JOIN (Jurnal Online Informatika)
Volume 3 No. 1 | Juni 2018 : 44-47
DOI: 10.15575/join.v3i1.207

Security Analysis on the Decentralized Energy Trading System Using Blockchain Technology

Sandi Rahmadika[1], Diena Rauda Ramdania[2], Maisevli Harika[3]
[1]Interdisciplinary Program of Information Security, Graduate School PKNU
Department of IT Convergence and Application Engineering
Pukyong National University, Busan, South Korea
[2]Jurusan Teknik Informatika, Fakultas Sains dan Teknologi,
Universitas Islam Negeri Sunan Gunung Djati Bandung
[3]JTK Politeknik Negeri Bandung, Jawa Barat, Indonesia
[1] sandika@pukyong.ac.kr, [2]diena.rauda@uinsgd.ac.id, [3]maisevli@jtk.polban.ac.id

Abstract- Blockchain turns both currencies and commodities into a digital form without relying on middleman which allows one person to trade with another include trading the renewable energy. Blockchain technology as a secure and low-cost platform to track the billions of eventual transactions in a distributed energy economy has attracted the attention of experts in various fields of science. The current form of centralized energy trading system is still suffering from security concerns, quality of service, and to name a few. A decentralized energy system using blockchain technology allows the parties to create a trading energy transaction via microgrid. The blockchain technology offers the promise of an immutable, single source of truth from multiple sources without a third-party involvement. In this paper, we describe, explore and analyze the prominent implementation of blockchain technology in the energy sector. Furthermore, we analyze the security issues and highlight the performance of several attacks that might be occurred in the proposed system.

***Keywords*- Blockchain, energy trading, microgrid, peer-to-peer network.**

I. INTRODUCTION

The trading of energy systems is evolving towards a more decentralized model that accommodate heterogeneous, competitive energy sources and energy storages systems (ESS). A majority of modern financial infrastructures are centralized and implicate the involvement of a trusted third party, which handles accounts, processes payments and provides security [1]. In general, the centralized trading system still has some drawbacks and becomes the death knell for energy providers. The decentralized as though possess a single point of failure from middleman that may disrupt the trading activities [2] as it affects directly to the consumer satisfaction. Hence, the research related to the trading activities to improve the quality of service has been extensively developed by experts including the trading system using blockchain technology in the energy sector.

At the initial step for trading renewable energy system has been exploring how to integrate and make connections for equipment with distributed energy resource system such as solar energy in a decentralized peer-to-peer network. As it has for centuries, commerce relies on trust and verified identity with cryptography protocol module embedded in the system to make sure the credibility of the data and the other security manners. Start as a cranny system on the market, nowadays it attracts the interest of the experts in several industries [3].

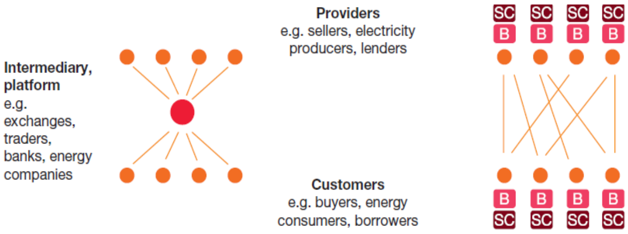
Providers
e.g. sellers, electricity producers, lenders
Intermediary, platform
e.g. exchanges, traders, banks, energy companies
Customers
e.g. buyers, energy consumers, borrowers
SC
B
SC
B
SC
B
SC
B
B
SC
B
SC
B
SC
B
SC

Fig 1. Centralized and decentralized structure

The essence of the decentralized system in the energy sector (see Fig. 1) is based on a powerful idea to organize, properly structure and steer to improve the quality service. It gives many advantages such as flexibility, scalability, and so on. Furthermore, a third party whose service is needed in the industries is no longer necessary in a decentralized blockchain system. A third party whose service is needed in the industries is no longer necessary in a decentralized blockchain system. Henceforth, it allows increasing the speed of transaction, reduces the cost, and improves the quality service of a trading system. Instead of only consume the energy, the blockchain grants the prosumers which have surplus energy to create a trading activity in order to sell his/her energy via smart grid.

The roadmap of the paper is organized as follows. Section II presents the previous work, whilst Section III describes the components of the system such as essential of blockchain, peer-to-peer network and many others. In Section IV, we discuss the prominent example of decentralized energy trading and we present the

Makalah dikirim: 29 Mei 2018; Revisi: 23 Juni 2018; Diterima: 30 Juni 2018; Publish: 30 Juni 2018

architecture of our model. The conclusion and the future work is outlined in Section V.

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 this paper. If there is any dispute during the transaction, the Distribution System Operator (DSO) is able to solve the problems among the parties. 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 is 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.

II. RESEARCH METHOD

A. FUNDAMENTAL OF BLOCKCHAIN

The blockchain network can be described as a data structure used to create the ledgers that contain a lot of information related to the transaction [6]. As it has for centuries, commerce relies on trust and verified identity with cryptography protocol module embedded in the system to make sure the credibility of the data and the other security manners. The timestamp as shown in Figure 2 is used in digital documents in order to prevent the tamper-proof by the attacker. The block in the blockchain is like a seal, if the attacker tries to break the seal, everyone allows to know the action. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin [7]. The hash is produced by running contents of the block in question through a cryptographic hash function e.g. Bitcoin uses SHA-256. An ideal cryptographic hash function can easily produce a hash for any input, but it is difficult to derive the input.

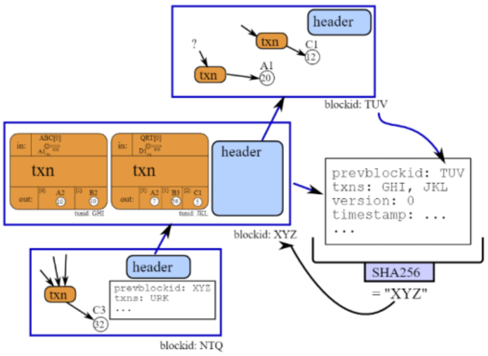

Fig 2. The information a block (transaction)

Table 1. Bitcoin blockheader format

Field	Description	Size
Version	Block Vers.num	4 bytes
Hash-Prev block	Hash of prev.header	32 bytes
Merkle root hash	Tx Merkle root hash	32 bytes
Time	Unix time stamp	4 bytes
nBits	Current difficulty	4 bytes
Nonce	Allows miners search	4 bytes

In various sectors, blockchain is being used to build some purposes such as financial registries, operational registries and one of the most popular one is smart contracts:

a. Financial registries: cryptocurrencies such as Litecoin, Bitcoin, and Dogecoin can be used as an alternative for the real currencies in the blockchain system.
b. Operational registries: blockchain allow tracking and certification of specific products or assets, including renting contracts, land registers and notary deals or votes.
c. Smart contracts (automated actions on the blockchain): is account holding objects and contain several code functions to make decisions, store data and send the cryptocurrencies to the next owner. The smart contract has an ability to execute the code (self-executing).

Proof-of-work in bitcoin, proof-of-stake and so on are various consensus protocols used to keep the blockchain secure [8]. It depends on the consensus protocol, the blocks are created and added to the blockchain differently. In proof of work, blocks are created by a procedure called mining, which keeps the blockchain safe. A probability of finding nNonce of proof H for given target T is:

$$P(H \leq T) = \frac{T}{2^{256}} \qquad (1)$$

The disadvantage of proof-work is related to efficiency that wastes too many computational resources to find the target value (hash puzzle). The hash in PoW begins with a number of zero bits hash (SHA-256) and involves kind of scanning for value when hashing a data.

B. RESILIENT OVERLAY NETWORK

An overlay network capable of delivering content, applications, and services to a global audience is a large distributed system [9]. Chord algorithm in overlay network provides a fast-distributed computation of hash function mapping keys to nodes responsible for them. It uses consistent hashing [10] which has several good properties. With high probability, when a Nth node joins (or leaves) the network, only an O(1/N) fraction of the keys are moved to a different location, this is clearly the minimum necessary to maintain a balanced load [11]. Fig. 3 shows a possible three-layered software structure for a cooperative mirror system. The highest layer would provide an interface to users, including naming.

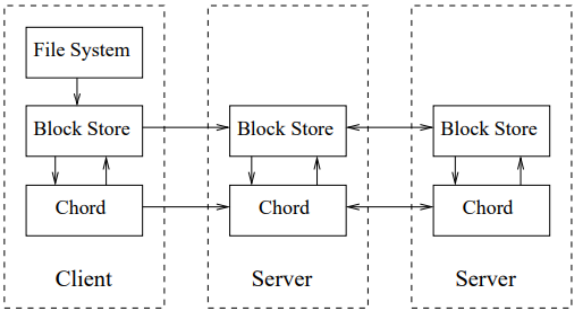

Fig 3. Chord-based distributed system

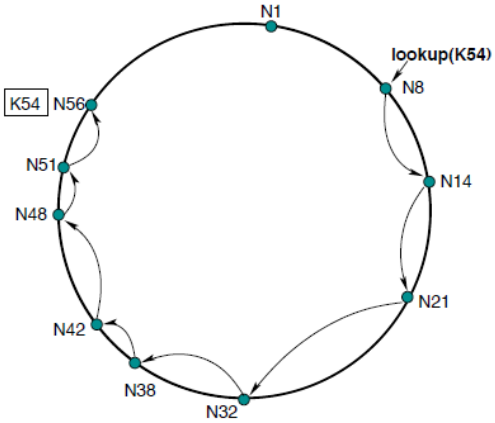

Fig 4. Chord-based distributed system

As shown in Fig. 3 a basic structure of chord algorithm from client to servers. From the client's side, there is a block such as a file system, block store and the chord itself. Whilst, from the server, there are block store and chord that connected to another server and the client. The main usage of the chord protocol is a query value [8] from a client to find a successor (k). This refers to an O(N) query time, and the N is referred to the number of rings applied. In our system model, the chord-based distributed system is used to know the location of the node among the neighbors in the decentralized trading system.

III. RESULT AND DISCUSSION

A. THE MODEL OF DECENTRALIZED ENERGY TRADING

The prominent example of a trading energy system that uses blockchain is Brooklyn microgrid [12] as shown in Figure 5 which is designed in the USA. It can be described as a solution that combines the security and transparency between the neighbors that is offered by blockchain concept. The goal of the system is to measure the ability of blockchain technology adapted in order to buy and sell the energy among the neighbors and how effective blockchain technology is adopted.

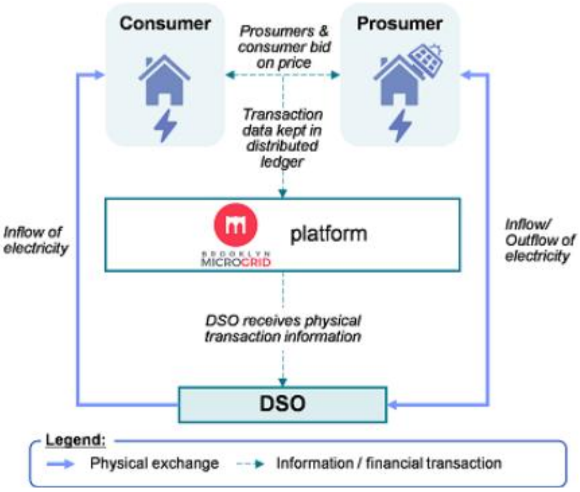
Consumer
Prosumers & consumer bid on price
Prosumer
Transaction data kept in distributed ledger
Inflow of electricity
platform
BROOKLYN MICROGRID
Inflow/ Outflow of electricity
DSO receives physical transaction information
DSO
Legend:
Physical exchange
Information / financial transaction

Fig 5. Brooklyn microgrid network [12]

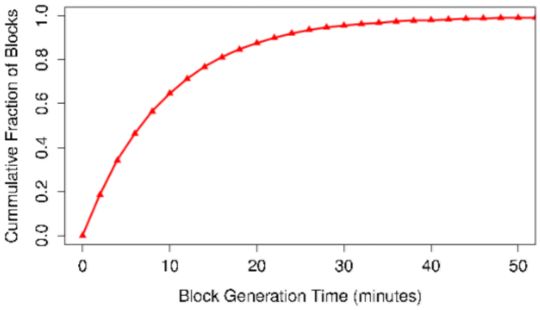

Fig 6. Block generation time in Bitcoin

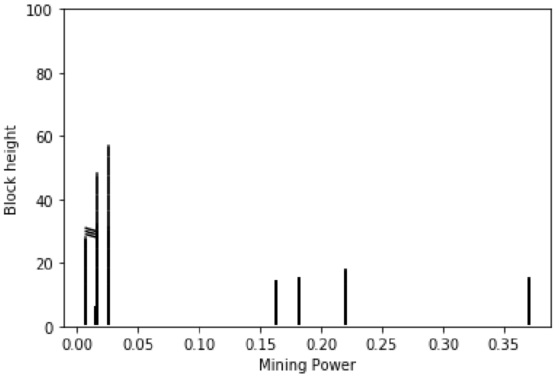

Fig 7. Performance of dishonest miner

A decentralized storage the transaction on the blockchain system allows keeping a distribute, transparency and secure record of energy transaction between the party which is tamper-proof from the attacker. Decentralized energy trading system would no longer require the third-party involvement e.g. banks, energy companies in order to do the energy trading activities among the traders. Instead, the process will run automatically and the energy will be sent after the miner solving the proof-of-work and propagates to the entire network which in the end the prosumer will get his/her reward. The router transmits the packet data of record transaction from a source to another computer in the peer-to-peer network. 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 prosumer who has surplus energy and wants to sell the energy announces to the network by giving details the information related to the amount of energy and the price. The consumers will be able to see that announcement and if the consumers want to do the transaction, it will execute by the miners via smart contract.

After a transaction is broadcast to the Bitcoin network. When that happens, it is said that the transaction has been mined at a depth of 1 block. With each subsequent block that is found, the number of blocks deep is increased by one. To be secure against double-spending, a transaction should not be considered as confirmed until it is a certain number of blocks deep. Cumulative distribution function (CDF) of block based on figure 6, the approximately 30% of Bitcoin blocks take between 10 and 40 minutes to be generated [13].

In the selfish mining attack, an attacker tries to find a new block by solving proof-of-work puzzle and keep the block secret and doing mining continuously till they reach the longest chain on the blockchain network. The selfish chain publishes their secret block if only the honest network comes close to their secret network or when the selfish chain wants to claim the unfair rewards. It will affect the rational miner in order to join in the selfish mining pool. The rational miners are preferred join to the pool with the highest revenue.

The selfish miner is relying on the power mining (resources) as shown in Fig. 7 and always competes with the honest miner to find a new block. Once their network becomes the longest, the selfish miner will easily to invalidate the valid block from the honest miner. The current assumption of Bitcoin system is safe as long as 51% of mining power is under the honest miner, but Eyal and Sirer [14] show the attacker can gain the unfair revenue with 25% hashing power.

The components model in the network architecture performs a key role in supporting the continuity of a system and 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.

III. CONCLUSION

The concept of blockchain technology is used for trading the renewable energy system in an environment among the neighbors in the peer-to-peer network. We discussed a model for trading energy in a small environment by using blockchain technology and then we analyzed security issues that might be occurred. The performance of the attacker is also presented. Blockchain technology with cryptographic embedded to support the security issues can become a possible solution for the future to create a secure trading renewable energy system in the environment among the neighbors. The energy and commodity transaction life cycle, even for simple transactions, involves a multitude of processes within each company and across market participants. Blockchain turns both currencies and commodities into a digital form without relying on middleman which allows one person to trade with another. For the future, the strategy is needed in order to prevent the various attack, especially in the overlay network.

IV. REFERENSI

[1] N.Z. Aitzhan and D. Svetinovic, "Security and Privacy in Decentralized Energy Trading through Multi-Signature, Blockchain and Anonymous Messaging Streams", IEEE Transactions on Dependable and Secure Computing, 2016.

[2] PwC Global Power, "Blockchain-an Opportunity for Energy Producers and Consumers?" PwC Global Power and Utilities, 2016.

[3] G. Karame, E. Androulaki, "Bitcoin and Blockchain Security", Information Security and Privacy Series, United States of America, Artech House, 2016.

[4] P. Danzi, A. Marko, C. Stefanovic, and P. Popovski, “Distributed Proportional-Fairness Control in Microgrids via Blockchain Smart Contracts”, arXiv: 1705.01453v2 [cs.MA], 2017.

[5] F. Imbault, M. Swiatek, R.de Beaufort and R. Plana, "The Green Blockchain Managing Decentralized Energy Production and Consumption", IEEE International Conference on Environment and Electrical Engineering (EEEIC/ I&CPS Europe), 2017.

[6] S. Nakamoto, “Bitcoin: A Peer-to-peer Electronic Cash System”, 2008.

[7] P. Narayan, “Building Blockchain Projects: Develop real-time DApps using Ethereum and JavaScript”, Birmingham-Mumbai, Packt Publishing Ltd. 2017.

[8] C. Troncoso, M. Isaakidis, G. Danezis and H. Halpin, Systematizing Decentralization and Privacy: Lesson from 15 Years of Research and Deployments, Proceeding on Privacy Enhancing Technologies: 307-329, 2017.

[9] K.S. Ramesh, M. Kasbekar, W. Lichtenstein, J. Manish, “Overlay Network: An Akamai Perspective”, University of Massachusetts, Amherst, Akamai Technologies Inc*

[10] Chord (peer-to-peer): https://en.wikipedia.org/wiki/Chord

[11] S. Ion, R. Morris, D. Karger, M. Frans Kaashoek, H. Balakrishnan, “Chord: A Scalable Peer-to-peer Lookup Service for Internet Applications”, SIGCOMM’01, San Diego, California, USA, 2001.

[12] Brooklyn Microgrid, Available online at: https://www.brooklyn.energy/

[13] Average Confirmation Time in Bitcoin: https://blockchain.info/charts/avg-confirmation-time

[14] I. Eyal, and E.G. Sirer, “Majority is not Enough: Bitcoin Mining is Vulnerable”, Financial Cryptography and Data Security, Berlin, 2014.