Research on Energy Blockchain Platform Based on Private Key Storage Algorithm of Image Information Hiding

Dong Xia¹, Hua Mao¹, Changwei Zhao², Shengyuan Zhong³*, Fanjin Wang⁴, Xiao Liu⁵

¹ State grid Tianjin power economic and technology research institute, Tianjin, 300171, China
² State grid Tianjin chengdong electric power supply company, Tianjin, 300171, China
³ School of mechanical engineering, Tianjin University, Tianjin, 300072, China
⁴ Nankai University, Tianjin, 300071, China
⁵ Tianjin green energy union technology development company, Tianjin, 300162, China
*Corresponding author’s e-mail: zhongshengyuan@tju.edu.cn

Abstract. With the adjustment of the world's energy structure, the proportion of clean energy represented by renewable energy is increasing. In response to the shortcomings of renewable energy instability, researchers have proposed the concept of the microgrid. However, with the expansion of the scale of the promotion of the microgrid, the traditional energy distribution system with the sales company as the core exposes the shortcomings of being inflexible. Based on this researcher's continuous exploration of new energy trading models, the energy blockchain has developed rapidly in recent years. Reliable private key storage is a necessary guarantee for the security of energy blockchain services. At present, blockchain private key storage technology still has many security risks in the new energy transaction mode. This paper first builds an energy blockchain platform inside the microgrid, so that all participants can complete energy transactions more safely and conveniently. At the same time, the energy blockchain private key storage technology based on image information hiding is proposed. The blockchain private key is hidden in the watermark information and embedded in the carrier image. A watermarking algorithm based on discrete wavelet transform and quantization index modulation is used to accurately extract the blockchain private key. Finally, the feasibility and security of the algorithm are proved by an example test analysis.

1. Introduction

With the rapid development of the economy, the demand for electricity is growing rapidly. Nevertheless, the centralized supply mode of the power grid has higher operating costs and energy losses due to the long physical distances between generation and consumption sites which are caused by the increase of the user scale [1]. Distributed Energy System (DES) with renewable energy such as solar energy and wind energy provides a solution to this energy dilemma [2]. However, the uncertainties and fluctuations of renewable energy need to be considered. In order to address the impact of the grid on renewable energy and take advantage of DES' flexibility, efficiency and economy, researchers are beginning to focus on more complete microgrid management [3].
In a DES-based microgrid, energy consumers can also be energy producers. If more individuals can participate in the microgrid energy transaction, the renewable energy generation will be absorbed nearby, thus avoiding impact on the large grid and improving energy efficiency [4]. In addition, this empowers energy consumers and producers within the microgrid to motivate local investments and help develop a self-sustaining microgrid community [5]. However, most of the operating status and price information of the power system are not transmitted to the end users in time under the existing market mechanism. At the same time, trust and security are also issues that the energy management platform needs to consider.

The emergence of blockchains has provided a new power trading model for microgrids. The blockchain is essentially an integrated distributed database of various computer technologies such as P2P networks, consensus mechanisms, encryption algorithms, and smart contracts. Blockchain technology has played a huge role in the power industry, and transactions between power sellers and consumers can be done through blockchains [6]. Consensus Systems and LO3 Energy partnered to build an interactive photovoltaic platform, TranActive Grid, based on the Ethereum blockchain system in a block in Brooklyn, New York [7]. Power transactions between users are completed through the energy blockchain platform and do not rely on third-party service providers. However, in the face of future large-scale energy blockchain transactions, the existing energy blockchain management platform rarely considers the security of users’ private information such as private keys.

To this end, this paper builds a blockchain-based energy management platform. The energy blockchain platform connects all members of the microgrid and enables smart and transparent transactions with smart contract technology. Meanwhile, this paper proposes an energy blockchain private key storage algorithm based on image information hiding. An improved quantized index modulation watermarking algorithm based on discrete wavelet transform is used to embed the private key as watermark information into the image. It has been tested and proved to have good transparency and excellent robustness, and can be adapted to the storage and use of the energy blockchain private key.

2. Energy blockchain platform

Based on blockchain & smart contract technology, the microgrid power energy trading platform realizes end-to-end trading of power energy within the microgrid and maximizes the activity and efficiency of power assets with high-speed and flexible transactions. Figure 1 shows the schematic diagram of the microgrid trading platform.

![Figure 1. Schematic diagram of the microgrid trading platform.](image)

All end users, power plants and power sales companies are connected to the trading platform via smart meters and smart contract protocol. The traditional way of selling electricity is done through the platform, and the transaction is safe, reliable and can be tracked throughout.

Moreover, since all end users access the blockchain platform, power transactions between users can also be completed through the platform. Figure 2 shows the electricity trading mode between users.
In this mode, a transaction is initiated when an A user needs to purchase electricity and the D user's renewable energy generation is excessive. The funds authorized by the user A pay the electricity fee to the user D via the bank, and at the same time pay the network fee to the grid S. The power of the D user is delivered to the A user via the grid. The entire payment process will be recorded in a certain block. The core power sales companies in traditional power trading are only used as an intermediate recorder in the blockchain trading platform, making the whole transaction process more flexible and fast. Due to the nature of the blockchain technology, user A and user D do not have to worry about being deceived even if the sales company is not at the core.

3. Private key storage algorithm

3.1. Algorithm flow

Based on the previous analysis, almost everyone can participate in real-time power trading with blockchain technology. But the problem with full participation is that not every participant has enough vigilance to protect the private key that they use to authorize the transaction. At present, the private key of the blockchain is stored by using wallet software or traditional encryption technology, which has the above security risks.

This paper proposes an energy blockchain private key storage algorithm based on image information hiding. The private key of the energy node is used as the text watermark information, and a specific watermark algorithm is selected to be embedded in the carrier image for storage to ensure the secure storage of the node private key information. Since this algorithm is mainly applied to the energy blockchain private key storage, it is necessary to select the best robust transform domain algorithm. Here, the discrete wavelet transform is selected.

The image information hiding technology not only hides the content of the private key but also hides the existence of the private key, which improves the storage security of the energy blockchain private key. The general process is shown in figure 3.

![Figure 3. General process of the algorithm.](image)

First, the energy node generates watermark information according to its blockchain private key and then embeds the watermark information into the image carrier according to a specific watermark embedding algorithm. The watermark extraction algorithm and its embedding process correspond to a certain degree, mainly based on the inverse extraction of the watermark information of the embedded
image according to the embedding algorithm. During the test, the original watermark information and the extracted watermark information are compared and detected, and some parameters of the algorithm are adjusted according to the bit error rate (BER).

3.2. Watermark information generation

Although the existence and specific information of the private key can be hidden by the image information hiding technology, the original private key information needs to be further processed for security. Figure 4 is a schematic diagram of this process.

![Figure 4. Schematic diagram of watermark information generation.](image-url)

If an attacker intercepts a watermark image and notices that important information is hidden in the watermark image during the process of energy trading, it may attempt to perform steganographic analysis to extract secret information. Therefore, a random number is added to the original private key to masquerade the private key information. At the same time, the addition of the error correction code not only reduces the error of the transmission process but also provides double protection for the original private key information.

3.3. Embedded algorithm

Since the image information hiding algorithm is for storing the private key of the energy node, the watermark image is generally stored in the terminal or hardware. Therefore, it is mainly considered that when image scaling, JPEG compression, noise attack, etc. occur, the algorithm can still correctly and completely recover the energy blockchain private key.

The quantization index modulation (QIM) algorithm has good robustness against common signal processing type attacks. The principle is that the watermark information and the original information of the host are quantified according to different quantizers, and the calculated result is an image containing watermark information. Therefore, this paper compares the BER of the traditional QIM algorithm, STDM algorithm and improved QIM algorithm, and finally chooses the improved gain invariant quantization index modulation watermarking algorithm. The main process of watermark embedding is shown in figure 5.

![Figure 5. Process of watermark embedding.](image-url)

Firstly, this paper chooses the appropriate watermark embedding layer and performs three-level discrete wavelet transform on it. The obtained result is embedded in the watermark information according to the watermark embedding algorithm. Then, the processed layer is subjected to discrete wavelet inverse transform to generate a carrier layer embedded with watermark information, and finally a complete watermark image is synthesized.

3.4. Private key extraction

The extraction algorithm and the embedding algorithm are basically symmetrical. However, the watermark information extracted at this time is masqueraded, and the error correction code of the watermark information needs to be decoded. Then remove the added random number and finally convert it to the original private key information. The main process is as shown in Figure 6.
4. Algorithm test

In order to test the performance of the algorithm, this paper simulates the embedded effect and extraction effect of the algorithm. This paper selects a randomly selected image on the Internet. Figure 7 shows the test sample.

The watermark information is any 256bits private key "10c0cf0e51162bd72968ec6f7bf31ba9e7bda2a3fa47986895bd8b1e5c5A532". The image resolution is uniformly adjusted to 960*720 before embedding the watermark during the test.

4.1. Embedding effect
Test the embedding effect of this algorithm with Figure 7 as an example. Figure 7 is a randomly selected JPG format image with a resolution of 1024*640. Figure 8 is one of the watermark images of the figure 7 embedding result.

The final test result sample has a BER of 0, and the extracted private key is complete. The algorithm is correct without any processing on the watermark image, and can accurately extract the blockchain private key information.

4.2. Robustness test

Image scaling, Poisson noise, and JPEG compression were used as attack tests, and a clipping attack was added as a comparison. The BER value after the attack is used as a verification indicator of robustness. Table 1 shows the results of the robustness test.

| Attack          | BER  | Zoom (0.5times) | Zoom (2times) | Zoom (4times) | Poisson's attack | Salt and pepper attack | Gaussian noise | Jpeg compress | Clipping attack |
|-----------------|------|-----------------|---------------|---------------|-----------------|-----------------------|----------------|--------------|----------------|
|                 | 0.0000 | 0.0000          | 0.0000        | 0.0000        | 0.0000          | 0.0000                | 0.0000        | 0.0000       | 0.4323         |

According to the test results in Table 1, it can be known that: For the image attack, such as image scaling, Poisson noise, JPEG compression, etc., the algorithm is robust. However, if processed by printing, trimming, etc., the watermark information will be lost to a certain extent, and it is difficult to recover accurate private key information. Therefore the watermark image of the implicit private key information cannot be printed or trimmed.
5. Conclusion
The energy blockchain is one of the means to deal with the large-scale application of distributed renewable energy in the future. However, the blockchain is in an early stage of exploration in energy applications, and there is currently no complete energy blockchain system. This paper builds an energy blockchain platform in a microgrid based on blockchain and smart contract technology.

At the same time, it is considered that the preservation of the private key needs to be safer and more convenient when a large number of users join. Therefore, this paper proposes an energy blockchain private key storage algorithm based on image information hiding. The quantization index modulation watermarking algorithm based on discrete wavelet transform used in this paper is robust and can effectively resist image attacks such as image scaling, JPEG compression and Poisson noise. The application of this method can make the constructed energy blockchain platform more reliable.

Acknowledgments
This work is supported by the project of research on market mechanism of integrated energy system based on blockchain technology.

References
[1] Silvente J, Kopanos GM, Pistikopoulos EN, Espuña A. (2015) A rolling horizon optimization framework for the simultaneous energy supply and demand planning in microgrids. J. Applied Energy, 155: 485–501.
[2] Mengelkamp E, Gärttner J, Rock K, et al. (2018) Designing microgrid energy markets. J. Applied Energy, 210: 870-880.
[3] Bahrami S, Amini MH. (2017) A decentralized framework for real-time energy trading in distribution networks with load and generation uncertainty. J. arXiv preprint arXiv: 1705.02575.;
[4] Guo L, Chen X, Deng H, He Y, Chen Q. (2018) A Framework of Operating Mechanism Based on Peer-to-Peer Transaction Among Distributed Energy Resources in Community Microgrid. J. Electric Power Construction, 39(07): 2-9.
[5] Coelho VN, Cohen MW, Coelho IM, Liu N, Guimarães FG. (2017) Multi-agent systems applied for energy systems integration: state-of-the-art applications and trends in microgrids. J. Applied Energy, 187: 820–32.
[6] Sikorski J J, Haughton J, Kraft M. (2017) Blockchain technology in the chemical industry: Machine-to-machine electricity market. J. Applied Energy, 195: 234-246.
[7] Nguyen C. (2016) An indie, off-the-grid, blockchain-traded solar power market comes to brooklyn. http://motherboard.vice.com/read/the-plan-to-power-brooklyn-with-a-blockchain-base dmicrogrid-transactive-solar.