Blockchain based smart energy trading platform using smart contract

Seung Jae Pee
Department of Electronic Engineering
Sogang University
Seoul, Korea
paul_0238@naver.com

Eung Seon Kang
Department of Electronic Engineering
Sogang University
Seoul, Korea
kes617@naver.com

Jae Geun Song
Department of Electronic Engineering
Sogang University
Seoul, Korea
1080skj@gmail.com

Ju Wook Jang
Department of Electronic Engineering
Sogang University
Seoul, Korea
jjang@sogang.ac.kr

***Abstract*— The energy market is entering the transitional period, and various types of energy markets such as solar energy will be formed beyond oil and gas. Correspondingly, energy prosumers that individuals and institutions produce and trade surplus electricity will become more widespread. Using the block chain, it guarantees the immutability and transparency of energy transactions, generates ERC20 tokens based on smart contracts, and transactions are automatically executed without third party intervention and can be extended to various transaction conditions. In the transaction, the energy is transferred using the Energy Storage System(ESS) which the seller and the buyer belong, and payment is made by transferring the token through a transaction. Based on this information, this paper suggests proposes a peer-to-peer (P2P) system that can freely trade the produced energy.**

***Keywords*— Blockchain, Smart Contract, Energy Trading, Smart City, ERC20 Token.**

I. Introduction

As the global pending issue linked with energy and environment is continuously raised, new renewable energy draws attention as a dominant alternative plan. [1] Renewable energy is recognized as environmentally friendly energy that replaces existing energy because it emits less pollutant and is renewable. Accordingly, infrastructure and platforms for renewable energy are gradually being developed, and there is a growing demand for expansion of renewable energy.

In this paper, we propose a new trading platform that using the block chain to further activate new energy resources that can be used in the future.

Blockchain is considered an open ledger where all online transactions are recorded and everyone is allowed to connect, to send or verify transactions. In other words, Blockchain is a digitized system of accounting records which records in details all transactions according to a mathematical set of rules to prevent illegal interference[2].

Each node (individual and institution) in a block chain become a prosumer who can produce, sell and buy energy, and can trade energy through a P2P network without going through a central organization.

Because trading is based on smart contracts, it is executed automatically without third party intervention. It is possible to set various transaction conditions but basic type of trading is that trading is established as much as the sales and purchase volumes matches based on the price set according to the total energy amount. This enables us to use energy more efficiently by forming an active energy trading platform that is out of the traditional way. At this time, if the amount of power and transaction records held by the node are recorded in the block-chain network, all data can be processed without risk of loss and attack, to prevent attacker nodes purchasing and selling indiscreet energy, we construct a private network that can only participate in authorized nodes.

II. Background

A. Blockchain

The blockchain is a P2P-based distributed data network system. Because the blocks are grouped into chains, they are named as blockchain. In the blockchain, all users participating in the network distribute and store history data in block format, which is a set of transactions. Since each node has a single secret key and a public key, it is possible to perform a digital signature on the transaction using the secret key and the hash function. Each node uses the public key to verify whether the subject of the digital signature actually signed the transaction[3]. The block containing this transaction has a structure of "chains" that are continuously connected along the time flow after being made at a specific cycle. Because all users hold transaction history, every user can verify the

978-1-5386-7822-0/19/$31.00 ©2019 IEEE

transaction history by checking the ledgers they hold. Therefore, transactions that are not validated can't be stored in the block. Thus, blockchain has three characteristics: data integrity, security, and decentralization[4].

B. Smart Contract

What is Smart Contract: Nick Szabo introduced this concept in 1994 and defined a smart contract as "A computerized transaction protocol that executes the terms of a contract"[5]. Nick Szabo suggested translating contractual clauses into code, and embedding them into property that can self-enforce them[6]. However, in blockchain systems, the meaning of smart contracts has evolved. Within the blockchain context, smart contracts are scripts recorded on the blockchain.(They can be thought of as roughly analogous to recorded procedures in relational database management systems[7]. Since they reside on the chain, they have a unique address. We trigger a smart contract by addressing a transaction to it. It then executes independently and automatically in a prescribed manner on every node in the network, according to the data that was included in the triggering transaction[4].

III. BLOCKCHAIN-BASED POWER TRADING

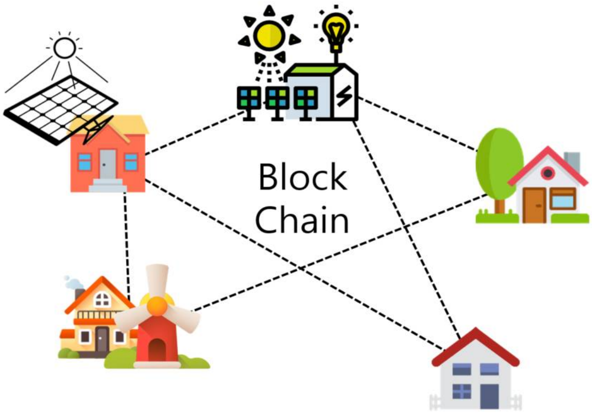

Figure 1. Blockchain network of prosumer

A. Blockchain network of prosumer

<Figure 1> shows that a company and an individual who produce and consume energy form a block chain network as a prosumer. The network is a private network that can only participate in authorized nodes. The private block chain is a block chain system that allows the system administrator to approve the transaction verification that was the role of the miner in the existing public block chain system.[8] Then, the power generated by each node is put on the energy market, and the purchaser who lacks energy can purchase and use the energy in the market.

B. Energy trading using ESS

However, there is a limit to the installation of the power network as the number of participating nodes increases. City-unit trading is possible to overcome this. The transmission of the token is through a block-chain network, and the transmission of energy is through the Energy Storage System(ESS). Like Figure 2 and Figure 3, the transmission of the token is transferred as a direct transaction of each node, in the case of energy, the individual ESS of the city is placed so that the seller delivers energy to the ESS and the buyer receives energy from the ESS. At this time, the ESS is connected to another blockchain, communicates the transaction information, checks the amount of retained energy for each city, and supplements the power of the missing ESS.

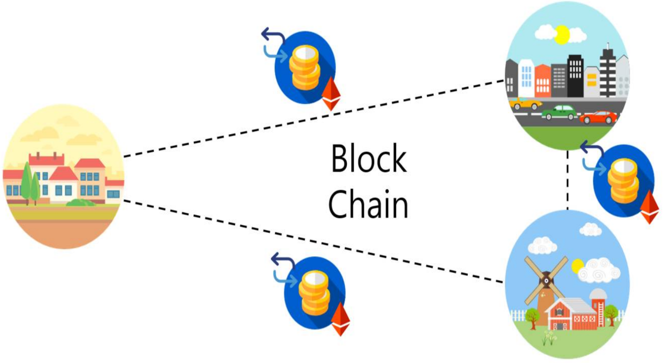

Figure 2. City-unit blockchain network

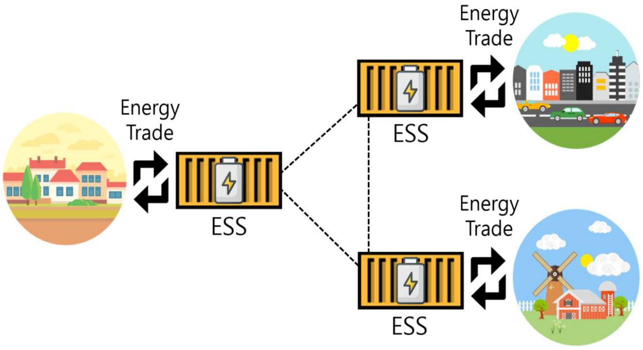

Figure 3. Energy trading using ESS

IV. TRADING METHOD(SMART CONTRACT)

A. Generate token

Create a token that ERC20 currency trading. The transmission of tokens follows the ERC20 standard.[9]

The DSO creates a token by creating a smart contract (which encodes the business logic and records it in the block chain, ensuring the enforcement and automation of the contract fulfillment). Smart contracts that you create will continue to be used in transactions.

B. Trading process

Once the price is determined, the DSO sends a transaction to update the price on the smart contract. When the price is updated, each node freely records the sale intention and the purchase intention on the block chain in the form of transaction. After receiving enough transaction requests, the transaction proceeds.

Based on the price set by the total amount of energy, the basic transaction type is that only when the purchase and sale requests for energy are received and the purchase and sales volume are matched.

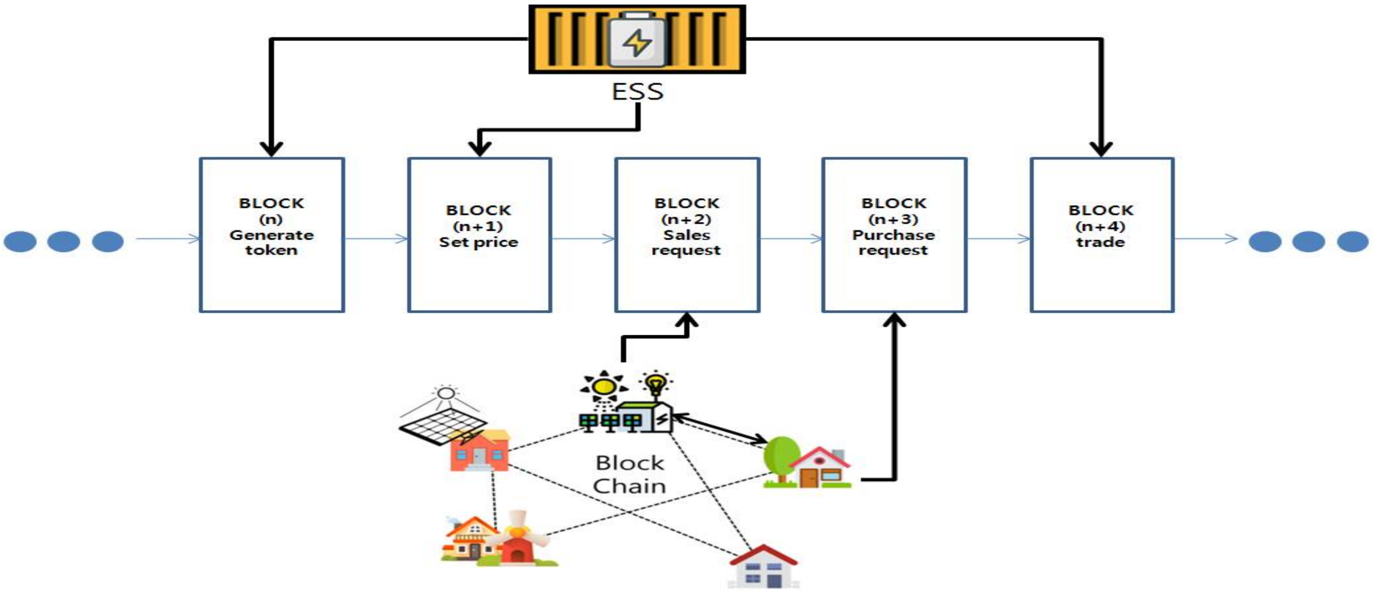

Figure 4. Diagram of total blockchain system

C. *Call for purchase*

Each node broadcasts a transaction including the amount of energy to buy. Nodes with lower balance than the price of energy to buy cannot broadcast transaction. After call for purchase, the smart contract gives DSO the authority of sending token to the prosumer so DSO can move the token from consumer to prosumer. Each call for purchase is consisted of the address of consumer and the amount of energy as an instance of struct and stored in array with sequence order.

D. *Call for sale*

Each node broadcasts a transaction including the amount of energy to sell. Like as the procedure for call for purchase, the information is recorded as an instance of struct which is consisted of the address of prosumer and the amount of energy to sell and stored in array with sequence order.

E. *Trade energy*

After the procedures of purchase and sale, DSO executes the trade. DSO compares the total amount of purchase and sale. Trade is accomplished if the amount of energy to buy and sell is equal. Then the smart contract moves the token and energy according to the accomplished trade and third trade is recorded on blockchain. <Figure 4> shows the overall transaction process.

F. *Smart contract code*

Figure 5 shows smart contract code of prevent double spending problem. In the case of Ethereum, the smart contract will not be executed until it is mined, so sometimes the later executed code will work first. To solve this double spending problem, Node A changes the right of withdraw node B from N to 0 first, confirms that it has changed normally without any problems, and then changes it back to M. If you ignore the fact that the order of execution of the code can be reversed by the mining order, there may be various security loopholes. We should think about this when writing smart contract code.

```
function decreaseApproval(address _spender, uint _subtractedValue)
public returns (bool) {
   uint oldValue = allowed[msg.sender][_spender];
   if (_subtractedValue > oldValue) {
     allowed[msg.sender][_spender] = 0;
   } else {
     allowed[msg.sender][_spender] = oldValue.sub(_subtractedValue);
   }

   Approval(msg.sender, _spender, allowed[msg.sender][_spender]);
   return true;
 }

 . . .

function Energybuy (uint256 amount) public {
   if (amount == 0)
      throw;
   if(amount*Energyprice > balances[msg.sender])
      throw;
   decreaseApproval(DSO,balances[msg.sender]);

   buying memory buy = buying(msg.sender,amount);
   buyings.push(buy);
   approve(DSO,amount*Energyprice);
   l++;
   fin(1);
 }
```

Figure 5. Smart contract code of prevent double spending

V. Conclusion

If we implement the energy trading platform proposed in this paper, we can solve the security problem through the block-chain private network and implement the P2P system that enhances the transparency and immutability by executing the automatic transaction without involving the third party using the smart contract. Because energy circulates virtually, energy use efficiency can be increased.

ACKNOWLEDGMENT

This research was supported by Basic Science Research Program through the National Research Foundation of Korea(NRF) funded by the Ministry of Education(NRF-2016R1D1A1B01009027), and the MSIT(Ministry of Science and ICT), Korea, under the ITRC(Information Technology Research Center) support program(IITP-2018-2017-0-01628) supervised by the IITP(Institute for Information & communications Technology Promotion).

REFERENCES

[1] Chang Hoon Lee: A Legal Study on Environmental Impacts of the New and Renewable Energy, (2015).

[2] Quoc Khanh Nguyen, Blockchain - A Financial Technology for Future Sustainable Development, (2016).

[3] Dale Ashton, "Irrigators' experience with water market intermediaries", The Australian Government acting through the Australian Bureau of Agricultural and Resource Economics – Bureau of Rural Sciences September 2010

[4] Seung Jae Pee, Jong Ho Nang, Ju Wook Jang (2018). "A Simple Blockchain-based Peer-to-Peer Water Trading System Leveraging Smart Contracts". [Online]. Available: https://csce.ucmss.com/cr/books/2018/ConferenceReport?ConferenceKey=ICM

[5] Tapscott Don, Tapscott Alex "The Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World." pp. 72, 83, 101, 127. ISBN 978-0670069972. May 2016

[6] N. Szabo. (1997). "The Idea of Smart Contracts". [Online]. Available: http://szabo.best.vwh.net/smart_contracts_idea.html

[7] MySQL Reference Manual, Using Stored Routines (Procedures and Functions), accessed on Mar. 15, 2016. [Online]. Available: http://dev.mysql.com/doc/refman/5.7/en/stored-routines.html

[8] "Hyperledger Architecture, Volume 1", https://www.hyperledger.org/wp-content/uploads/2017/08/Hyperledger_Arch_WG_Paper_1_Consensus.pdf, Aug. (2018).

[9] Fabian Vogelsteller and Vitalik Buterin. (2015). ERC-20 Token Standard. https://github.com/ethereum/EIPs/blob/master/EIPS/eip-20.md.