A New Way of Mobile Energy Trading

Chaoyue Tan[1], Yuling Chen[1,2(✉)], Xiaojun Ren[1,2], and Changgen Peng[1]

[1] State Key Laboratory of Public Big Data, College of Computer Science and Technology, Guizhou University, Guiyang, China
Ylchen3@gzu.edu.cn

[2] Block Chain Laboratory of Agricultural Vegetables, Weifang University of Science and Technology, Shouguang 262700, China

Abstract. Current blockchain-based energy trading models raise serious concerns regarding the high and capped transaction latency and expensive service charges. In this study, a mobile energy trading scheme based on lightning network is presented. The focal point of the scheme lies in transfer of value occurs off-blockchain, which addresses the problem of transaction latency. Micropayment channels create a communication between two parties to update balances constantly, deferring what is broadcast to the blockchain in a single transaction netting out the total balance between those two parties. The found security is guaranteed by committing funds into a multisignature address. Additionally, a security analysis is conducted within the context of the proposed model to identify potential vulnerabilities.

Keywords: Blockchain · Lightning network · Mobile energy trading · Off-blockchain · Transaction latency

1 Introduction

In the mobile energy transaction scenario, a microgrid or distributed generation (DG) with small-scale and decentralized transaction characteristics can participate in the electricity trading market as a seller or buyer of electricity [1]. With the rapid expansion of the volume of distributed energy transactions, issues such as privacy leakage and low efficiency of transactions have been increasingly prominent. Due to the distributed structure and decentralization of the blockchain, it is similar to distributed energy transactions. The combination of energy trading provides a new development direction for energy trading [2]. Chen et al. [3] discussed the use of energy blockchain in the energy field and proposed development proposals based on the feature of energy transition trend and blockchain technology. Wang et al. [4] designed a blockchain-based EV charging pile sharing platform, and improved the transaction mechanism and process by using smart contracts. Zhang et al. [5] proposed a blockchain electric vehicle charging model which including three-layer distribution algorithm for optimal scheduling of electric vehicle electrical changing station, also verify the applicability of the model to distributed grid layout.

J. Xiong et al. (Eds.): MobiMedia 2021, LNICST 394, pp. 123–132, 2021.
https://doi.org/10.1007/978-3-030-89814-4_9

At present, the consensus schemes and network architecture of existing solutions are decentralized. Due to the lack of synergy and high efficiency among various chains, the large-scale application of new energy and the use of marketization are greatly restricted [6]. In 2016, the storage capacity of each block has approached 1 MB, which means that some transactions could not be packaged in the block in time and energy nodes need more time to confirm these transactions [7]. With the development of decentralized applications, there is an urgent need to modify the code of blockchain to improve the processing capacity and ensure the scalability of blockchain [8], e.g. Side Chain [9] and Block Slicing [10].

Lightning network is a decentralized trading network, which has been proven that it has strong adaptability to high-frequency transaction scenarios, can improve its scalability and execute massive transactions in a real-time way [11]. The author in reference [6] studied the development status of lightning network and its possible non-monetary uses, meanwhile created a new business model based on lightning applications (LAPPs), micro-channel payment and small transactions. The author in reference [12] discusses the requirements that need to be fulfilled to properly support micropayment in IoT, and further the extent to which different blockchain technologies can fulfill those requirements. As well as proves that the performance of Lightning network is superior to traditional blockchain solutions. Based on blockchain, lightning network and smart contract technology, the author in reference [13] proposed a charging pile sharing economy model, which points out that builds a blockchain-enabled energy trading platform is possible.

Generally, according to the backdrop discussed above, in this paper, we adopt lightning network to construct an off-chain bidirectional payment channel, which enables the buyer node to pay to seller nodes directly, and propose a mobile energy trading scheme. And then, we utilize multi-signature and a series of decrementing timelocks to ensure the security of the payment channel. Finally, we conduct a comprehensive experimental evaluation to evaluate the trading performance. Experimental evaluations show the effectiveness of the proposed mobile energy trading scheme by comparison with other schemes. The main contributions of this paper are as follows:

1. We propose a mobile energy trading scheme based on lightning network that can improve trading efficiency remarkably and decrease service charge by off-chain transactions.
2. Our scheme combines Lightning Network and energy transaction, which gives a new way to small high-frequency energy trading.

The rest of the paper is organized as follows. Section 2 gives some preliminaries. Section 3 gives the details of our proposed scheme. Section 4 provides some experimental results and evaluation analysis. Finally, Sect. 5 concludes the paper.

2 Preliminaries

2.1 Lightning Network

There are two core concepts of lightning network: Recoverable Sequence Maturity Contract (RSMC) and Hashed Time Lock Contract (HTLC). Assuming that there exists

a micro-payment channel between two entities, before execute the trading operation, these entities will pre-deposit funds in the micro-payment channel, and then the funds allocation scheme will be confirmed by both entities in every subsequent transaction, the old version is signed for cancellation operation. When a transaction finished, the final transaction result with signatures of the entities will be broadcast to the blockchain network, and then the funds will be pay to the wallet address of both parties after the final confirmation.

There are two types of creation payment channel: direct payment channel and indirect payment channel. The direct payment channel means that energy nodes of a transaction apply for a multi-signed address on the blockchain and pre-deposit funds. The indirect payment channel means that energy nodes of a transaction build a payment channel with the help of middle nodes which have direct payment channel. The update of the payment channel refers to that both parties modify and record the new proportion of funds in the multi-signature address according to the transaction situation, and use their private keys to confirm. After each update of the proportion of funds, energy nodes will generate a new private key for the next record confirmation. When the transaction is over, the two parties will broadcast the final transaction results to the block chain for capital settlement, then closing the trading channel.

2.2 Multiple Short Signature Scheme [14]

Initialization: Key generation center (KGC) sets k as the security parameter, G_1 and G_2 are cyclic groups of order Q which is a large prime, P is a generator of G_1, e:$G_1 \times G_1 \rightarrow G_2$ is a safe bilinear mapping. Select the random number s as the master key of the system and calculate the public key $P_{pub} = sP$, use it as the main public key of the system, then select two collision-resistant Hash functions $H_1 : \{0, 1)^* \rightarrow Z_q^*$, $H_2 : \{0, 1)^*$. KGC public system parameters: $\{q, P, e, G_1, G_2, P_{pub} H_1, H_2\}$. And keep the system master key s secret.

Key Generation: Users register with KGC, which assigns each user a uniquely identify ID and randomly selects a key to generate a tag $K_{ID} \in Z_q^*$, Generate the user private key $x_{ID} = sH_1(ID, K_{ID}, s)$, Calculate the public key $y_{ID} = x_{ID}P$.

Multiple Signature: Multiple signatures for M users $L = \{U_1, U_2, \ldots U_M\}$, Their identity sets are $L_{ID} = \{ID_1, ID_2, \ldots ID_M\}$, The specific signature steps are as follows:

a. U_1 signs the message m and calculates $h = H_2(m)$, $S_1 = ID_{1xID_1 h}$, send identify ID_1, message m, partial signature S_1 to the next user U_2.
b. After received message, U_2 firstly verifies validity of signature, and then sign.

① compute $h = H_2(m)$.
② Verify whether $e(S_1, P) = e(h, ID_{1yID_1})$ is true, if not, verification failed and return FALSE.
③ compute $S_2 = S_1 + ID_{2xID_2}, h$, send ID_1, ID_2, m and Part of the signature S_2 to next user U_3.

c. Multiple signature verification: user verifies the multiple signature *SM* of the given message *m*, and the correctness of the signature algorithm is verified as follows:

$$e(S_M, P) = e(\sum_{i=1}^{M} ID_i x_{ID_i}, h, P) = e(h \sum_{i=1}^{M} ID_i y_{ID_I})$$

3 The Proposed Scheme

3.1 System Model

The proposed scheme mainly includes two different entities: users and charging piles. Each user chooses different states, charge or discharge, according to current energy status. Charging piles include energy providers, community shared charging piles, shopping mall charging piles, etc. The parameters involved in our proposed scheme are shown in Table 1:

Table 1. Parameters

Description	Name
User	U_i
Distributed generation	*DG*
Charging piles	*CP*
Retail price	*S_EP*
Electricity sales	*ES*
Purchase tariff	*P_EP*
Electricity Purchasing	*EP*
Volume of electricity sold	*C_ES*
Volume of electricity Purchasing	*C_EP*

The main structure of our scheme is shown in Fig. 1. All participants, distributed generations (*DGs*), the charging piles (*CPs*), users, need to register before they trade so they can query some information of themselves and other registrants. When completed registration process, the electricity sales quotation *S_EP* and the electricity sales ES are submitted to the blockchain in each transaction cycle, while the user submits the electricity purchase quotation *P_EP* and the electricity purchase *EP*. The smart contract matches the quotations of both parties according to the quotation matching mechanism defined by the system, and announces transaction information, including the current selling price, buying price, and transaction price. Successfully matched transaction parties will issue transaction settlement certificates through the Lightning Network, including transaction electricity sales *C_ES* and transaction electricity purchase fees *C_EP*, as transaction vouchers, which will be uploaded to the blockchain after the transaction is completed for redistribution of the capital ratio and returned to the accounts of both parties.

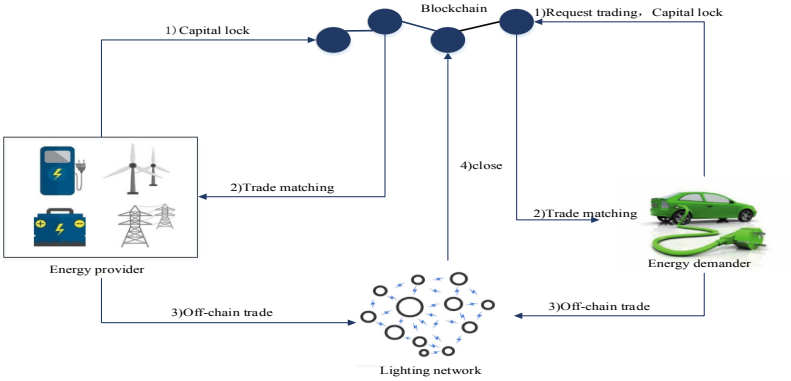

Fig. 1. System model of our proposed scheme

3.2 Registration

This part is divided into user registration and charging pile registration. 1) User registration: users login to ethereum through mobile terminals such as mobile phones to register. After registration, each user gets a unique *ID*. 2) Charging pile registration: the company to which the charging pile belongs will uniformly register each charging pile, and the smart contract will calculate according to the power of the charging pile and lock the corresponding funds on the blockchain. Similarly, each charging pile also has a corresponding identity Identification *ID*. The detail process of registration shows is Table 2.

Table 2 . Registration steps

Registration:	
Step1	KGC assign a unique identity ID to the user or the charging pile, select the private key randomly to generate the tag K_{ID}
Step2	Generate the user private key $x_{ID} = sH_1(ID, K_{ID}, s)$
Step3	Calculate the public key $y_{ID} = x_{ID}P$
Step4	*KGC* send the corresponding key to the user

3.3 Transaction Application

After registration, the user can log in to the Ethernet to initiate a transaction request and retrieve whether there is a transaction channel between both parties. If exists, the smart contract locks the corresponding funds on the blockchain according to the charge or discharge amount provided by the user. If does not exist, the user chooses whether to build a payment channel with the energy provider according to his own wishes. If the user chooses to build a payment channel, the payment channel is built according to the smart contract shown in Table 3, and if not, the best payment channel is matched for both parties in the transaction.

Table 3. Smart contract

Contract:	
Step1	Building *Founding Transaction (FT)*: pre-deposit funds in multi-signed address User & Sale, privacy key sign;
Step2	$U_i$building *Commitment Transaction1a (C1a):* The transaction contains two outputs that are used to redeem the funds they have locked up; First output: *User2 & Sale*, set *sequence number* = *50*, Used to control the return of funds to both sides of the transaction wallet address time, when *C1a* is triggered, the funds locked in FT will be returned to the Sale wallet address on a delayed basis; Second output: *Sale,* when *C1a* is triggered,the funds locked in FT will be returned to the Sale wallet address immediately; * The execution condition of this transaction is that User quits the transaction before the transaction ends;
Step3	*DG* or *CP* constructs *Commitment Transaction1b (C1b);*
Step4	*DG* or *CP* sign *C1a then send to* U_i, U_i*sign C1b* and send to *DG* or *CP;*
Step5	Broadcast *Founding Transaction (FT)* to blockchain;

3.4 Off-Chain Transaction

When there is no payment channel between the two parties, the Lightning Network matches the best payment channel. After the matching is successful, the two parties will conduct the transaction through the intermediate node. The successful matching is that the transaction receiver sends the secret *R* to the transaction initiator within the specified time. That is, to verify the authenticity of the intermediate node, both parties to the transaction will pass a secret *R* through the intermediate node within a specified time, and start the transaction after successful verification. The transaction process is shown in Fig. 2:

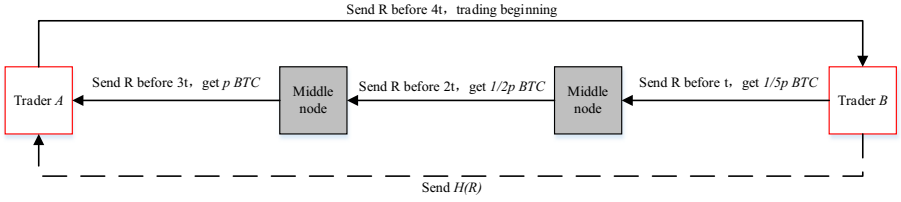

Fig. 2. Off-chain transaction

Price matching mechanism. This mechanism sorts the seller's quotations from low to high, and sorts the buyers' quotations from high to low. When the quotations are the same, they are sorted according to the time of submission. Among them, the optimal selling price (*OSR*) is the seller's lowest price, and the optimal buying price (*OBR*) is the buyer's highest price. When *OBR* is greater than *OSR*, the transaction can be conducted. Suppose that the lowest quotation of the seller is P_{min}, the highest quotation of the

buyer is P_{max}, and the transaction price is $P_{fin} = \frac{P_{min}+P_{max}}{2}$. Each time the matching is completed, the buyer and the seller can re-adjust the price according to their own conditions for the next matching.

4 Analysis

4.1 Security Analysis

Anti-tampering attacks. The transaction mode of this agreement is to record each transaction and use the private key to sign for confirmation, upload the final transaction result to the blockchain for proportional distribution of funds. In each Transaction update, the private key recorded last time will be sent to the other party to construct a Breach Remedy Transaction, and attackers will upload the outdated Commitment Transaction record to the blockchain to gain benefits. As shown in Fig. 3, when a malicious attacker broadcasts an out-of-date Transaction certificate to the blockchain, the other party will immediately know and sign a Breach Remedy Transaction 1A with the private key and broadcast it to the blockchain. Due to the sequence number = 50 in the out-of-date Transaction certificate, it will delay getting its own funds for 50 blocks. An honest trader will be broadcast to the blockchain and immediately receive all the money.

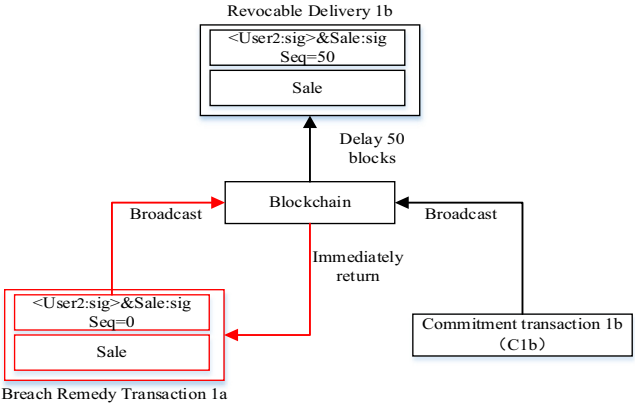

Fig. 3. Anti-tampering attacks

4.2 Transaction Performance Analysis

The size of a block in the Bitcoin blockchain is about 1M, and each transaction is about 250 bytes, which means there are about 4194 transactions in one block, so the transaction throughput of the blockchain is about 7 transactions per second. In addition, the transaction fee in the blockchain is charged by bytes, so the transaction fee is about from 0.0001 to 0.0005 BTC for one transaction [15]. Each transaction needs to wait for confirmation of 6 blocks before it is confirmed to be valid. If the transaction is

small high-frequency transaction like energy trading, the waiting time will be longer, because the miners give priority to transactions with higher fees according to the level of transaction fees. When the two parties have a payment channel, they can conduct transactions directly through the payment channel without any commission. If there is no payment channel between the two parties, the transfer through the intermediate node only needs to pay a small fee to the intermediate node. However, when several small transactions are carried out on the blockchain, the fee will be much higher than that of the Lightning network (Table 4).

Table 4 . Trading contrast

Trading scheme	Trading cost	Trade confirmation speed	Handling capacity
Blockchain-based scheme	0.0001–0.0005BTC	60 min	About seven strokes per second
Our scheme	Petty handling charge	instant confirmation	The more trades, the faster

Table 5 shows the comparison of the mobile energy trading protocol in the proposed scheme and the existing protocol. Comparing from the Transaction performance, fairness of transaction, and key security. Here, "√" satisfies the performance and " ×" dissatisfies the performance.

Table 5. Trading contrast

Trading scheme	Transaction performance	Fairness of transaction	Defense MITM attack
Ayman et al. [16]	About seven strokes per second	√	×
Nurzhan et al. [17]	uncertain	√	×
Our scheme	Petty handling charge	√	√

5 Conclusion

In this paper, we have explored the opportunities brought by lightning network to empower energy trading based on the existing literature in the field, and builds a mobile energy trading solution based on lightning network. Our scheme states out a new way of energy trading. Particularly, we have first provided a bidirectional payment channels for small high-frequency transactions like energy trading. We have then analyzed in detail the limitation of blockchain for energy trading and expound the whole process of off-chain trading. Through the comprehensive analyze, we have proved that our scheme can

reduce the block chain overload caused by small high-frequency transactions, moreover it avoids high transaction fees caused by mining and long waiting time for transaction confirmation, meanwhile, it greatly improves trading performance. In addition, due to the existence of Multi-signature, Hash Time Lock and Sequence Number, the security of this scheme is guaranteed. Bidirectional payment channels improve scalability of blockchain but it has limitations. Fee policies of intermediate nodes may influence the whole network, our next work is exploring how to balance fee of intermediate.

Acknowledgement. This work is financially supported by the National Natural Science Foundation of China under Grant No. 61962009. In part by the Major Scientific and Technological Special Project of GuiZhou Province under Grant No. 20183001. and in part by the Open Funding of GuiZhou Provincial Key Laboratory of Public Big Data under Grant No. 2018BDKFJJ003 and No. 2019BDKFJJ011.

References

1. Wang, J., Zhou, N., Wang, Q., et al.: Elecricity direct transaction mode and stratey in microgrid based on blockchain and continuous double auction mechanism. Proc. CSEE **38**(17), 5072-5084+5304 (2018)
2. Xu, J., Ma, L.: Application of block chain technology in distributed energy trading. Electr. Power Autom. Equipment **40**(08), 17-22+30 (2020)
3. Chen, Y., Zhao, Q., Gong, Y., et al.: Discussion on electric vehicle charging transaction based on block chain technology. Electr. Power Eng. Technol. **39**(06), 2–7 (2020)
4. Wang, G., Yang, J., Wang, S., et al.: Distributed optimization of power grid considering EV transfer scheduling and block-chain data storage. Autom. Electr. Power Syst. **43**(08), 110–116 (2019)
5. Zhang, X., Liu, C., Chai, K.K., Poslad, S.: A privacy-preserving consensus mechanism for an electric vehicle charging scheme. J. Network Comput. Appl. **174** (2021)
6. Ren, A., Feng, L., Cheong, S., et al.: Optimal fee structure for efficient lightning networks. In: 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS). IEEE (2018)
7. Yu, H., Zhang, Z., Liu, J.: Research on scaling technology of bitcoin blockchain. J. Comput. Res. Dev. **54**(10), 2390–2403 (2017)
8. Harris, B.: Bitcoin and Lightning Network on Raspberry Pi. Apress, Berkeley, CA (2019)
9. Singh, A., Click, K., Parizi, R.M., Zhang, Q., Dehghantanha, A., Choo, K.-K.: Sidechain technologies in blockchain networks: an examination and state-of-the-art review. J. Network Comput. Appl. **149**, 102471 (2020)
10. Erdin, E., Cebe, M., Akkaya, K., Solak, S., Bulut, E., Uluagac, S.: A Bitcoin payment network with reduced transaction fees and confirmation times. Comput. Networks **172**, 107098 (2020)
11. Stasi, G., Avallone, S., Canonico, R., et al.: routing payments on the lightning network. In: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData). IEEE (2018)
12. Robert, J., Kubler, S., Ghatpande, S.: Enhanced Lightning Network (off-chain)-based micropayment in IoT ecosystems. Future Gener. Comput. Syst. **112**, 283–296 (2020)
13. Linghai, Q., Xue, L., Bing, Q., et al.: Shared economy model of charging pile based on block chain ecosystem. Electr. Power Constr. **38**(09), 1–7 (2017)

14. Liming, Z., Lanlan, C., Qing, Z.: Short multi-signature scheme for distributed approval workflow. Appl. Res. Comput. **37**(02), 521–525 (2020)
15. Fang, L., Zhuoran, L., He, Z.: Research on the progress in cross-chain technology of blockchains. J. Software **30**(6), 1649–1660 (2019)
16. Esmat, A., de Vos, M., Ghiassi-Farrokhfal, Y., Palensky, P., Epema, D.: A novel decentralized platform for peer-to-peer energy trading market with blockchain technology. Appl. Energy **282**, 116123 (2021). https://doi.org/10.1016/j.apenergy.2020.116123
17. Nurzhan, Z., Davor, S.: Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams. IEEE Trans. Depend. Secure Comput. **15**(1), 840–852 (2016)