A Blockchain Approach for the Future Renewable Energy Transaction

Sandhi Rahmadika1, Diena Rauda Ramdania2, and Maisevli Harika3

1Interdisciplinary Program of Information Security, Graduate School PKNU Pukyong National University, Busan, South Korea
2Informatics Engineering, UIN Sunan Gunung Djati Bandung, Indonesia
3Computer Engineering and Informatics, Politeknik Negeri Bandung, Indonesia

Abstract. Blockchain technology holds great promise to rewire the current financial system which relies on the third party. Every transaction is recorded in a secure and transparent for the parties in the blockchain network. Blockchain technology in the energy sector becomes an interesting topic among researchers at this moment. The use of blockchain allows producers and consumers to trade energy transactions through smart grids because of a decentralized energy trading system. The trading activities without a third party involved would reduce the cost of a transaction thus it brings to a new level of quality of service in the trading system. In this paper, we propose an architectural model for decentralized energy trading system among the neighbors that allows the producer who has the surplus energy to conduct a trading activity with his/her neighbors. The transactions manage by the miners in the same blockchain network. Moreover, we analyze the security issues from various attacks and presenting the performance of the selected attack that might occur in the model.

1. Introduction
The majority of the financial structure is a centralized form including the trading system. The centralized system relies on a third party (middleman) to process the transaction between the payee and the payer [1]. Some weaknesses are still found in centralized trading systems and affect consumer satisfaction because they can interfere with trading activities [2]. Moreover, the privacy of the consumer might be a problem in the decentralized system as shown by Wood and Newborough [3] that revealed the pattern by energy provider that allows predicting the behavior of consumers by modeling their daily activities based on the energy consumption. Thus, the centralized system becomes the main key for the energy providers. Researchers have done a lot of research related to trade. In the energy sector the trading system using blockchain technology was also developed.
The renewable energy and decentralized blockchain (see Figure 1) are two technologies that are worth betting on for the future [4]. It brings many advantages such as cost reduction, effectivity, and make the process more efficient. In order to guarantee the credibility of transaction security, trading can be done if the buyer's identity has been verified with a cryptographic module embedded in the system.
In an industry perspective, blockchain has many advantages such as flexibility and scalability. Blockchain also provides opportunities for energy producers to sell their surplus energy to their neighbors. In addition, in a decentralized blockchain system, third-party services are no longer needed. As such, blockchain allows an increase in terms of transaction speed, quality of trading system services, and reduced costs. Instead of only consuming energy, the use of blockchain technology can provide energy trading opportunities by producers who have excess energy.

In this paper, we propose a model for energy trading using a decentralized blockchain scheme among neighbors. The producers who want to sell their energy announce the amount of energy and the price on the bid board and then later be invisible to the consumers in the same blockchain network. The consumer who interests in bidding then creates a communication with the producer. If the agreement is reached, the transaction will be executed by the miners in the peer-to-peer network. Additionally, we highlight the security issues that might arise in our model by presenting the performance of the dishonest miners in term of selfish mining attack. The goal of the attacker is to find the weaknesses of the system by attacking the structure of the peer-to-peer network, create a dishonest pool, and many others.

2. Related Work

In this section, we present the prior research related to the decentralized energy trading by using blockchain technology that is linked to our work. A concept of decentralized energy trading through multi-signatures and the anonymous messaging stream has been proposed by Aitzhan and Davor [1]. The system is built by following the Bitcoin protocol via peer-to-peer messages (anonymity transaction). There are two types of communication in the system that is sending a private message and broadcast the message. The algorithm of energy trading between the payer and payee is also given in the paper. In the case, there are any problems during the transaction, the Distribution System Operator (DSO) in charge to solve the problem. However, the authors did not elaborate the attacker performance such as selfish mining, eclipse attack and double spending attack in the model.

The green blockchain concept for managing the energy was proposed by Imbault et.al [4] that explored and created a green certificate in eco-district. There are no information details related to the security issues in this system. Recently, Danzi et.al [5] have shown a concept of distributed proportional-fairness control via blockchain smart contract. The aim of the study is to enhance the efficiency, especially for the transmission losses in the smart grid. The research goal is to enhance the efficiency of the renewable energy (reduce the losses during transmission). The security issues on the blockchain applied are out of the topic in this research. Therefore, inspired by the predecessor related work, we propose a scheme for decentralized energy trading system using blockchain technology in a peer-to-peer network. In addition, we elaborate the performance of dishonest miner in the model.

3. Preliminaries

3.1. Fundamental of Blockchain and Peer-to-peer Network

Blockchain technology supports a new generation of transactional applications and streamlined business processes by establishing the trust, accountability, and transparency which are essential to modern
commerce [6]. A blockchain technology is a data structure used to create a decentralized ledger and composed in a serialized manner. One block of sequel blockchain contains a set of information that refers to the transactions and the hash value from the previous block, the timestamp, block reward, the number of blocks, and many others. The previous information of the transaction that later becomes an input for the next transaction thus forms a block.

Blockchain can hold the information and set the rules on how the information is updated. This technology can prevent fraud and corruption, yet it can be used to solve many other problems depending on how people implement and use it. Blockchain technology can support a new generation of transactional applications and streamlined business processes by establishing the trust and transparency that are essential to modern commerce with the guarantee of security based on several cryptographic protocols [7]. A blockchain scheme allows a digital data to be propagated to the network, thus every party in the network has the same version of the data. The new block in Bitcoin can be added to the blockchain if only the miner successfully solves the hash puzzle (proof-of-work) and reach the consensus for every transaction. A bitcoin address is an identifier of 26 to 35 alphanumeric characters and the address is computed from an Elliptic Curve Digital Signature Algorithm (ECDSA) public key for which the address owner knows the corresponding private key by using a transformation based on hash function. In typical for the decentralized system (see Fig. 2) there is no any single failure from a third party because it eliminates the involvement of a third party to control the entire system. It also enables a peer to broadcasts the information to another peer on the network [8].

The network in peer-to-peer is connected by default. The peers provide incoming TCP connections (port 8333 for Bitcoin) to refer to the other peers. A peer in the Bitcoin is typically not aware of other full nodes’ IP addresses and it is maintained by the community such as Bitcoin members which provide a dynamic system that generates automatically IP addresses of the peers by frequently checking the node in the same network [9]. A peer-to-peer transaction is done by the owner which transfers some of the cryptocurrencies to the next owner by signing a hash value from the previous transaction. Even though the peer-to-peer network has a favorable feature such as fault-tolerance but the structure of the peer-to-peer is still vulnerable. For example, the parties need to be aware of the risk from the propagation of dishonest miner code, the legality to tamper the data and any other attack within the peer-to-peer network. Hence, in this paper, we discuss various attacks in our model (blockchain in general) e.g. the attack on the structure of a peer-to-peer network such as Eclipse attack and Sybil attack which somehow manipulate the peer-to-peer network and will be able to get any advantages which would harm the victim.

3.2. The Core of Node Join in P2P

In the peer-to-peer (P2P) overlay network of blockchain system, the fundamental problem is related to the how efficient to find a peer that shares a requested message yet the way to connect from one node to another node. The Chord protocol in the peer-to-peer network supports the communication system among the nodes, especially when the node propagates the data block (computation value of hash) to the entire blockchain network. The Chord protocol has some characteristic such as simplicity in provable the value and performance context, and it only needs a few nodes within the routing overlay [10].

![Figure 2](image-url)
The Chord based distributed system manages the information system to join and leave the system, whilst the protocol possesses the hash properties as follows:

1. Pre-image resistance can be defined such as \( r = [0.1]^r \) message, \( r = [H(Z); z = H]\) \(-1\) (r)
2. 2nd pre-image resistance, let define by message z to find some: \( x' \) s.t. \( H(x') = H(z) \). It must be very difficult to find the original value.
3. Collision resistance, two messages m1, m2. The probability of hashes are equal \( P(H(m1) = H(m2)) \) must be very small.

![Figure 3. Chord ring (m = 6)](image)

The chord protocol assigns each node and keys an m-bit identifier using the hash algorithm (SHA-1, SHA-256). The node as the result of the hash IP-address and the key is simply the hash key. The identifier is ordered on an identifier circle module 2m as shown in Figure 3, the chord ring literally the circle of numbers from 0 to 2m-1. The main function of the chord protocol is a query value from a client to find a successor (k). In the decentralized energy trading system, the chord-based distributed system is used to know the location of the node among the neighbors which is more efficient.

4. Desentralized Energy Trading System

In this section, we show examples of existing and most well-known blockchain technologies in the energy area. As following, we present our architecture model and the algorithm of transaction among the parties.

4.1. LO3 Peer-to-Peer Energy

Blockchain changes the way the transaction between the payee and the payer from a centralized structure (energy companies, banks) toward the decentralized structure. In the decentralized energy trading system, the transaction is carried out directly between producer and the consumer. All of the information related to the trading activity is stored on blockchain storage and distributed to the entire network. The prominent example of blockchain in the energy sector is LO3 peer-to-peer energy (see Fig. 4). This system has implemented by selling the electricity to the nearest neighbors. The prediction for calculations of market value shows that the market is worth $5 billion a year [11].

The system can be described as a solution that combines the security and transparency between the neighbors that is offered by blockchain concept. The decentralized model of the trading system directly makes a clean transaction, more accessible and many other advantages. By leveraging the LO3 model, the parties download the mobile app that lets them join the local microgrid community. Whenever producer wants to sell the electricity to the neighbors, he/she announce the available energy and the price. Once the transaction is complete, then the producer earn the cryptocurrencies, as well the consumer gets the energy.
4.2. Propose Decentralized Model of Energy Trading System

Blockchain technology remedies the problem in the centralized energy trading such as a failure of the third party, reduce the transaction cost yet the consumers have many options. In practice, the equipment e.g. smart grid is necessary to support the trading activity. In this sense, we assume every party in the blockchain network install the smart grid. The households which produce the energy allow transferring the energy to the consumer when he/she earn the cryptocurrencies. The model ensures that producers cannot transfer the same energy twice to the different consumer and vice versa. The consumer is not allowing to use the same coin to purchase the energy (double spending).

The decentralized storage on the blockchain system allows keeping a distribute data, transparency and secure record of energy transaction as well it is tamper-proof from the attacker. In this regard, the attacker is not able to change the content of one block but should change the whole content of the block in the blockchain network which is impossible. The trading system would no longer require the middleman involvement e.g. banks, energy companies to execute the transaction between the traders. In general, the architecture of trading renewable energy system in the peer-to-peer network can be seen in Figure 5.

There are four prosumers which have the surplus energy and willing to sell their energy to the neighbors in need. Whenever the producer wants to sell the energy, he/she announces to the auction board which gives detail information related to the amount of energy that they want to sell and information of the

---

**Figure 4.** Peer-to-peer energy use case [11]

**Figure 5.** Decentralized Energy Trading System

**Figure 6.** Propagating the Record of Transactions
price. One of a node in the network acts as a distributed system operator (DSO) that solving the dispute between the traders likewise, the problem in trading activities e.g. the consumer did transfer the coin but still does not receive the energy from producer. Furthermore, whenever the producer announces the claims of his/her energy in the auction board, the DSO then checkup whether the energy really exists as claimed or not. To obtain the result of data communication during the transaction, we add the additional components.

The components of the network consist of the router, local computer and laptop, switch and wireless router. In the packet of network terms, a router literally can be defined as a device that determines for a packet to be forwarded to the destination point which connects between the networks. In case, there are any requests from the different computer, the router will check the IP address and used as a hash key to direct to the destination. In this system, the router transmits the packet data of record transaction as shown in Fig. 6 from source to another computer in the peer-to-peer network.

The components model in the network architecture performs a key role in supporting the continuity of a system. It has the input and output gateway of the data blocks. In charge of distributing and replicating the data record of a transaction in the peer-to-peer network, the component requires knowledge of data blocks location, as well as ability to fetch data blocks in the appropriate node that contains the requested data and return to the requester. Define \( n_f \) as a time to finish the service since the connection between the node is generated. For the request coming from the node, then a request is random from several nodes. To define the service time \( s \) as follow:

\[
s = \begin{cases} 
  n_f, & \text{if the peer is connected} \\
  n_f + \delta, & \text{if the peer is not connected} 
\end{cases}
\]  
(1)

To manage the I/O of routing overlay in the network, promoting scalability and load balancing capabilities, we assume there is a node manager component which follows the algorithm of the Chord protocol. When a node wishes to be inserted into the network this component generates a new identifier for the node according to the protocol and notify other nodes to make it more accessible. The digital signer component to manage the integrity of new data blocks which contain the information of the transaction. The data integrity is essential since it is maintaining and assuring the accuracy and consistency of data over its entire life-cycle [12].

The status of communication data based on Fig. 6 shows that the success rate is 100% in propagating the data transaction among the parties in the same peer-to-peer network with chord protocol embedded. The average time to broadcast the information to the peers in the network is 2.24ms for 200 byte ICMP echoes (Internet Control Message Protocol). The data source and destination is recorded randomly at n period time. The wireless routers use WPA-PSK and PSK Pass Phrases to connect with other devices and every message is encrypted by using AES (Advanced Encryption Standard). The principle design of AES is based on a substitution-permutation network and a combination of both substitution and permutation technique and then can be applied in software and hardware.

Algorithm 1 presents an energy trading system between the producer, client and the distributed system operator that acts as a third party. The decentralized energy system using blockchain technology open the opportunity for the producers to not only consume the energy but also able to perform the trading activities. Algorithm 1 line 7-9 is an injecting energy process by the producer to the client right after the transaction gets confirmed by the miner. Line 12 is a method to prevent the double spending attack in the trading system. If there is a notification from auction board that producer willing to sell the energy by gives the detail information to the network, then a distributed system operator checks the claimed whether the energy exists or not. Finally, in line 17-21 is a process transfer the energy to the new owner. The distributed system operator will play a role if there is a dispute during the trading.
5. Security Issues, Opportunity, and Limitations
In this session, we elaborate the various attack that might occur in our model (Bitcoin blockchain in general). The intuition of the attacker is to disrupt the decentralized network, manipulating the transaction, and obtain the unfair revenue.

Selfish mining attack – Since this attack is discovered in 2014 by Eyal and Sirer [13], it became one of the most widely researched topics by the experts in various fields. The selfish mining attack shows that Bitcoin is not incentive-compatible as assumed. The key idea of this attack is to find the block as fast as the miner can and keeping the block secret which is invisible to the public network and deliberately forking the chain. The attacker can gain the reward if \(0 \leq \alpha \leq 0.5\). Recently, Sapirshtein, et al. [14] shows the optimal selfish mining strategy by the dishonest miner with only has 0.23 of mining power can obtain the unfair revenue. The selfish miner is totally relying on the resources to find a block. Moreover, the dishonest miner affects the rational miner to join the selfish mining pool because the pool has bigger revenue compare to honest revenue [15].

The simulation of this attack was running between the honest miner and dishonest miner to find a new block in the blockchain network. The honest miner follows the Bitcoin protocol, while the dishonest miner mimics the selfish mining protocol with the variant hash rate (mining power). The goal of the dishonest miner is to discover the new block till becoming the longest chain and gaining the revenue after publishing the block to the public network. In our setting, we arrange the selfish miners compete with honest miners in 14 days to solving the proof-of-work and discover the new block. The maximum of mining power of selfish miner is 0.4 and the simulation was running randomly from 0.0 through 0.0 for 14 days.

Based on the simulation result in Figure 7, the information related to the block height of the transactions that are conducted by the parties. There are 51 new blocks are successfully added in the blockchain network, whilst during the transaction, there are 4 orphaned blocks and the average block height time is 7.72 minutes. Furthermore, in Figure 8 shows the performance of dishonest miner. There are 12
dishonest miners with different mining power from 0.0 to 0.4. We set the maximum number in 0.4 because if the attacker has mining power 0.51 in one pool, then it is certain they will be able to take over the network. For more details can be seen in Table 1. Once the dishonest miner has 0.322 mining power then it is enough to get the unfair revenue and will be able to gain the revenue larger than it should be. It proves that dishonest miner is not necessary to have 51% mining power to get an unfair revenue.

![Figure 7. Block height of the Transaction](image1)

![Figure 8. The Reward of Selfish Miners](image2)

Table 1. Performance of Selfish miner

| No | Dishonest Miner (DM) | Mining Power | Revenue (Ratio) | SM Succeed? (Y/N) |
|----|----------------------|--------------|-----------------|-------------------|
| 1  | Miner 1              | 0.009        | 0.000           | N                 |
| 2  | Miner 2              | 0.018        | 0.000           | N                 |
| 3  | Miner 3              | 0.019        | 0.000           | N                 |
| 4  | Miner 4              | 0.027        | 0.000           | N                 |
| 5  | Miner 5              | 0.161        | 0.112           | N                 |
| 6  | Miner 6              | 0.181        | 0.112           | N                 |
| 7  | Miner 7              | 0.238        | 0.212           | N                 |
| 8  | Miner 8              | 0.259        | 0.215           | N                 |
| 9  | Miner 9              | 0.287        | 0.388           | N                 |
| 10 | Miner 10             | 0.322        | 0.425           | Y                 |
| 11 | Miner 11             | 0.333        | 0.457           | Y                 |
| 12 | Miner 12             | 0.361        | 0.597           | Y                 |

**Sybil attack** – This attack happens in the peer-to-peer structure of our system. Sybil attack can be thought as a single attacker that somehow able to control several nodes on a peer-to-peer network as shown in Fig. 8. Sybil attack is a very serious threat in the blockchain system that relies on a peer-to-peer structure when the nodes propagate the information to the other nodes in the blockchain network. Therefore, Douceur [16] pointed out that the Sybil attack is always possible to happen in the peer-to-peer structure without a logically centralized authority.

![Figure 9. Sybil Attack that Controls the Victim Node](image3)
Eclipse attack – It can be described as the attacker has an ability to gains control over a network and with the proper manipulation of a peer-to-peer network, the adversary can eclipse a node so that it is only communicating with the attacker's node. Recently, Heilman et al. showed how to attack the Bitcoin over a blockchain system by manipulating the node in the blockchain network [17]. For example, the attacker could possess a large number of IP addresses at his or her disposal and controls a large number of machines (e.g., a botnet). The adversary could be an internet service provider (ISP) or a nation-state adversary. Eclipse entails blinding the view of the victim from the blockchain network. Moreover, the adversary isolates the honest node out of the blockchain network by monopolizing the victim's connection.

There are still many shortcomings in our model. Likewise, we do not elaborate the structure of smart grid used by producer and consumer. The smart grid technologies are supposed to make possible two-way communication between the parties in trading activities. It is a challenge in the future to create a clean energy transaction for the traders.

6. Conclusion
An architecture model for decentralized energy trading system using blockchain technology in the overlay network has been discussed in this paper. The blockchain structure allows the parties to conduct the energy trading activities among the neighbors via the smart grid. With adequate equipment, the model is promising to be developed. Thus, it makes a better and transparent energy transaction with many options for the traders. However, the structure of the peer-to-peer network in the blockchain is still vulnerable to attack. The attackers could manipulate the network, issues the hundreds of fake transactions, and gain the unfair revenue. For the future work, we need to focus more on creating strategies to prevent attacks especially in the structure of the overlay network. Yet, the model of equipment such as smart grid, inverter, and the smart meter is also necessary to be explored.

Acknowledgment
This work was supported by Institute for Information & communications Technology Promotion (IITP) grant funded by the Korea government (MSIT) (No.2017-0-00156, The Development of a Secure Framework and Evaluation Method for Blockchain) and partially supported by the MSIT (Ministry of Science and ICT), Korea, under the ITRC (Information Technology Research Center) support program (IITP-2017-2015-0-00403) supervised by the IITP (Institute for Information & communications Technology Promotion)

References
[1] N. Zhumabekuly Aitzhan and D. Svetinovic, 2016, “Security and Privacy in Decentralized Energy Trading through Multi-signatures, Blockchain and Anonymous Messaging Streams,” IEEE Trans. Dependable Secur. Comput., pp. 1–1.
[2] P. Global, 2017, “Blockchain an Opportunity for Energy Producers and Consumers?” PwC Global Power and Utilities.
[3] G. Wood and M. Newborough, 2003, “Dynamic energy-consumption indicators for domestic appliances: Environment, behaviour and design,” Energy Build., vol. 35, no. 8, pp. 821–841.
[4] F. Imbault, M. Swiatek, R. De Beaufort, and R. Plana, 2017, “The green blockchain: Managing decentralized energy production and consumption,” in Conference Proceedings - 2017 17th IEEE International Conference on Environment and Electrical Engineering and 2017 1st IEEE Industrial and Commercial Power Systems Europe, EEEIC / I and CPS Europe 2017.
[5] A. M. P. Danzi, 2017, “Distributed Proportional-Fairness Control in Microgrids via Blockchain Smart Contracts”.
[6] S. Nakamoto, 2008, “Bitcoin: A Peer-to-Peer Electronic Cash System,” www.bitcoin.org, p. 9.
[7] P. Narayanan, Building Blockchain Projects: Develop real-time DApps using Ethereum and JavaScript. Birmingham-Mumbai: Packt Publishing Ltd.
[8] S. Rahmadika and K.-H. Rhee, 2018, “Blockchain technology for providing an architecture model of decentralized personal health information,” Int. J. Eng. Bus. Manag., vol. 10, pp. 1–12.

[9] H. M. N. D. Bandara and A. P. Jayasumana, 2013, “Collaborative applications over peer-to-peer systems-challenges and solutions,” Peer-to-Peer Netw. Appl., vol. 6, no. 3, pp. 257–276.

[10] “Chord protocol.” [Online]. Available: https://en.wikipedia.org/wiki/Chord_(peer-to-peer).

[11] Exer, 2017, “Business whitepaper”.

[12] S. Rahmadika, P. H. Rusmin, H. Hindersah, and K. H. Rhee, 2017, “Providing data integrity for container dwelling time in the seaport,” in Proceedings - 2016 6th International Annual Engineering Seminar, InAES 2016, pp. 132–137.

[13] I. Eyal and E. G. Sirer, 2014, “Majority is not enough: Bitcoin mining is vulnerable,” in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 8437, pp. 436–454.

[14] A. Sapirshtein, Y. Sompolinsky, and A. Zohar, 2017, “Optimal selfish mining strategies in bitcoin,” in Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), vol. 9603 LNCS, pp. 515–532.

[15] S. Rahmadika, D. R. Ramdania, and M. Harika, 2018, “Security Analysis on the Decentralized Energy Trading System Using Blockchain Technology,” vol. 3, no. 1, pp. 44–47.

[16] J. R. Douceur, 2002, “The Sybil Attack,” pp. 251–260.

[17] E. Heilman, A. Kendler, A. Zohar, and S. Goldberg, 2015, “Eclipse Attacks on Bitcoin’s Peer-to-Peer Network,” USENIX Secur. Symp., pp. 129–144.