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 a middleman, allowing one person to trade with another, including trading renewable energy. This study aims to explore the implementation of blockchain technology in the energy sector. The method used involves describing, exploring, and analyzing the prominent implementation of blockchain technology in energy trading. The research has found that the current form of centralized energy trading systems still suffers from security concerns and a lack of quality of service. A decentralized energy system using blockchain technology allows parties to create energy trading transactions via microgrid. Blockchain technology promises an immutable, single source of truth from multiple sources without third-party involvement. Furthermore, we analyzed the security issues and highlighted the performance of several attacks that might occur in the proposed system. Understanding these aspects is crucial for developing a secure and efficient energy trading platform.

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

I. INTRODUCTION

The trading of energy systems is evolving towards a more decentralized model that accommodates heterogeneous, competitive energy sources and energy storage systems (ESS). Most modern financial infrastructures are centralized and involve a trusted third party, which handles accounts, processes payments, and provides security [1], [2]. In general, the centralized trading system still has some drawbacks and becomes the death knell for energy providers. The decentralized possesses a single point of failure from a middleman that may disrupt trading activities [3]–[5] as it directly affects consumer satisfaction. Hence, the research related to 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.

The initial step for trading renewable energy systems has been exploring, integrating, and making connections for equipment with distributed energy resource systems such as solar energy in a decentralized peer-to-peer network. As it has for centuries, commerce relies on trust and verified identity, with a cryptography protocol module embedded in the system to ensure data credibility and other security measures. Starting as a niche system on the market, nowadays, it attracts the interest of experts in several industries [6].

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 of service. It gives many advantages, such as flexibility, scalability, etc. Furthermore, a third party whose service is needed in the industries is no longer necessary in a decentralized blockchain system. Henceforth, it increases the transaction speed, reduces the cost, and improves the quality of service of a trading system. Instead of only consuming energy, the blockchain allows prosumers with surplus energy to create a trading activity to sell their energy via an intelligent grid.

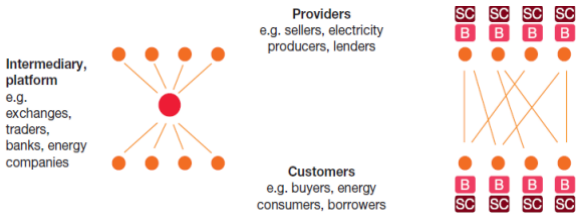

Fig 1. Centralized and decentralized structure

Several researchers have proposed a concept of decentralized energy trading through multi-signatures and the anonymous messaging stream [7], [8]. 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: sending a private message and broadcasting 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) can solve the problems among the parties. The authors did not elaborate on the attacker's performance, such as selfish mining, eclipse attack, and double spending attack in the model.

Imbault et al. [9] proposed the green blockchain concept for managing energy and exploring and creating a green certificate in an eco-district. There are no details

ISSN 2527-1682 (Print)
ISSN 2527-9165 (Online)

related to the security issues in this system. Recently, Danzi et al. [10] showed the concept of distributed proportional fairness control via a blockchain smart contract. The study aimed to enhance efficiency, especially regarding 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 ledgers containing much transaction information [11]–[13]. As it has for centuries, commerce relies on trust and verified identity with cryptography protocol modules embedded in the system to ensure the credibility of the data and other security manners. As shown in Fig 2, the timestamp is used in digital documents to prevent the attacker from tamper-proofing it. The block in the blockchain is like a seal; if the attacker tries to break the seal, everyone is allowed 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 [14], [15]. The hash is produced by running the contents of the block in question through a cryptographic hash function, e.g., Bitcoin uses SHA-256. An ideal cryptographic hash function can easily create a hash for any input, but it is challenging to derive the input.

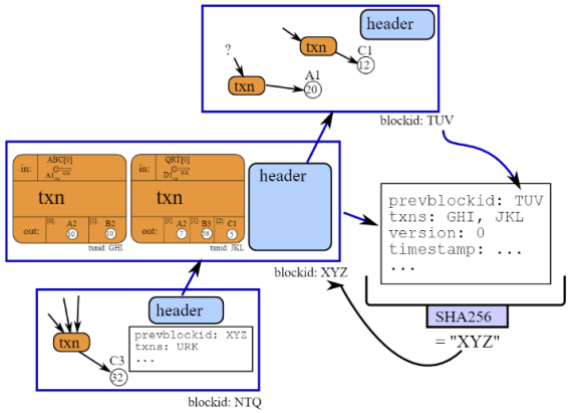

Fig 2. The information a block (transaction)

In blockchain architecture, a block consists of two main parts: the transaction block, which contains all the transactions within the block, and the block header. The block header is a short and strictly formatted data field that prepends every block. It includes six fields, each serving a different function. Table 1 provides a detailed description of the functionalities of these fields.

Table 1. Bitcoin block header 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 [16] and operational registries [17], [18] , and one of the most popular ones is the smart contracts [19], [20]:

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

Proof-of-work in Bitcoin, proof-of-stake, and so on are various consensus protocols that keep the blockchain secure [21]. It depends on the consensus protocol. The blocks are created and added to the blockchain differently. In proof of work, blocks are made by mining, which keeps the blockchain safe. A probability of finding nNonce of proof H for given target T is:

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

The disadvantage of proof-work is related to efficiency, which wastes too many computational resources to find the target value (hash puzzle). The hash in PoW begins with several zero-bit hashes (SHA-256) and involves scanning for value when hashing data.

B. RESILIENT OVERLAY NETWORK

An extensive distributed system is an overlay network that delivers content, applications, and services to a global audience [22]. The chord algorithm in the overlay network provides a fast-distributed computation of hash function mapping keys to nodes responsible for them. It uses consistent hashing [23], which has several good properties. With high probability, when a n_{th} node joins (or leaves) the network, only an O(1/N) fraction of the keys are moved to a different location. This is the minimum necessary to maintain a balanced load [24]. 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.

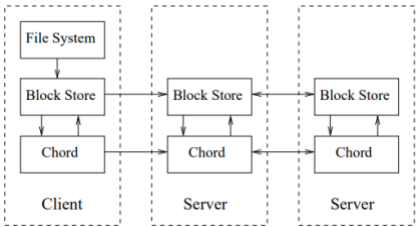

Fig 3. Chord-based distributed system

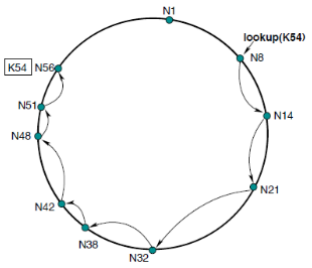

Fig 4. Chord-based distributed system

As shown in Fig 3, the chord algorithm has a basic structure from client to server. From the client's side, there is a block, such as a file system, block store, and the chord itself. Block stores and chords are connected to another server and the client from the server. The primary usage of the chord protocol is a query value [21] from a client to find a successor (k). This refers to an O(N) query time, and the N refers to the number of rings applied.

As shown in Fig 4., each node has a successor and a predecessor. The successor to a node is the next node in the identifier circle in a clockwise direction. The predecessor is counter-clockwise. However, typically, there are "holes" in the sequence (because of failure or departure). Regarding the possibility of the holes, each node records an arc of $2r + 1$ nodes in the middle of which it stands, i.e., the list of r nodes preceding it and r nodes following it. This list results in a high probability that a node can correctly locate its successor or predecessor, even if the network suffers from a high failure rate [21].

In our system model, the chord-based distributed system is used to know the node location among the neighbors in the decentralized trading system.

III. RESULT AND DISCUSSION

A. DECENTRALIZED ENERGY TRADING MODEL

A prominent example of a blockchain trading energy system is the Brooklyn microgrid [24] as shown in Figure 5, designed in the USA. It can be described as a solution that combines the security and transparency between the neighbors offered by the blockchain concept. The system aims to measure the ability of blockchain technology to buy and sell energy among the neighbors and how effective blockchain technology is adopted.

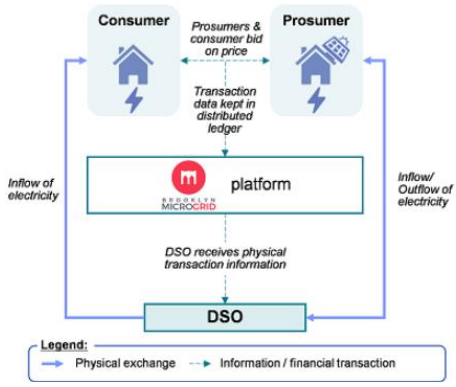

Fig 5. Brooklyn microgrid network [25]

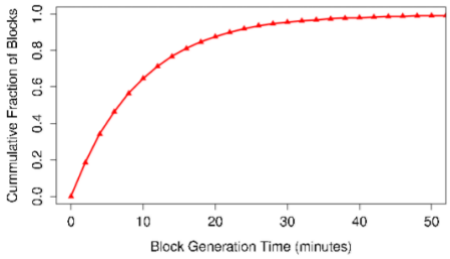

Fig 6. Block generation time in Bitcoin

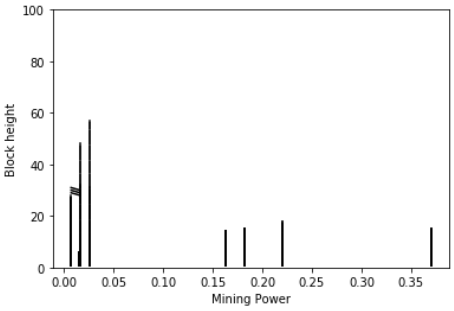

Fig 7. Performance of dishonest miner

Decentralized storage of the transaction on the blockchain system allows for keeping a distributed, transparent, and secure record of energy transactions between the parties, which is tamper-proof from the attacker. A decentralized energy trading system would no longer require third-party involvement, e.g., banks and energy companies, to do energy trading activities among the traders. Instead, the process will run automatically, and the energy will be sent after the miner solves 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 transactions 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 using AES (Advanced Encryption Standard). The prosumer who has surplus energy and wants to sell the energy announces to the network by giving details on the amount of energy and the price. The consumers will be able to see that announcement, and if they want to do the transaction, it will be executed by the miners via a 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 found, the number of blocks deep increases by one. To be secure against double-spending, a transaction should not be considered as confirmed until it is several blocks deep. The cumulative distribution function (CDF) of blocks based on Fig 6 shows that approximately 30% of Bitcoin blocks take between 10 and 40 minutes to be generated [26].

In a selfish mining attack, an attacker tries to find a new block by solving a proof-of-work puzzle, keeping the block secret, and mining continuously till it reaches the longest chain on the blockchain network. The selfish chain publishes its secret block if only the honest network comes close to its secret network or when the selfish chain wants to claim unfair rewards. It will affect the rational miner to

join the selfish mining pool. The rational miners prefer to enter the pool with the highest revenue.

The selfish miner relies on 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 quickly invalidate the valid block from the honest miner. The current assumption of the Bitcoin system is safe as long as 51% of the mining power is under the honest miner, but Eyal and Sirer [21] show the attacker can gain 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 block location and the ability to fetch data blocks in the appropriate node containing the requested data and return it to the requester.

III. CONCLUSION

Blockchain technology is used to trade renewable energy systems in an environment among neighbors in the peer-to-peer network. We discussed a model for trading energy in a small environment using blockchain technology and then analyzed possible security issues. The performance of the attacker is also presented. Blockchain technology with cryptographic embedded to support the security issues is a potential solution 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 currencies and commodities into a digital form without relying on middlemen, allowing one person to trade with another. In the future, a strategy is needed to prevent various attacks, especially in the overlay network.

IV. REFERENCES

[1] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," *Telecomm. Policy*, vol. 41, no. 10, pp. 1027–1038, 2017.

[2] W.-T. Tsai, R. Blower, Y. Zhu, and L. Yu, "A system view of financial blockchains," in *2016 IEEE Symposium on Service-Oriented System Engineering (SOSE)*, 2016, pp. 450–457.

[3] S. McLean and S. Deane-Johns, "Demystifying blockchain and distributed ledger technology–hype or hero?," *Comput. Law Rev. Int.*, vol. 17, no. 4, pp. 97–102, 2016.

[4] P. De Filippi, "The interplay between decentralization and privacy: the case of blockchain technologies," *J. Peer Prod. Issue*, no. 7, 2016.

[5] M. Atzori, "Blockchain technology and decentralized governance: Is the state still necessary?," *Available SSRN 2709713*, 2015.

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

[7] N. Z. Aitzhan and D. Svetinovic, "Security and Privacy in Decentralized Energy Trading Through Multi-Signatures, Blockchain and Anonymous Messaging Streams," *IEEE Trans Dependable Secur. Comput*, vol. 15, no. 5, pp. 840–852,, doi: 10.1109/TDSC.2016.2616861.

[8] E. Mengelkamp, B. Notheisen, C. Beer, D. Dauer, and C. Weinhardt, "A blockchain-based smart grid: towards sustainable local energy markets," *Comput. Sci. - Res. Dev.*, vol. 33, no. 1–2, pp. 207–214,, doi: 10.1007/S00450-017-0360-9/METRICS.

[9] F. Imbault, M. Swiatek, R. Beaufort, and R. Plana, "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*. doi: 10.1109/EEEIC.2017.7977613.

[10] P. Danzi, M. Angjelichinoski, C. Stefanovic, and P. Popovski, "Distributed proportional-fairness control in microgrids via blockchain smart contracts," in *2017 IEEE International Conference on Smart Grid Communications, SmartGridComm 2017*, pp. 45–51,. doi: 10.1109/SMARTGRIDCOMM.2017.8340713.

[11] S. Nakamoto, "Bitcoin: A Peer-to-peer Electronic Cash System"."

[12] E. Karafiloski and A. Mishev, "Blockchain solutions for big data challenges: A literature review," in *IEEE EUROCON 2017-17th International Conference on Smart Technologies*, 2017, pp. 763–768.

[13] B. Notheisen, J. B. Cholewa, and A. P. Shanmugam, "Trading real-world assets on blockchain: an application of trust-free transaction systems in the market for lemons," *Bus. Inf. Syst. Eng.*, vol. 59, pp. 425–440, 2017.

[14] R. Pass and A. Shelat, "Micropayments for decentralized currencies," in *Proceedings of the 22nd ACM SIGSAC Conference on Computer and Communications Security*, 2015, pp. 207–218.

[15] Y. Liu *et al.*, "An efficient method to enhance Bitcoin wallet security," in *2017 11th IEEE International Conference on Anti-counterfeiting, Security, and Identification (ASID)*, 2017, pp. 26–29.

[16] K. Fanning and D. P. Centers, "Blockchain and its coming impact on financial services," *J. Corp. Account. Financ.*, vol. 27, no. 5, pp. 53–57, 2016.

[17] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "Secure and Trustable Electronic Medical Records Sharing using Blockchain," *AMIA Annu Symp Proc*, vol. 2017, pp. 650–659,.

[18] A. Shahaab, I. A. Khan, R. Maude, C. Hewage, and Y. Wang, "Public service operational efficiency and blockchain – A case study of Companies House, UK," *Gov Inf Q*, vol. 40, no. 1, p. 101759, doi: 10.1016/J.GIQ.2022.101759.

[19] E. Hillbom and T. Tillström, "Applications of smart-contracts and smart-property utilizing blockchains," 2016.

[20] A. Law, "Smart contracts and their application in supply chain management." Massachusetts Institute of Technology, 2017.

[21] C. Troncoso, M. Isaakidis, G. Danezis, and H. Halpin, "Systematizing Decentralization and Privacy: Lessons from 15 Years of Research and Deployments," *Proc. Priv. Enhancing Technol.*, no. 4, pp. 404–426,, doi: 10.1515/popets-2017-0056.

[22] R. K. Sitaraman, M. Kasbekar, W. Lichtenstein, and M. Jain, "Overlay Networks: An Akamai Perspective," in *Advanced Content Delivery, Streaming, and Cloud Services*, vol. 9781118575, pp. 305–328,. doi: 10.1002/9781118909690.CH16.

[23] I. Stoica, R. Morris, D. Karger, M. F. Kaashoek, and H. Balakrishnan, "Chord: A scalable peer-to-peer lookup service for internet applications," *ACM SIGCOMM Comput. Commun. Rev.*, vol. 31, no. 4, pp. 149–160,, doi: 10.1145/964723.383071.

[24] E. Mengelkamp, J. Gärttner, K. Rock, S. Kessler, L. Orsini, and C. Weinhardt, "Designing microgrid energy markets: A case study: The Brooklyn Microgrid," *Appl Energy*, vol. 210, pp. 870–880,, doi: 10.1016/J.APENERGY.2017.06.054.

[25] P. Treleaven, R. G. Brown, and D. Yang, "Blockchain Technology in Finance," *Comput. (Long Beach Calif.*, vol. 50, no. 9, pp. 14–17,, doi: 10.1109/MC.2017.3571047.

[26] "Average Confirmation Time in Bitcoin." [Online]. Available: https://blockchain.info/charts/avg-confirmation-time