxy signer from a proxy signature according to *K*.

Private-key's dependence: The private key of the proxy signer is generated by the private key of the original signer, meaning that δ depends on *x*.

Cancelability of proxy key: An original signer can send a message signed by him to the other to declare the invalidation of *K* at any time, once the original signer wants to end the delegation and cancel the proxy signature.

5. Case Study

This section provides case studies to demonstrate the application of the proxy signature mechanism on blockchains under the principal-agent management model of SES. MATLAB is used to simulate the digital signature located in the core layer of the blockchain. Moreover, the hash of the sent message is produced by CaptfEncoder, a cross-platform network security toolkit. Some hash functions, including MD1, MD5-32, SHA-1, SHA-256 and SM3, can be selected in the toolkit. To compare and verify the effectiveness of the principal-agent management model based on the proposed proxy signature mechanism in the blockchain environment, two application scenarios, including the digital signature process and the consensus process on an SES market blockchain, are simulated in the following sections.

5.1. Digital Signature Process

A digital signature process on an SES market blockchain based on the proposed proxy signature mechanism is shown in Figure 5. In the process, there are three types of nodes: delegation nodes (i.e., owners of energy storage resources), proxy nodes (i.e., SESOs) and verification nodes (i.e., other nodes on the blockchain, including demanders, other suppliers, power grid and so on). A delegation node as an original signer delegates its digital signature power to a proxy node—i.e., a proxy signer. The proxy node signs a bidding message of SES, and sends the message and its proxy signature to verification nodes. The verification nodes verify the proxy signature, and accept the message if the proxy signature is valid.

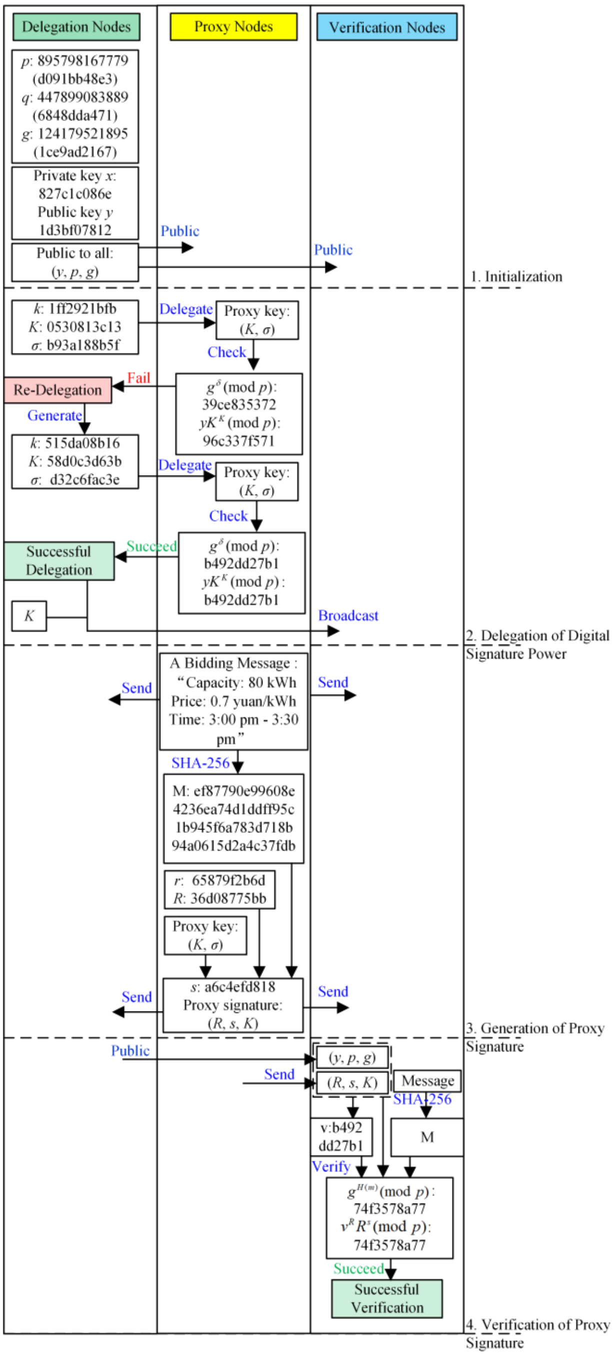
Delegation Nodes
Proxy Nodes
Verification Nodes
p: 895798167779 (d091bb48e3)
q: 447899083889 (6848dda471)
g: 124179521895 (1ce9ad2167)
Private key x: 827c1c086e
Public key y 1d3bf07812
Public to all: (y, p, g)
Public
Public
1. Initialization
k: 1ff2921bfb
K: 0530813c13
σ: b93a188b5f
Delegate
Proxy key: (K, σ)
Check
Fail
Re-Delegation
g^{δ} (mod p): 39ce835372
yK^{K} (mod p): 96c337f571
Generate
k: 515da08b16
K: 58d0c3d63b
σ: d32c6fac3e
Delegate
Proxy key: (K, σ)
Check
Successful Delegation
Succeed
g^{δ} (mod p): b492dd27b1
yK^{K} (mod p): b492dd27b1
K
Broadcast
2. Delegation of Digital Signature Power
A Bidding Message : “Capacity: 80 kWh Price: 0.7 yuan/kWh Time: 3:00 pm - 3:30 pm”
Send
Send
SHA-256
M: ef87790e99608e4236ea74d1ddff95c1b945f6a783d718b94a0615d2a4c37fdb
r: 65879f2b6d
R: 36d08775bb
Proxy key: (K, σ)
s: a6c4efd818
Proxy signature: (R, s, K)
Send
Send
3. Generation of Proxy Signature
Public
Send
(y, p, g)
(R, s, K)
Message
SHA-256
v:b492dd27b1
M
Verify
$g^{H(m)}$ (mod p): 74f3578a77
$v^{R}R^{s}$ (mod p): 74f3578a77
Succeed
Successful Verification
4. Verification of Proxy Signature

Figure 5. The digital signature process on an SES market blockchain based on the proposed proxy signature mechanism.

It can be seen from Figure 5 that a safe prime p of 40 bits is selected, and the encryption bits are determined. A generator g is selected according to the characteristics of the safe prime and the method described above. Then a private key x generates randomly, and then the public key y can be obtained based on the private key. For each node on the blockchain, the group (y, p, g) can be queried publicly.

In this case, there are two delegation processes between the delegation node and proxy node. In the first process, a random number k with a value of "1ff2921bfb" is generated, and then the proxy key (K, δ) is computed and sent to the proxy node. After receiving the proxy key, the proxy node queries the public key of the delegation node, and checks the received key through Equation (6). However, the check fails due to the unequal values of the equation, and therefore a message about this is answered by the delegation node. Presently, another random number k with a value of "515da08b16" is generated. Similarly, the proxy key is sent and checked successively. The new proxy key passes the check in the second process. Therefore, the proxy node accepts the delegation from the delegation node successfully. From the above analysis, it can be found that the delegation process of the proposed proxy signature mechanism has a certain probability of failure because of the value of k. However, it only has a modest impact on the whole process because the time of delegation process is negligible compared to the total agent time.

The proxy node will participate in the SES market and exercise the rights on behalf of the delegation node after accepting the delegation. In this case, the proxy node wants to sell the idle energy storage resources from 3:00 to 3:30 p.m. according to the scheduling of the delegation node. Therefore, a bidding message, whose contents are "Capacity: 80 kWh; Price: 0.7 yuan/kWh; Time: 3:00 p.m.–3:30 p.m.", will be signed and sent to other nodes. It is worth mentioning that the bidding price in the message is determined based on the experience and information of the proxy node—i.e., SESO. For the signing process, firstly, the hash of the message is obtained by a specified hash function (SHA-256 is used in this paper). Moreover, the proxy signature is generated based on a new random number, system parameters and the proxy key. Then, the message and its proxy signature are sent to other nodes including the delegation node.

The message is accepted only when the proxy signature is verified by the verification nodes successfully. In Figure 5, the verification nodes verify the proxy signature according to the received signature and the message from the proxy node, as well as the public information from the delegation node. The verification result shows that the message is signed by the proxy node on behalf of the delegation node and is not modified after signing. The bidding information from the accepted message will be matched in the next stage of the transaction process of SES.

In order to further represent the characteristics of the proposed proxy signature mechanism, another digital signature process on the SES market blockchain based on the traditional ElGamal digital signature mechanism is simulated as shown in Figure 6.

In this case, the owner still delegates his management rights or transaction rights to the SESO off-line. However, on the blockchain, the node of the owner needs to sign the message by his own private key personally. It can be seen from Figure 6 that the proxy node (i.e., SESO) sends the bidding message encrypted by the public key of the owner to the delegation node (i.e., the node of the owner) first. Then the message is decrypted by the private key of the delegation node, and the message is signed by the private key and sent to other nodes, if the delegation node is online and non-faulty. Otherwise, the above process will not be completed until the delegation node is online or recovered from the fault. The encryption/decryption process and the signature process of the ElGamal algorithm are presented in [32].

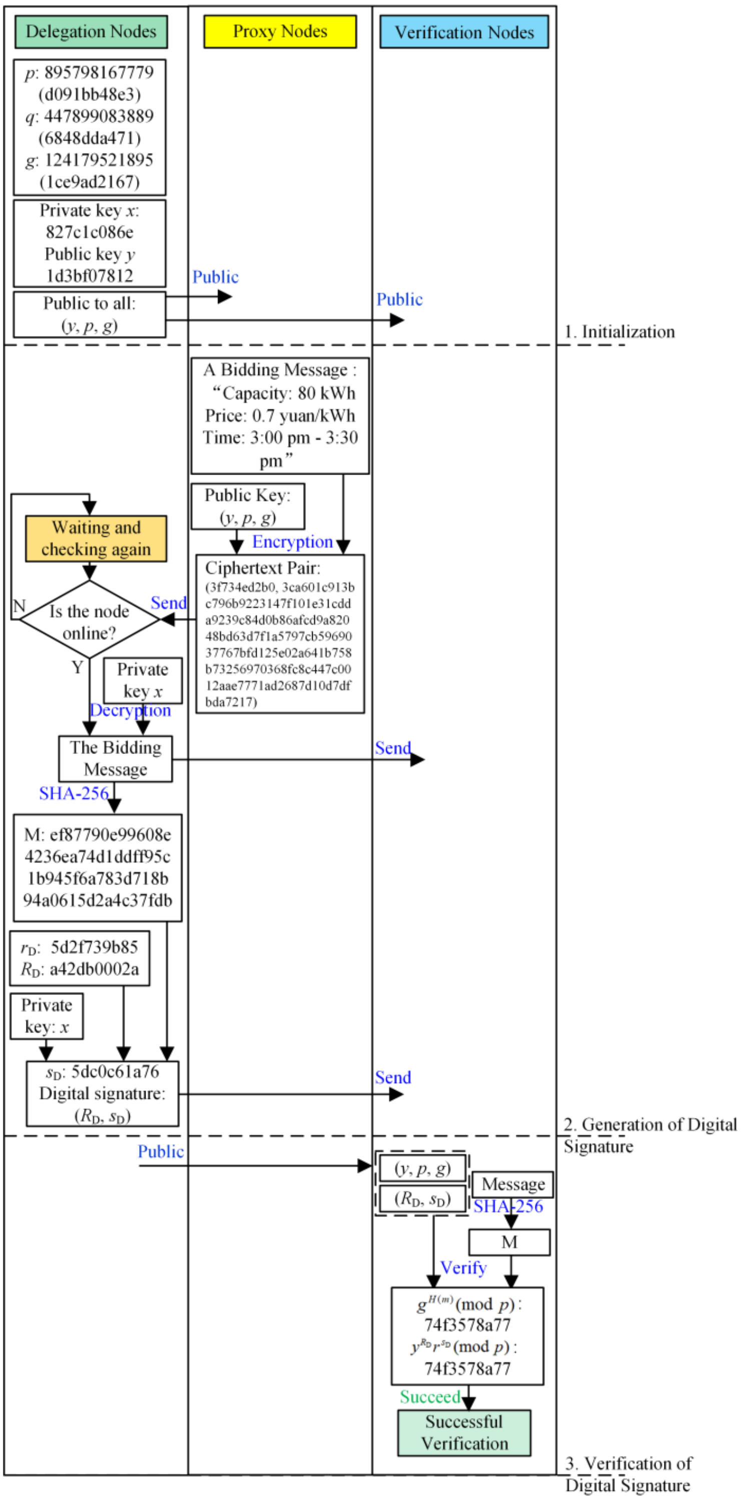
Delegation Nodes
Proxy Nodes
Verification Nodes
p: 895798167779 (d091bb48e3)
q: 447899083889 (6848dda471)
g: 124179521895 (1ce9ad2167)
Private key x: 827c1c086e
Public key y 1d3bf07812
Public to all: (y, p, g)
Public
Public
1. Initialization
A Bidding Message : "Capacity: 80 kWh Price: 0.7 yuan/kWh Time: 3:00 pm - 3:30 pm"
Public Key: (y, p, g)
Encryption
Ciphertext Pair: (3f734ed2b0, 3ca601c913b c796b9223147f101e31cdd a9239c84d0b86afcd9a820 48bd63d7f1a5797cb59690 37767bfd125e02a641b758 b73256970368fc8c447c00 12aae7771ad2687d10d7df bda7217)
Waiting and checking again
Send
N
Is the node online?
Y
Private key x
Decryption
The Bidding Message
Send
SHA-256
M: ef87790e99608e 4236ea74d1ddff95c 1b945f6a783d718b 94a0615d2a4c37fdb
r_D: 5d2f739b85
R_D: a42db0002a
Private key: x
s_D: 5dc0c61a76 Digital signature: (R_D, s_D)
Send
2. Generation of Digital Signature
Public
(y, p, g)
(R_D, s_D)
Message
SHA-256
M
Verify
g^{H(m)} (mod p): 74f3578a77
y^{R_D} r^{s_D} (mod p): 74f3578a77
Succeed
Successful Verification
3. Verification of Digital Signature

Figure 6. The digital signature process on an SES market blockchain based the traditional ElGamal digital signature mechanism.

Obviously, without the proxy signature mechanism, the SESO cannot accomplish the whole market transaction process on the blockchain on behalf of the owner alone, though the SESO has accepted the delegation. The core power of the market transaction on blockchains—i.e., digital signature power—is still kept by the delegation node. Therefore, the execution of all the market behaviors, including information issuing, bidding, data querying and contract signing, need to be signed by the online delegation node, where the transaction efficiency may be affected because of the fault or disconnection of the node. In this situation, the SESO is unable to obtain the whole transaction rights on the blockchain and only acts as a decision-making consultant who provides transaction strategies to the owner, which greatly reduces the value and function of the SESO.

5.2. Consensus Process

The consensus mechanism is the core part in blockchains, achieving the validation and confirmation of the ledgers on blockchains and reaching the uniformity of the distributed database. At present, practical Byzantine fault tolerance (PBFT) is a common consensus mechanism in consortium blockchains that are the first choice in the energy sector including SES [15]. A typical consensus process of PBFT is shown in Figure 7 [34]. It can be seen that the consensus process includes five phases: request, pre-prepare, prepare, commit and reply. A message from the client (i.e., "C" in the Figure 7) will be validated and accepted by other nodes (i.e., "0", "1", "2" and "3" in the Figure 7, though "3" is faulty at this time) through the consensus process. More detail about PBFT, such as the analysis of process, performance evaluation and implement techniques, can be found in [34].

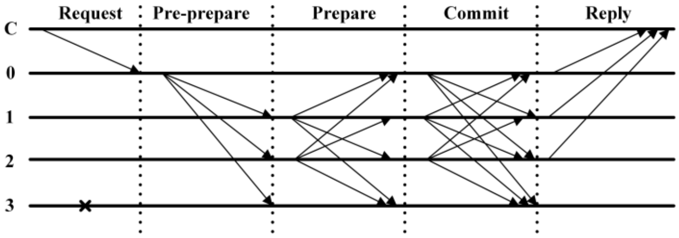

Figure 7. The typical consensus process of practical Byzantine fault tolerance (PBFT).

The prepare phase of PBFT is selected in this case. In the phase, a prepare message with the digital signature of the node is multicast to all other nodes when the node accepts the pre-prepare message in order for all nodes to verify the correctness of the message with each other. Therefore, on an SES blockchain, a prepare phase based on the traditional scheme and a prepare phase based on the principal-agent model with the proxy signature mechanism are, respectively, shown in Figures 8 and 9. It is assumed that there are five nodes deployed on the blockchain, including a primary node and four follower nodes. The primary node is selected according to the node number, the node state and the validation result.

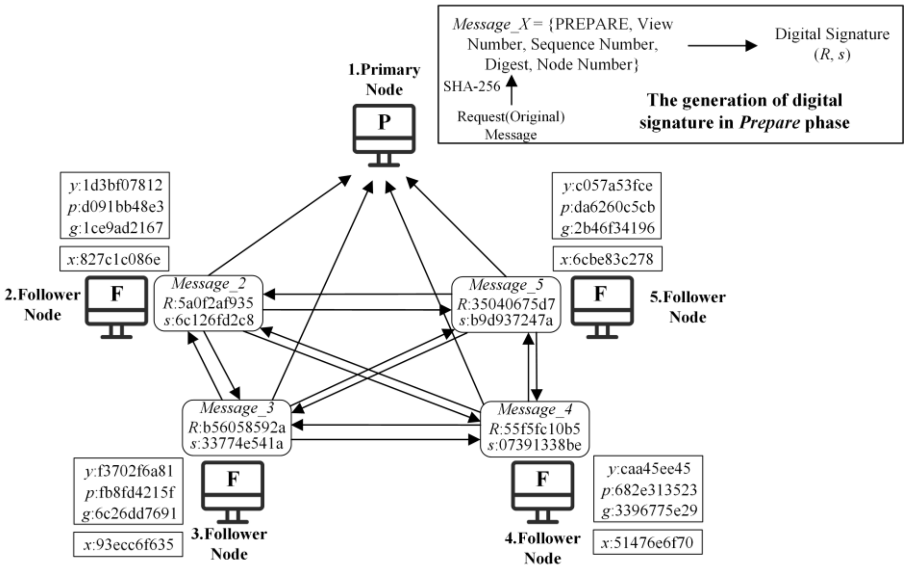

Figure 8. The prepare phase based on the traditional scheme.

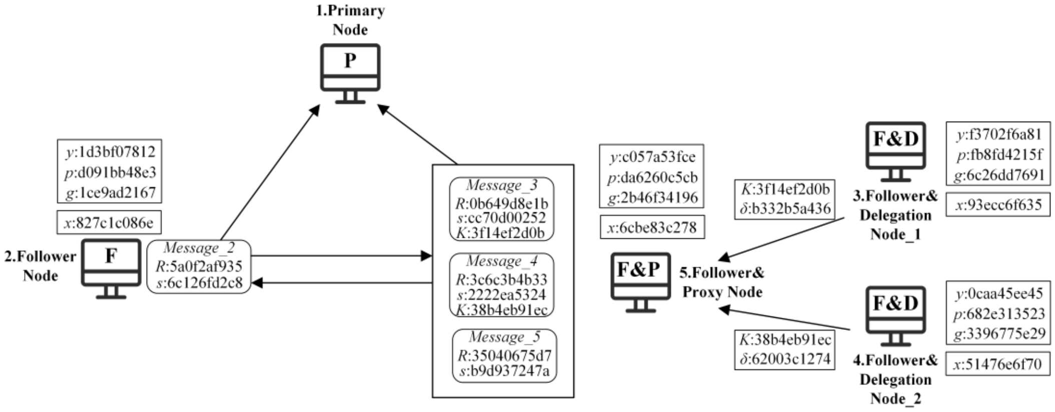

Figure 9. The prepare phase based on the principal-agent model with the proxy signature mechanism.

It can be seen from Figure 8 that the other nodes, except for the primary node, multicast a prepare message to all nodes on the blockchain. The prepare message consists of two parts: the prepare message body and its digital signature produced by the private key of the node. The prepare message body consists of a label of "PREPARE", the view number and sequence number of this consensus process, the digest of the original message from the client forwarded by the primary node in the pre-prepare phase and the node number. Then, the prepare message body is signed by the node, and the digital signature for the prepare message body is obtained. The digital signature mechanism based on the ElGamal algorithm is applied in the consensus process. Once the signature is verified to be correct and the view number and sequence number are right, the node that receives the prepare message will accept the message. At last, when the node accepts enough messages from other nodes (twice the number of tolerable faulty nodes of the blockchain), the node will start the commit phase and multicast a commit message to other nodes. It is worth mentioning that the nodes on the blockchain may be in different phases of the consensus process at a certain time, and therefore the figures show the message exchange at the same prepare phase.

As shown in Figure 9, node 5 accepts the delegations from node 3 and node 4 at the same time. Therefore, node 5 is the proxy node, and node 3 and node 4 are the delegation node. For a blockchain supporting the proxy signature mechanism, although the primary node sends a pre-prepare message to the delegation nodes, the proxy node will multicast the prepare message on behalf of the delegation nodes when it receives the pre-prepare message even if the delegation nodes may be faulty or off-line. The sent messages from the proxy node and the corresponding delegation nodes are consistent. It can be seen from Figure 9 that node 5 multicasts three prepare messages to other nodes, including a message of node 5 itself and two messages signed by using the proxy keys. The nodes that receive the three messages, node 1 and node 2, also accept these messages if the ordinary digital signature and the proxy signatures are verified. In addition, node 1 and node 2 can tell whether a received message is coming from a normal follower node or a proxy node according to the structure of the signature. If a message signed by the proxy node is identified as a malicious message, the proxy node, not the delegation node, will be responsible for this.

When the principal-agent model with the proxy signature mechanism is utilized in the consensus process based on PBFT, the stability of the network can be enhanced because the proxy nodes deployed in the professional servers of SESOs may be healthier and more robust than ones deployed in the servers of owners. Moreover, the efficiency and speed of the consensus process are also improved due to the reduced amount of the nodes that need to multicast messages. However, the security of the consensus process may be affected by the proxy signature mechanism once a proxy node accepts the delegations from a great number of delegation nodes. The reason for this is that the content of multicast messages is decided by the proxy nodes independently, and the delegation nodes probably do not know what the proxy node does. In order to address the above problem, the number of delegations that a proxy node can accept should be limited according to the total number of nodes on the blockchain.

On the other hand, the proxy nodes are less likely to attack the blockchain maliciously but have a strong incentive to maintain it because the proxy nodes—i.e., SESOs, rely more on the SES market blockchain from the perspective of interest. Finally, the malicious behaviors of the proxy nodes will be recorded in the blockchain, which can hold the malicious nodes accountable.

6. Conclusions

A management method of SES based on a proxy signature mechanism in the blockchain environment is proposed in this paper. Several conclusions are drawn as follows:

1. Based on budget cost, profit expectation, management ability and market rules, the owners of idle energy storage resources can select a suitable management model, such as a self-operation model or principal-agent model, to gain more profits in the SES market.

2. Blockchains can meet the demands of SES well. The fairness, efficiency and credibility in the sharing process can be achieved by blockchains and basic technologies.

3. The proxy signature mechanism can achieve the delegation of digital signature power under the premise of security and reliability, which is suitable for the principal-agent model in the blockchain environment.

4. Two typical application scenarios for the principal-agent model with the proxy signature mechanism on an SES blockchain, the digital signature process of an SES bidding message and the consensus process based on PBFT are simulated and compared. Some characteristics such as the online decision support, the agent for the off-line or faulty delegation nodes and the enhanced efficiency of consensus processes are represented, providing the potential to improve the flexibility of the SES market and its blockchain.

Future work will focus on the SES market mechanism considering the principal-agent model and the application of the proxy signature mechanism on the data sharing and transaction blockchain of SES.

Author Contributions: Conceptualization, L.D., L.Y. and Z.L.; methodology, Y.W. and W.Q.; software, Y.W., W.Q. and Y.P.; validation, W.Z., W.Q. and Y.P.; formal analysis, Y.W.; investigation, H.N.; resources, L.D., H.N. and Z.L.; data curation, Y.P.; writing—original draft preparation, Y.W. and W.Q.; writing—review and editing, L.D., L.Y. and Z.L.; visualization, W.Q.; supervision, Y.W. and W.Z.; project administration, Y.W., L.D. and H.N.; funding acquisition, L.D., H.N. and Z.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by the Science and Technology Project of the State Grid Qinghai Electric Power Company.

Acknowledgments: This work was supported by the Science and Technology Project of the State Grid Qinghai Electric Power Company.

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

References

1. Nosair, H.; Bouffard, F. Reconstructing operating reserve: Flexibility for sustainable power systems. *IEEE Trans. Sustain. Energy* **2015**, *6*, 1624–1637. [CrossRef]
2. Liu, S.; Zhao, Y.; Lin, Z.; Liu, Y.; Ding, Y.; Yang, L.; Yi, S. Data-driven event detection of power systems based on unequal-interval reduction of PMU data and local outlier factor. *IEEE Trans. Smart Grid* **2019**, *11*, 1630–1643. [CrossRef]
3. Liu, S.; Lin, Z.Z.; Zhao, Y.; Liu, Y.; Ding, Y.; Zhang, B.; White, S.E. Robust system separation strategy considering online wide-area coherency identification and uncertainties of renewable energy sources. *IEEE Trans. Power Syst.* **2020**, *35*, 3574–3587. [CrossRef]
4. Zhang, D.; Wang, J.; Lin, Y.; Si, Y.; Huang, C.; Yang, J.; Huang, B.; Li, W. Present situation and future prospect of renewable energy in China. *Renew. Sustain. Energy Rev.* **2017**, *76*, 865–871. [CrossRef]
5. Weitemeyer, S.; Kleinhans, D.; Vogt, T.; Agert, C. Integration of renewable energy sources in future power systems: The role of storage. *Renew. Energy* **2015**, *75*, 14–20. [CrossRef]
6. Shrestha, T.K.; Karki, R. Utilizing energy storage for operational adequacy of wind-integrated bulk power systems. *Appl. Sci.* **2020**, *10*, 5964. [CrossRef]

7. Lombardi, P.; Schwabe, F. Sharing economy as a new business model for energy storage systems. *Appl. Energy* **2017**, *188*, 485–496. [CrossRef]
8. Kalathil, D.; Wu, C.; Poolla, K.; Varaiya, P. The sharing economy for the electricity storage. *IEEE Trans. Smart Grid* **2019**, *10*, 556–567. [CrossRef]
9. Chakraborty, P.; Baeyens, E.; Poolla, K.; Khargonekar, P.P.; Varaiya, P. Sharing storage in a smart grid: A coalitional game approach. *IEEE Trans. Smart Grid* **2019**, *10*, 4379–4390. [CrossRef]
10. Liu, J.; Zhang, N.; Kang, C.; Kirschen, D.; Xia, Q. Cloud energy storage for residential and small commercial consumers: A business case study. *Appl. Energy* **2017**, *188*, 226–236. [CrossRef]
11. Gai, K.; Wu, Y.; Zhu, L.; Qiu, M.; Shen, M. Privacy-preserving energy trading using consortium blockchain in smart grid. *IEEE Trans. Ind. Informat.* **2019**, *15*, 3548–3558. [CrossRef]
12. Dong, Z.; Luo, F.; Liang, G. Blockchain: A secure, decentralized, trusted cyber infrastructure solution for future energy systems. *J Mod. Power Syst. Clean Energy* **2018**, *6*, 958–967. [CrossRef]
13. Wang, N.; Zhou, X.; Lu, X.; Guan, Z.; Wu, L.; Du, X.; Guizani, M. When energy trading meets blockchain in electrical power system: The state of the art. *Appl. Sci.* **2019**, *9*, 1561. [CrossRef]
14. Astarita, V.; Giofrè, V.P.; Mirabelli, G.; Solina, V. A review of blockchain-based systems in transportation. *Information* **2020**, *11*, 21. [CrossRef]
15. Christidis, K.; Devetsikiotis, M. Blockchains and smart contracts for the Internet of things. *IEEE Access* **2016**, *4*, 2292–2303. [CrossRef]
16. Wang, J.; Wu, L.; Choo, K.-K.R.; He, D. Blockchain-based anonymous authentication with key management for smart grid edge computing infrastructure. *IEEE Trans. Ind. Inform.* **2019**, *16*, 1984–1992. [CrossRef]
17. Andoni, M.; Robu, V.; Flynn, D.; Simone, A.; Dale, G.; David, J.; Peter, M.; Andrew, P. Blockchain technology in the energy sector: A systematic review of challenges and opportunities. *Renew. Sustain. Energy Rev.* **2019**, *100*, 143–174. [CrossRef]
18. Zia, M.F.; Benbouzid, M.; Elbouchikhi, E.; Muyeen, S.M.; Techato, K.; Guerrero, J.M. Microgrid transactive energy: Review, architectures, distributed ledger technologies, and market analysis. *IEEE Access* **2020**, *8*, 19410–19432. [CrossRef]
19. Zhu, S.; Song, M.; Lim, M.-K.; Wang, J.; Zhao, J. The development of energy blockchain and its implications for China's energy sector. *Resour. Policy* **2020**, *66*, 101595. [CrossRef]
20. Han, D.; Zhang, C.; Ping, J.; Yan, Z. Smart contract architecture for decentralized energy trading and management based on blockchains. *Energy* **2020**, 117417. [CrossRef]
21. Wang, S.; Taha, A.F.; Wang, J.; Kvaternik, K.; Hahn, A. Energy crowdsourcing and peer-to-peer energy trading in blockchain-enabled smart grids. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *49*, 1612–1623. [CrossRef]
22. Jiang, Y.; Zhou, K.; Lu, X.; Yang, S. Electricity trading pricing among prosumers with game theory-based model in energy blockchain environment. *Appl. Energy* **2020**, *271*, 115239. [CrossRef]
23. Cha, S.-C.; Chen, J.-F.; Su, C.; Yeh, K.-H. A blockchain connected gateway for BLE-based devices in the Internet of Things. *IEEE Access* **2018**, *6*, 24639–24649. [CrossRef]
24. Li, L.; Liu, J.; Cheng, L.; Qiu, S.; Wang, W.; Zhang, X.; Zhang, Z. Creditcoin: A privacy-preserving blockchain-based incentive announcement network for communications of smart vehicles. *IEEE Trans. Intell. Transp. Syst.* **2018**, *19*, 2204–2220. [CrossRef]
25. Chandel, S.; Cao, W.; Sun, Z.; Yang, J.; Zhang, B.; Ni, T.-Y. A multi-dimensional adversary analysis of RSA and ECC in blockchain encryption. In *Future of Information and Communication Conference*; Springer: Cham, Switzerland, 2019; pp. 988–1003.
26. Kumar, M.M.; Prasad, M.V.; Raju, U.S.N. BMIAE: Blockchain-based multi-instance Iris authentication using additive ElGamal homomorphic encryption. *IET Biometrics* **2020**, *9*, 165–177. [CrossRef]
27. George, G.; Sankaranarayanan, S. Light weight cryptographic solutions for fog based blockchain. In Proceedings of the 2019 International Conference on Smart Structures and Systems (ICSSS), Chennai, India, 14–15 March 2019; pp. 1–5.
28. Mambo, M.; Usuda, K.; Okamoto, E. Proxy signatures for delegating signing operation. In Proceedings of the 3rd ACM Conference on Computer and Communications Security, New Delhi, India, 14–16 March 1996; pp. 48–57.
29. Lixin, Z.; Fengli, W. Strategy for China intercity-railway operation management model based on varied investors. *Transp. Res. Proc.* **2017**, *25*, 3808–3816. [CrossRef]

30. Casino, F.; Dasaklis, T.-K.; Patsakis, C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. *Telemat. Inform.* **2019**, *36*, 55–81. [CrossRef]
31. Li, S.; Zhang, S.; Andrews-Speed, P. Using diverse market-based approaches to integrate renewable energy: Experiences from China. *Energy Policy* **2019**, *125*, 330–337. [CrossRef]
32. ElGamal, T. A public key cryptosystem and a signature scheme based on discrete logarithms. *IEEE trans. Inf. Theory* **1985**, *31*, 469–472. [CrossRef]
33. Wang, P.; Zhang, F. An efficient collision detection method for computing discrete logarithms with Pollard's rho. *J. Applied Math.* **2012**, *2012*, 635909. [CrossRef]
34. Castro, M.; Liskov, B. Practical byzantine fault tolerance. In Proceedings of the Third Symposium on Operating Systems Design and Implementation (OSDI'99), New Orleans, LA, USA, 22–25 February 1999; Volume 99, pp. 173–186.

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.