Anonymous Energy Loan System on a Smart Grid

Ming-Te Chen[1,a], Chu-Xuan Liang[2,b], and Chia Chu Chen[3,c]

[1,2,3] National Chin-Yi University Technology department of
Computer Science and Information Engineering, 41170 Taichung, Taiwan
[a]mtchen@ncut.edu.tw, [b]s4A817016@student.ncut.edu.tw, [c]croussrm@gmail.com

A smart contract is a state-of-the-art and programmable decentralized blockchain application that can replace banks and serve as a new and fair decentralized financial center. In this paper, we propose an anonymous crowdfunding energy loan system that employs smart contracts and a zero-knowledge proof in a smart grid. This system, which focuses on the energy generated from crowdfunding, enables each party to lend its energy to others. Users who generate energy can input their energy into a smart contract address anonymously and use a zero-knowledge proof to fetch the energy from storage in the smart grid. Users who borrow energy from the smart contract also remain anonymous in this proposed scheme. Moreover, if the borrower refuses to repay the lending energy, then their anonymity can be revoked. Additionally, our scheme employs a lending methodology in which smart contracts can automatically process loan transactions made by each party in the smart grid.

Key Words: Smart contract, Smart grid, Zero-knowledge proof, Loan system

1. INTRODUCTION

A smart contract is a modern and useful type of blockchain technology that enables users to execute script programs on the blockchain and reach a consensus with others. Because smart contracts are considered to be trustworthy and neutral, they are widely used in many fields. They can be used for rights management for Internet of Things (IoT) applications[7], the sharing of medical records[3], and even the control of smart cities[6]. Because large companies such as Tesla expect to begin using virtual currencies, an increasing amount of research on the development and management of smart contracts will be conducted in the next few years. Moreover, smart contracts will begin replacing physical banks as new, virtual financial centers.

Crowdfunding is a financing method that is used for fund-raising to reach a target within a specific period. After reaching this target, the user generates a product and delivers it to the customer. In comparison with traditional financing methods, crowdfunding offers greater accessibility to funds, given that the project team reaches its target by a specified deadline. In addition, as long as the project receives approval and support from the public, the first product can be developed through crowdfunding with the attraction of an early bird price, thus providing opportunities for small-scale business entrepreneurs or creative individuals.

Many unique platforms are available on the Internet, such as China"s Duocaitou, which focuses on small cultural and creative businesses that have already obtained substantial funds and employed special methods to maintain the flow of funds[8].

In this paper, we propose an anonymous energy-lending system that operates through smart contracts on a smart grid. The architecture of the smart grid enables users to lend energy to an energy platform, whereafter the platform can relend energy to others.

This structure can solve the problem of insufficient funds for these entrepreneurs without additional fees because no centralized institution is employed in this scheme, thus reducing energy costs through avoidance of the institution's service fee. Our proposed scheme contains the following features:

1. Lender's anonymity protection: In this system, the lender can anonymously borrow energy from the platform. Moreover, a zero-knowledge proof can be used for proof of identity when the lender wants a refund.

2. Decentralization: Smart contracts are the solution to centralization, and this technology provides an effective solution to help users reach a consensus. Our scheme offers a neutral platform on which smart contracts replace physical banks.

3. Traceability: The borrower can borrow and repay energy from our platform anonymously. When borrowers cannot repay their loans, the system can trace the identity of these borrowers.

4. Zero-knowledge proof: In this system, a zero-knowledge proof is used to prove the identity of users, enabling these users to prove that they are the real borrowers without disclosing their wallet address.

The remainder of this paper is structured as follows. Section 2 describes other systems. Section 3 presents our scheme.

2. RELATED WORK

Although blockchain technologies and cryptocurrencies have recently gained popularity, they do not provide users with the ability to receive loans.

Loans have always been an integral component of the human economy, especially in the past 10 years. This is because a loan system allows the global economy to grow and creates more job opportunities. However, banks lack a solution for how to issue people loans and trace the loaner to get the money back, and this constitutes a serious societal problem. As a solution, Guo et al.[5] proposed a credit-based payment method for fast peer-to-peer energy trading in which some trusted banks are included in the smart grid. In the system, each node has its own credit score that allows it to lend energy to others. Additionally, Guo et al.[4] proposed another credit-based transaction system that addresses the problem of IoT device storage.

Other researchers, however, rather than adopt a credit-based system in a smart grid, have proposed other methods of addressing this problem. One example is the method proposed by Aitzhan and Svetinovic[1], in which a multisignature scheme is employed with a decentralized arbitrator that is involved in the transaction process. Additionally, Luo et al.[2] proposed an SPB system that uses a private blockchain and smart meter to solve electricity trading problems. However, none of these schemes offer an energy-lending functionality in the smart grid.

Our methodology is that proposing an energy-lending platform in the smart grid which can make the energy transaction between the energy borrowers and the loaners with the help of the smart contracts. Moreover, building such an energy-lending platform that it also increase the energy transaction between users in the same smart gird efficiently. Additionally, this system also can prevent the centralization system monopolizing the energy market and let the users have more energy choices.

Therefore, we propose an energy-lending system that employs blockchain technology in the smart grid network. In addition to offering users anonymity protection in the smart grid, this system provides a zero-knowledge proof and crowdfunding capabilities to enable users to borrow energy from the energy loan system anonymously.

3. PROPOSED SCHEME

Some definitions are provided as follows for some of the terms used in this section.

1. Loaner: A legal user who can upload personal energy to a smart contract address and fetch energy from the corresponding address in the smart grid.

2. Borrower b: A legal user/company for which there exists a guaranteed corporation that can confirm the party's identity and claim responsibility for the party's behaviour. After the borrower has been authenticated by a guarantee corporation, they are given a credit score.

3. Guaranteed corporation g: A guarantee corporation can authenticate and issue a credit score to the borrower b.

Table 1: Notation definitions and descriptions

Notation	Description
b	a borrower who she/he attempts to borrow the money.
M_b	Borrower b borrowed money.
D_b	The money deadline for borrowing money that the borrower b borrows.
C_b	The credit score of the borrower b.
C_g	The credit score of the guarantee corporation g.
W_b	The credit weights of the borrower b.
W_g	The credit weights of the guarantee corporation g.
$C(M_b, D_b)$	This function will return the minimum credit score that can be borrowed.
$E(D_b)$	Expire function will return the expired date that the borrower have to repay.

4. Platform: The platform is established on the basis of smart contracts, with which it can store energy, execute programs, and reach a consensus. The smart contract also calculates the credit score of the borrower when the borrower attempts to borrow energy by using the following equation:

$$C(M_b, D_b) \leq C_b \cdot W_b + C_g \cdot W_g \qquad (1)$$

(1) Setup Phase
In this phase, the system establishes a user wallet address and a smart contract address and chooses a guarantee corporation. The entire process is illustrated in **Fig.1**.

- *Step 1:* The platform provider chooses the system parameters ($C(M_b, D_b)$, C_b, W_b, C_g, W_g) and prepares the smart contract and then publishes them.
- *Step 2:* Users initialize their private keys and wallet addresses. The platform provider also selects some trusted users to be members of a guaranteed corporation to help the platform review borrowers' scores and issue credit scores.

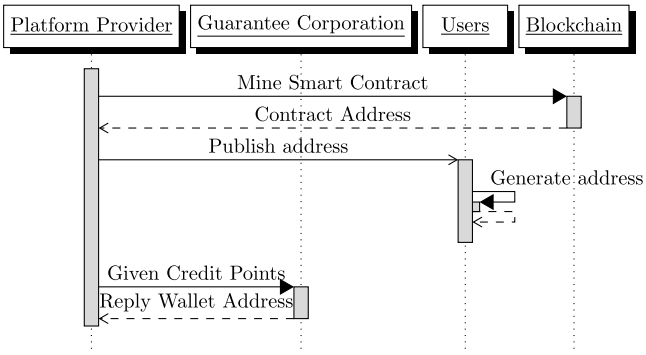

Fig.1: Setup Phase

- *Step 3:* Finally, the platform transfers the credit scores to the guaranteed corporation, and the guaranteed corporation returns the corresponding wallet addresses to the platform provider.

(2) Lend Phase
Before loaners lend energy on the platform in this phase, some steps are implemented, which are described as follows.

- *Step 1:* When users attempt to borrow energy on the platform, they must first find a guarantee corporation that is willing to endorse them. The guaranteed corporation reviews this user's loan records and remaining loan repayment amount.
- *Step 2:* The borrower receives a credit score and a zero-knowledge token that can serve as proof that the borrower has undergone review by a guarantee corporation.
- *Step 3:* The borrowers send their zero-knowledge token and borrowed amount to the smart contract on the energy platform. The smart contract can execute a zero-knowledge proof for the guarantee corporation and allow energy to be borrowed if the proof is valid.
- *Step 4:* The smart contract on the platform evaluates the borrower's credit scores by using Formula (2) and establishes an expiration date by adopting $E(D_b)$.

$$C(M_b, D_b) \leq C_b \cdot W_b + C_g \cdot W_g \qquad (2)$$

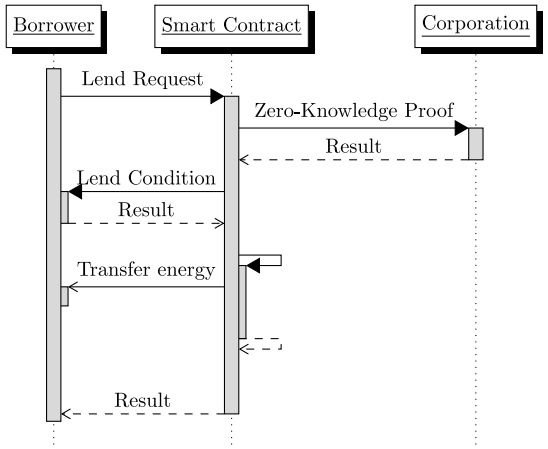

Fig.2: Lend Phase

(3) Repay Phase
After the loan result has been returned, the borrower must check whether the loan must be repaid. For this phase, we demonstrate how the borrower's credit scores can be increased and how their energy loan can be repaid.

- *Step 1:* The borrower forwards their energy and token to the energy platform. After they have been received, the platform checks whether the energy amount matches that on the token. If it does, then the energy is placed in energy storage.
- *Step 2:* If no disputes have occurred, then the credit scores of the borrower and corporations are increased, and the borrower can subsequently return the borrowed energy by the expiration date.

(4) Tracing Phase
If the borrower cannot or does not agree to repay the energy, the borrower's guaranteed corporation publishes their identity to the platform in the smart grid. The platform then punishes the guaranteed corporation and the borrower by reducing their credit scores or adding to the repayment amount for the borrowed energy.

- *Step 1:* When the platform registers that the loan time has expired, it identifies the guarantee corporation and notifies the corporation to help determine the borrower's identity.
- *Step 2:* The guarantee corporation then decrypts the identity of the borrower in question and publishes it to the public board of the blockchain network on the smart grid. Additionally, this guarantee corporation adds the borrower's identity to the block list and pays a fine for the borrower not returning the loan amount by the specified expiration date.

4. CONCLUSION

In this paper, we propose an anonymous energy-lending system in which smart contracts are employed in a smart grid with a zero-knowledge proof. This system allows users to make energy transactions and lend energy without the need for trusted third parties.

REFERENCES

1) N. Z. Aitzhan and D. Svetinovic. Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. *IEEE Transactions on Dependable and Secure Computing*, 15(5):840–852, 2018.

2) A. Dorri, F. Luo, S. S. Kanhere, R. Jurdak, and Z. Y. Dong. Spb: a secure private blockchain-based solution for distributed energy trading. *IEEE Communications Magazine*, 57(7):120–126, 2019.

3) P. S. R. Garcia and J. H. Kleinschmidt. Sharing health and wellness data with blockchain and smart contracts. *IEEE Latin America Transactions*, 18(06):1026–1033, 2020. DOI: 10.1109/TLA.2020.9099679.

4) W. Hou, L. Guo, and Z. Ning. Local electricity storage for blockchain-based energy trading in industrial internet of things. *IEEE Transactions on Industrial Informatics*, 15(6):3610–3619, 2019.

5) Z. Li, J. Kang, R. Yu, D. Ye, Q. Deng, and Y. Zhang. Consortium blockchain for secure energy trading in industrial internet of things. *IEEE Transactions on Industrial Informatics*, 14(8):3690–3700, 2018. DOI: 10.1109/TII.2017.2786307.

6) J. M. Montes, C. E. Ramirez, M. C. Gutierrez, and V. M. Larios. Smart contracts for supply chain applicable to smart cities daily operations. In *2019 IEEE International Smart Cities Conference (ISC2)*, pages 565–570, 2019. DOI: 10.1109/ISC246665.2019.9071650.

7) O. Novo. Blockchain meets iot: an architecture for scalable access management in iot. *IEEE Internet of Things Journal*, 5(2):1184–1195, 2018. DOI: 10.1109/JIOT.2018.2812239.

8) L. Xuefeng and W. Zhao. Using crowdfunding in an innovative way: a case study from a chinese crowdfunding platform. In *2018 Portland International Conference on Management of Engineering and Technology (PICMET)*, pages 1–9, 2018. DOI: 10.23919/PICMET.2018.8481838.