Journal of Artificial Intelligence Practice (2022)
Clausius Scientific Press, Canada

DOI: 10.23977/jaip.2022.050104
ISSN 2371-8412 Vol. 5 Num. 1

A User Privacy Protection Scheme in Incentive Demand Response Transaction Based on Blockchain

Shaomin Zhang[a,*], Jiahui Pang[b] and Baoyi Wang[c]

School of Control and Computer Engineering, North China Electric Power University, China
a. zhangshaomin@126.com, b. pangjiahui0304@126.com, c. wangbaoyi@126.com
**corresponding author*

Keywords: incentive demand response, privacy protection, blockchain, power transaction

Abstract: As the smart grid gradually transforms, incentive demand response is becoming increasingly popular. Incentive demand response based on an auction mechanism not only increases the interest of users in participating, but also increases the benefits to the maximum. However, there are problems of non-transparent transactions and leakage of user privacy during these transactions. To solve the above-mentioned problems in the incentive demand response transaction process, a scheme based on the combination of blockchain and incentive demand response is proposed. A blockchain demand response transaction mechanism is designed in the scheme to address the issue of user data leakage. The scheme not only ensures user privacy and transaction transparency, but also features tamper-evident data and traceable transactions. The scheme optimises the demand response transaction process and increases transaction efficiency.

1. Introduction

Nowadays, to combat climate change, China is gradually moving towards a green economy with the goal of “carbon peaking and carbon neutrality”. In the severe power supply and demand situation, incentive demand response, as an important part of the grid, plays a vital role in keeping the balance of power supply and demand. Incentive demand response can cut peaks and fill valleys, thus benefiting the demand side as well as the generation side, achieving a win-win outcome [1]. Incentive demand response rewards participating users who provide balanced power demand and is a more flexible model for DR programs [2]. Users play an important role in grid demand response and are an integral part of the grid. Ensuring the legitimacy and security of user transactions during demand response transactions is always research focus for researchers. It is important to study the privacy protection issues in the transaction process in incentive demand response. Assuming that the grid is to monitor a small part of the grid at a high temporal frequency, such as the need to access information about the users of a particular substation or the residential electricity consumption of a street every 15 minutes (or more frequently), an attacker accessing smart metering data can infer private information about the users using interference-free load monitoring techniques [3]. ALM

(Appliance Load Monitoring) is also used for monitoring and locating people in the room, because (e.g. what equipment is running or what state it is working in) the user's lifestyle can be reacted to by the operating state of the equipment [4].

As an emerging technology, the use of blockchain's distributed ledger and decentralized processing can not only solve the problem of data tampering in demand response and ensure the authenticity and trustworthiness of data, but also reduce the cost of enterprises through decentralized processing. The cost of maintaining trust between different subjects can be greatly reduced by blockchain-based demand response transaction mechanism. Demand response and blockchain are combined to create a demand response transaction mechanism that allows for a dynamic balance of efficiency, cost and privacy. Under this mechanism, customers are optimally compensated for the reduction of their usual electricity bills and the authenticity of the transaction.

2. Related Work

There are many problems in demand response business, such as the security of the contract cannot be guaranteed and problems of privacy leakage during the transaction. Blockchain has a great advantage in solving these problems. The authors [5] designs a blockchain-based demand response system that addresses the security and trust issues that exist, examining aspects such as interconnection consensus mechanisms, operational processes, and chain-making machines. The authors [6] designs an energy system that relies on OpenADR for interoperability, which relies on smart contracts on the blockchain for privacy protection against data tampering, and which provides validity guarantees for users. The literature [7] studies the concept of load shifting for demand response and uses genetic algorithms to solve for the average load profile, reducing peak loads as well as significantly reducing costs. Gai et al [8] proposes a permissioned smart grid edge model to address privacy and energy security issues, using group signature and covert channel authorization techniques to ensure the legitimacy of users. An optimal security-aware strategy is constructed through smart contracts running on a blockchain platform to address security and privacy issues. Li et al [9] proposes an optimized scheduling real-time demand response strategy that is model-free and does not require knowledge of the uncertainty distribution using a trust region policy optimization (TRPO) based policy search algorithm to train the neural network. The scheme is effective under real electricity prices and outdoor temperature conditions. The literature [10] proposes a design approach for a distributed energy management system with real-time demand response, consisting of multiple intelligences and using block chains and alternating direction multiplication for real-time demand response. Deshpande et al [11] proposes a fair and efficient mechanism for disaster tolerance distribution, proposing a blockchain-based framework to address the problems of opacity, non-reliability and non-traceability in demand response operations in the grid, capable of balancing various demand response metrics paradigms. Kalakova et al [12] uses a distributed double auction mechanism where each node can become an auctioneer, eliminating single point of attack, creating a decentralized energy trading platform, reducing transmission losses, and improving system efficiency and security. The literature [13] proposes a blockchain-based credit management method for demand response resources, which reduces the default risk of users and applies smart contracts to the ethereum test chain to reduce the invocation cost of demand response resources, and users with high credit values can obtain more benefits and maintain the stable development of the demand response resource trading market.

This paper first establishes a blockchain-based demand response transaction communication model for home users, and proposes a blockchain-based incentive demand response transaction mechanism and user privacy protection scheme, which is dedicated to improving the efficiency and security of the incentive demand response process. The rest of the paper is as follows. In Section three the design ideas and the system model are presented. In section four the scheme security is evaluated. In section five the overall content of the scheme is summarised as well as the issues to be studied in the future.

3. System Architecture

3.1. Design Ideas

Blockchain is essentially a distributed database of tamper-evident data that can be decentralized to prevent the use of central databases, and has features such as tamper-evident, open and transparent, and traceable. This solution mainly protects the user's identity information, the transaction price and the power value, and uses the above-mentioned features of blockchain to make the demand response transaction process transparent and traceable, preventing third parties from changing the transaction data and thus leading to a loss of benefits for the user.

This paper proposes an architecture for a blockchain-based incentive demand response system based on the characteristics of blockchain. This architecture contains five entities involved in the transaction, including the electricity market(EM), demand response providers(DRP), multiple electric users(EU),electricity suppliers(ES) and a trusted third entity (blockchain). The process of incentive demand response transactions in this architecture is shown in Figure 1. DD is represented as a distributed database in Figure 1.

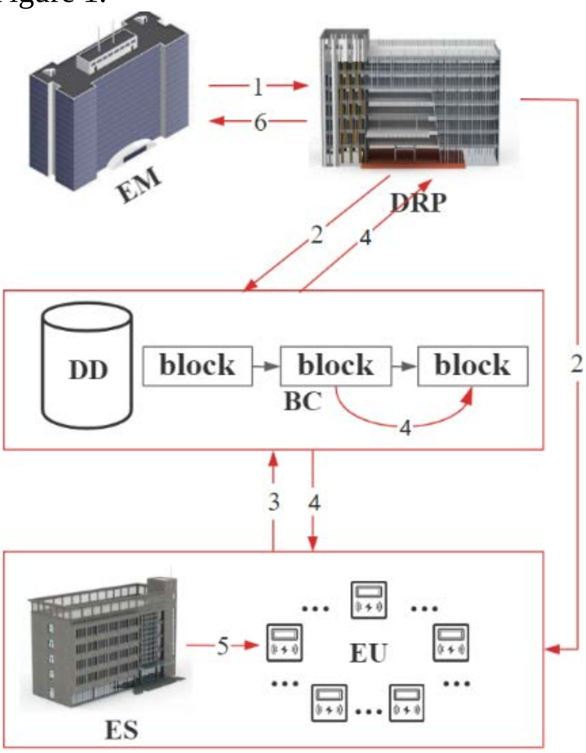

Figure 1: System architecture diagram.

3.2. System Implementation Process

The specific process is explained as follows.

1.The electricity market in the grid sends demand response signals to demand response providers.

2.Once the demand response provider receives the demand response signal, it submits the bid information to the blockchain and notifies the user to bid, after which it is ready to initiate the transaction process.

3.The blockchain first verifies the user's identity reputation value, after which the electricity user submits information to the blockchain and, after participating in consensus through the blockchain's consensus mechanism, stores the relevant information submitted by the demand response provider and the user.

The transaction is then formally initiated and the electricity is priced through a pricing algorithm, after which the winning user is determined.

4.The results of the auction are uploaded to the blockchain by consensus mechanism and notified to demand response providers and customers as well as electricity suppliers.

5.The winning user receives a reward, such as a discount or coupon, after which the user is discounted when purchasing electricity.

The electricity supplier reduces the cost based on the information saved in the blockchain and the corresponding user, and generates an electricity bill to be saved in the blockchain.

6.The demand response provider informs the electricity market that the transaction has ended and the electricity market sets the corresponding power price strategy.

3.3. Pricing Algorithm

The pricing algorithm is related to the total real-time load demand within the power system and the prevailing price is determined by solving the optimization problem.

In order to ensure that better customer participation can be motivated and that grid cost losses are minimized, the real-time price should not be lower than the prevailing electricity price, i.e. the real-time price ≥ the prevailing electricity price ($P \geq P_1$). The pricing function is expressed as follows (1):

$$S_E(P; u, d) = \left[(P - P_1)\sum_{n=1}^{N} u_n - \theta \sum_{n=1}^{N} d_n\right]^2 \tag{1}$$

where: u is the energy demand of all users; d_n is the dissatisfaction of user n; and θ is a weighting factor weighing the price gain and user satisfaction. To determine the optimal auction price P, pricing requires knowledge of the energy demand of all users and the value of their dissatisfaction.

Therefore, the blockchain holds the information passed from the user, i.e. the two-dimensional variable (u_n, d_n). Then the optimal real-time auction price is

$$P^* = \underset{P \geq P_1}{\operatorname{argmin}}\, S_E(P; u, d) \tag{2}$$

4. Results Analysis

4.1. Security Analysis

A blockchain-based incentive demand response transaction mechanism is investigated, which is secured by blockchain technology to achieve decentralized storage and to avoid malicious tampering of data by electricity users. The basic structure of the blockchain is shown in Figure 2, including blocks and chains, which are connected in series to form the blockchain. The blocks are divided into a block header and a block body, and the block body holds a large amount of auction transaction information, with each block arranged in an orderly manner with each other. As soon as one block of information is tampered with and changed, then all subsequent blocks of information are bound to change as well, so this ensures the authenticity and correctness of the information.

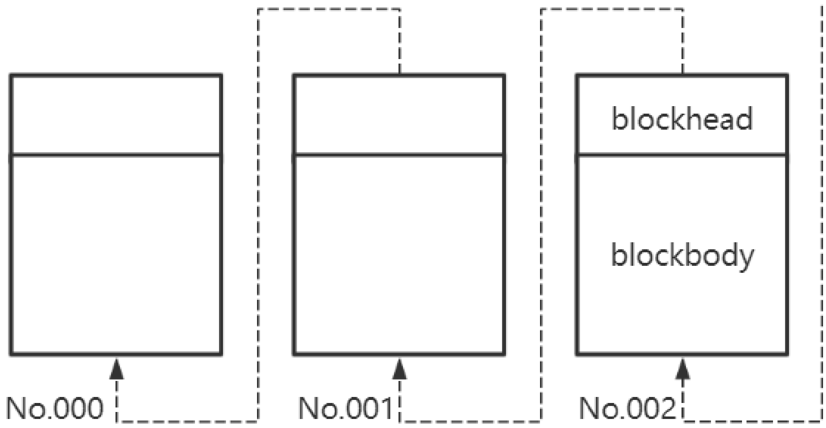

Figure 2: Blockchain.

5. Conclusion

The role of incentive demand response in regulating peaks and valleys cannot be underestimated. Protecting user privacy during response transactions and making the transaction process fair and equitable is a problem that we always have to study carefully. As an emerging technology that combines various techniques of cryptography, research combining the two has become the focus nowadays, so a blockchain-based scheme for protecting user privacy in incentive demand response transaction is proposed. The scheme is able to make transaction transparent while protecting the privacy of the user, and is able to store records in a distributed manner for subsequent checking. It makes a contribution to future research in this area of the grid. How to further increase user satisfaction and motivate more users to participate is the next question to be studied.

References

[1] R. Bai, P. He, Y. Gu, S. Xing. Analysis of Residential Demand Response in Electricity Markets with Wind Generation[J]. Machinery and Electronics, VOL. 39, NO. 7, Pages: 19-23, 2021.

[2] M. Y u and S. H. Hong. A real-time demand-response algorithm for smart grids: A Stackelberg game approach[J], IEEE Transactions on Smart Grid, VOL. 7, NO. 2, Pages: 879-888, 2016.

[3] F. Zhai, W. Xu,Y. Feng, Y. Sun. Design of Improved Paillier Algorithm for Privacy Preserving Scheme of Smart Meter[J]. Electric Power Information and Communication Technology, VOL. 14, NO. 12, Pages: 52-57, Dec. 2016.

[4] L. Yu, H. Li, X. Feng and J. Duan. Nonintrusive appliance load monitoring for smart homes: recent advances and future issues[J]. IEEE Instrumentation & Measurement Magazine, VOL. 19, NO. 3, Pages: 56-62, June 2016.

[5] F. Gong, S. Tian, D. Li et al. Design of Demand Response System Based on Blockchain[J]. Electric Power Information and Communication Technology, VOL. 18, NO. 6, Pages: 82-88, 2020.

[6] Patsonakis C, Terzi S, Moschos I, et al. Tzovaras. Permissioned Blockchains and Virtual Nodes for Reinforcing Trust Between Aggregators and Prosumers in Energy Demand Response Scenarios[C]. 2019 IEEE International Conference on Environment and Electrical Engineering and 2019 IEEE Industrial and Commercial Power Systems Europe (EEEIC / I&CPS Europe), Pages: 1-6, 2019.

[7] Pavithra N, Esther P B. Residential demand response using genetic algorithm [C]. 2017 Innovations in Power and Advanced Computing Technologies (i-PACT), Pages: 1-4, 2017.

[8] K. Gai, Y. Wu, L. Zhu, L. Xu and Y. Zhang. Permissioned Blockchain and Edge Computing Empowered Privacy-Preserving Smart Grid Networks[J]. IEEE Internet of Things Journal, VOL. 6, NO. 5, Pages: 7992-8004, Oct. 2019.

[9] H. Li, Z. Wan and H. He. Real-Time Residential Demand Response[J]. IEEE Transactions on Smart Grid, VOL. 11, NO. 5, Pages: 4144-4154, Sept. 2020.

[10] D. Ogawa, K. Kobayashi and Y. Yamashita. Blockchain-Based optimization of Energy Management Systems with Demand Response[C]. 2020 IEEE 9th Global Conference on Consumer Electronics (GCCE), Pages: 58-59, 2020.

[11] V. Deshpande, L. George, H. Badis and A. A. Desta. Blockchain Based Decentralized Framework for Energy Demand Response Marketplace[C]. NOMS 2020-2020 IEEE/IFIP Network Operations and Management Symposium, Pages:1-9,2020.

[12] A. Kalakova, A. Zhanatbekov, A. Surash, H. S. V. S. Kumar Nunna and S. Doolla. Blockchain-based Decentralized Transactive Energy Auction Model with Demand Response[C]. 2021 IEEE Texas Power and Energy Conference (TPEC),Pages:1-6, 2021.

[13] B. Wang, Q. Wang, Y. Li, et al. Transaction mechanism of demand response resource considering credit in blockchain environment[J]. Automation of Electric Power Systems, VOL. 45, NO. 5, Pages: 30-38, Oct. 2019.