Corrigendum: Research on application model of blockchain technology in distributed electricity market

IOP Conf. Ser.: Earth Environ. Sci. 93 (2017) 012065

S Cheng1, B Zeng1 and Y Z Huang1

1North China Electric Power University, Changping District, Beijing, China

Page 7:

Figure 3 remains protected by copyright and is not available under the CC BY licence attached to this article. The figure has been taken from this article:

http://nrgcoin.org/assets/pdf/NRGcoin_Virtual_Currency_for_Trading_of_Renewable_Energy_in_Smart_Grids.pdf

The figure caption should read:

“Figure 3. An Example Scenario. Copyright M. Mihaylov”

The figure should be referenced as:

“M. Mihaylov, S. Jurado, N. Avellana, K. Van Moffaert, I. Magrans de Abril and A. Nowé, "NRGcoin: Virtual Currency for Trading of Renewable Energy in Smart Grids," in Proc. of the 11th International Conference on the European Energy Market (EEM), Krakow, Poland, 2014.”
Research on application model of blockchain technology in distributed electricity market

S Cheng¹,², B Zeng¹, Y Z Huang¹

¹ North China Electric Power University, Changping District, Beijing, China
E-mail:15810868303@163.com

Abstract. In the context of current energy Internet, the emergence of a large number of energy productive consumers will create a new business model. In the decentralized electricity market, the cost of traditional centralized solution construction, management and maintenance is too high, and it is difficult to support the collection, transmission, reception, storage and analysis of massive data. To provide a solution to this phenomenon, we apply the blockchain technology to this distributed electricity market to achieve peer to peer transactions in the power systems. The blockchain technology which is very popular nowadays will be used in power system to establish a credible direct transaction between devices. At first, this article analyzes the future direction of the development of power systems, studies the characteristics of decentralized power systems and summarizes the main issues in the development process. Then, we analyze the basic characteristics of blockchain and put forward a new transaction framework in consideration of problems existing in current energy market. The transaction framework is based on the blockchain technology in the distributed electricity market and includes the pricing method, the power transaction system architecture, various modules of the trading system and the details of the whole transaction system runtime. This framework provides a viable solution for increasingly complex energy transactions.

1. Introduction

1.1. Background
At present, the rapid development of large data and Internet technology is driving the whole social form and infrastructure changes. This sort of change not only contains different types of economic systems, but also includes the corresponding management model. In this flattened social system, the boundaries between consumers, businesses, governments and regulators are becoming increasingly blurred [1]. All nodes can understand the actual operation of the system through a flat system network structure and can also affect the operation of the system. What’s more, with the development of energy Internet, the advancement of electricity market reform and the popularization of distributed power generation, energy storage, electric vehicle and demand side response, a large number of consumers will evolve into prosumers. The emergence of the prosumers also makes the current power system in the supply and demand boundaries gradually blurred. The current power system operation and management models are gradually unable to meet the various types of energy unit "plug and play" access mode [2].

1.2. Decentralized power system resources
Decentralized power generation (DG) is a form of power generation that is directly connected to the distribution network or users’ meter installation. It includes photovoltaic cell power generation, wind power generation and fuel cell power generation. According to the different power generation technology, decentralized power generation can be divided into renewable energy decentralized power generation, modular decentralized power generation and combined heat and power generation. With the development of new battery energy storage, power generation cost with decentralized power generation device is getting lower and lower, and some have even been close to that with the traditional centralized power plant, therefore the application scope of decentralized power generation will be more and more widely. In addition, the emergence of electricity retail market will also be a strong promotion of decentralized energy production development. Decentralized energy production with its clean environmental protection and local power generation service users and many other advantages, will have an increasing market share. With the development of distributed renewable energy and distributed energy storage permeability, the boundaries of supply and demand in traditional energy and power systems are becoming increasingly blurred, and scattered energy production leads to the emergence of a large number of productive consumers.

Figure 1 describes the energy systems that include a variety of new energy sources. In the future of the electric energy system, there will be a great possibility of the following situation: in the sunny weather it can produce a lot of electricity, while in the cold windless weather there will be the situation lack of electricity. In some areas, decentralized power systems may also imply constraints on the local grid [3].

![Figure 1. Future energy system framework. Copyright J. Mattila](image)

With the infiltration of decentralized power systems and the increasing power data, how to build a new, reliable and effective energy trading model is very urgent. The key to solving such problems is to ensure that the balance of electricity production and consumption, which is essential to increase the flexibility of electricity production and consumption [4]. If a power consumer can autonomously allocate electricity, making the allocation effective, self-sustaining and free from external control, then the entire power system will become much more flexible. There are already similar application cases, such as the use of blockchain technology between adjacent households for power exchange.
1.3. Contributions
To summarize, in order to cope with the problems raised above, this paper constructs a decentralized trading platform based on the blockchain technology, which will realize the decentralized pricing and P2P (Peer-to-Peer) transactions in the distributed power market, and realize an effective trading model to deal with the increasing volume of power transaction information and the increasingly blurred development trend of supply and demand.

In our view, the contributions of this paper include:

- We analyze the future direction of the development of power systems, study the characteristics of decentralized power systems and summarize the main issues in the development process.
- Based on the analysis of possible problems in the decentralized power energy system, we propose the application of the blockchain technology to the future transaction mode in electric power transaction. In addition, by comparing the traditional power transaction model and the blockchain based transaction model, we sum up the advantages of the latter to adapt to modern power development.
- We propose a transaction framework in decentralized electricity market based on the blockchain technology. First, we set up a power trading model, and clearly demonstrated its trading process. Then, we develop a pricing mechanism under the framework of this transaction to promote the balance between supply and demand among users.

2. Blockchain technology

2.1. The overview of blockchain technology
As a distributed accounting system, the blockchain has the characteristics of high reliability and decentralization, so that it can be well adapted to the decentralized system structure [5]. Shared economic and ecological environment based on the block chain technology can promote the development of decentralized systems. Through data encryption, timestamp, intelligent contract and other technical means, we can achieve the peer-to-peer transactions (P2P) in the absence of third-party trusted endorsement. The introduction of blockchain technology can reduce the barriers to entry trading systems, while ensuring the transparency and quick access to asset transactions.

Energy Internet technology is the focus of current academic attention. The third industrial revolution, represented by energy Internet technology, is booming with its core research areas expanding from the smart grid, the energy Internet to the global energy Internet [6,7]. Energy Internet is based on the existing power grid. Through advanced power electronics and information technology, a large number of new power network nodes which consist of distributed energy collection devices, distributed energy storage devices and a variety of load can be connected to achieve energy flow, two-way flow of energy information on the shared network.

This paper will start from the development trend of power transaction in the background of energy Internet, combine the existing problems and the problems that may arise in future development of electricity market with the relevant characteristics of blockchain, and propose a kind of point-to-point power trading framework based on the blockchain technology in the electricity market, including the power transaction system architecture, the various modules of the trading system, and the details of the entire transaction system runtime.

The concept of Bitcoin was first proposed in 2008, when it was used as a way of securely conducting electronic financial transactions without the need for centralized authorization. In the Bitcoin trade network, there is only one complete chain of transactions, the main chain, which is made up of a large number of blocks. Since each transaction is relatively fragmented, in order for better statistical transactions, the blocks are introduced. The bitcoin system creates a block every ten minutes or so, which contains all the transaction information for that period. Each block also contains the ID of the previous block, so that each block can find its previous node, which can be pushed from the latest block to the starting node, thus forming a complete transaction chain.

The blockchain is an emerging technology based on decentralized computing and data storage,
protected by a combination of cryptographic signatures and distributed sharing mechanisms. Even in the presence of network attacks and communication interruption, participants on the blockchain network can achieve a general agreement on the state of the system [8]. This contrasts sharply with the traditional architecture. In the traditional architecture, the central coordinator defines the state of the system, but may receive the effect of attack or misconduct. The basic architecture of the blockchain is shown in figure 2. Figure 2 shows the block $B^0$ to $B^{i+1}$ with the detailed information of $B^i$. Blocks are connected by encrypted hashes, protecting content from being changed and allowing the history to be audited. Participants for P2P networks are $M_i$ (i=1,2,...,N). The message that the network broadcasts contains commands (control actions, account extraction, etc.) of the system status, and each node can use the verification function to verify the feasibility of each message.

![Figure 2. Symbolic representation of data in blockchain.](image)

The blockchain header contains a timestamp, a concise encrypted hash with the contents of the previous block, and the result of a validation test that is difficult to forge under computational and economic constraints. The new blocks are broadcast to the network. Their validity will be checked, and the nodes will be consistent in the system's update status. When the state transition function can execute the computer code embedded in the transmission $M^i$, the effect of the blockchain can be further extended. These smart contracts can be checked and reviewed very transparently and can be guaranteed to be implemented on the web. The pillars of the block chain structure are the contents of the block loop connection, validating the new block with the P2P consensus and verifying the communication with the encrypted signature. These key processes can provide a representation of the system state without intervention of the trusted central authority. While this architecture introduces some computational expenses, it can guarantee the eternal invariance of transaction history, the transparency and verifiability of the transaction, and the ability to adapt the system to the coordination between parties that do not trust each other.

### 2.2. The basic characteristics of blockchain

As can be seen in the above content, the blockchain has some very obvious features. Table 1 compared the existing energy transactions and energy transactions based on blockchain.

| Table 1. Comparison between existing electricity transactions and transactions based on blockchain. |

---

NEFES 2017                                                                                                                ... Conf. Series: Earth and Environmental Science 93(2017 ) 012065           doi:10.1088/1755-1315/93/1/012065
### Trading Platform

| Data Object       | Non-sequential data. In accordance with the transaction, the central database generates specific transaction data. |
|-------------------|-------------------------------------------------------------------------------------------------------------|
| Transaction       | The trading entity completes the transaction through a trusted central trading body, such as an electricity trading centre. |
| Structure         | There is no trusted central organization. And there is no need for mutual trust between the transactional entities. Transactions are traded through smart contracts and the blockchain trading system. |
| Information       | The information extension is not high. The transaction information is stored in the centralized transaction mechanism. Only the central organization can check the information. If the central organization is attacked, it may lose some or all of the transaction information. |
| Extension         | The information is highly accessible. The blockchain can record all the transaction records from the start of the coin system. Therefore, each transaction is recorded and maintained by all the nodes. Each transaction object can view all the transaction information. Thus, the transaction process has a good traceability. |
| Security          | Security is low. Once the central authority is attacked, the data may be lost or tampered with, which will result in serious consequences. |
|                   | Security is relatively high. The data is stored in each node of the network. It is maintained by all nodes. |

### 3. Power transaction framework based on blockchain technology

#### 3.1. Transaction process

The transaction system based on the blockchain technology is decentralized, whose transaction information can be tracked to ensure the privacy of the transaction node information. This part will propose a power trading framework based on the blockchain technology in the distributed electricity market.

In the future, without central pricing agencies in the distribution network or regional energy Internet market, the pricing of power resources are real-time. Here is an example if we assume a transaction scenario and analyze the transaction chain based on the blockchain [9]. Assuming that there are power purchase node A and supply node B in the system, the basic flow of the transaction is as follows:

- Node A predicts that its distributed renewable energy will fluctuate in a short time \([ t_0, t_1]\), or suddenly the power load increases, requiring more power supply. It will send his own purchase demand information in the P2P network. The information release requires node A to process its own public key \(A\text{-Publickey}\) and private key \(A\text{-PrivateKey}\) with the encryption function to generate the address for transaction authentication and information transmission, as follows:

\[
T_{A-add} = \text{Hash}(A - \text{Publickey}); \quad A - \text{Publickey} = \text{Hash}(A - \text{PrivateKey})
\]

Among them, \(T_{A-add}\) stands for the address of node A, \text{Hash} for the encryption process to generate
node address, and $T_{A\text{-add}}$ for the result that is calculated after SHA256 and Base58. Then the node A broadcasts the purchase request information to the network:

$$M_{in,A} = (E_1 \oplus \{t_0, t_1\} \oplus A-Publickey \oplus T_{A\text{-add}})$$

(2)

Among them, $E_1$ stands for the purchase demand, $\{t_0, t_1\}$ for the period to purchase electricity resources. All the participating nodes in the transaction system are able to receive the transaction request information $M_{in,A}$ issued by the node A.

- User B accepts the transaction request issued by A, and on the basis of analysis of its own energy demand and energy supply, it is considered that the corresponding energy resource can be provided for user A in $\{t_0, t_1\}$. Node B will also generate the corresponding transaction authentication and information transmission address $T_{B\text{-add}}$ to send the response message:

$$M_{A\text{-add},B} = (E_2 \oplus \{t_0, t_1\} \oplus P_0 \oplus LT_{ID} \oplus \text{Sign}(E_1, \{t_0, t_1\}, LT) \oplus B-Publickey \oplus T_{B\text{-add}})$$

(3)

Among them, $E_2$ is the power supplied by B, $P_0$ is the quotation of B for the electricity transaction, $LT_{ID}$ is the record address of the last transaction information in the blockchain at Node B, $\text{Sign}(E_1, \{t_0, t_1\}, LT)$ is the encryption signature B through B-Publickey on the transaction response and the contents of last transaction. Because there are multiple power suppliers and multiple quotation, the information is encrypted with A-Publickey and sent to user A.

- After receiving the information sent by Node B, user A decrypt the message digest sent by B with its own private key A-Publickey to get the entire content of $M_{A\text{-add},B}$. At the same time, it gets the content information in the signature $\text{Sign}(E_1, \{t_0, t_1\}, LT)$ in addition, the $LT_{ID}$ and the corresponding Merkel tree can quickly locate the last transaction, verify whether there is a public key for B in this transaction, and extract the transaction information LT to compare with the signature content to ensure that the transaction is real, which can also verify that $M_{A\text{-add},B}$ is actually sent by node B.

The subjective behavior of the user will affect the effectiveness of the power resources, but the user can obtain the deviation between the amount of the agreement and the amount of the settlement in all transactions on the basis of the transaction information. And then according to the amount of deviation he can estimate the quality of the supplied power to determine whether he should amend his purchase amount. In addition, if there are multiple power resource supply nodes or individual supply nodes cannot meet the demand, then the EMS of node A needs to optimize his own purchase combination strategy according to the resource quotation and the available quantity of different nodes. In order to simplify the description of the information exchange and transaction process, we assume that the power supply of node B can meet the needs of node A, that is, $E_1 = E_2$.

- If A does not accept the quotation of B, it may be required that B provides a secondary offer, or terminate the transaction. In the process of price agreement, nodes A and B can still use the public key to encrypt the information and then send information to the target address.

If A accepts the quotation of B, A will send the contract script information to B. In the transaction, because after the transaction is completed, he overall output / energy characteristics of the user A and B will change, it is necessary to report the second level of EMS to adjust optimization boundaries of the user A and B. At the same time, in order to ensure that the IDR resources will not be "secondary payments", the script information must contain the signature of the regional energy Internet operator. The regional EMS should ensure that a user can only trade the power resource for one time in a transaction settlement cycle, that is, the output / energy characteristics reported to the second level EMS can only be modified once in one cycle to ensure the effectiveness of the transaction. Therefore,
the transaction information structure of the contract transaction should be:

\[ \text{Script}_1 = (\text{Sign}.A || \text{Sign}.B || \text{Sign}.DSO || (E_2, [t_1, t_2], P_i) \) \]  \hspace{1cm} (4)

After receiving Script\textsubscript{1}, the regional EMS will modify the output / energy curve reported by the users A and B. Till the time \( t_4 \), the script will trigger the energy resource of node B, and then EMS will read the actual output / energy curve of B to record. To the end of the transaction \( t_5 \), A and B need to confirm again:

\[ \text{Script}_2 = (\text{Sign}.A || \text{Sign}.B || \text{Sign}.DSO || E_3) \]  \hspace{1cm} (5)

Among them, \( E_3 \) is the actual amount of electricity trading. Once Script\textsubscript{2} is signed by three parties, then A needs to pay in accordance with the previous agreement to the cost of B. After the completion of the transaction, the transaction information written in formula 1 will be broadcast to the whole network. After all nodes have verified the transaction information, they can be written to the current block.

3.2. Pricing method

Through the entire power trading platform, we use Nbitcoin to carry out the sale of electricity. Nbitcoin uses distributed databases throughout the entire P2P transaction network nodes to manage currency issuance, record currency transactions and account balance information. In addition, it uses cryptographic design verification to repeat consumption to ensure the security of all aspects of currency circulation. In this trading market, unlike the technology that relies on the forecast and the market, the system operator charges the users according to the actual power usage situation and awards the users according to the actual situation of the electric power, so as to realize the whole transaction system based on the disperse digital currency, that is, the Nbitcoin.

![Diagram](image_url)

**Figure 3.** Example scenario. Copyright M. Mihaylov\textsuperscript{(12)}
Below we present a sample scenario, as shown in figure 3, which will help us visualize the whole process [10,11,12]. A user P generates a certain amount of electrical energy and feeds it to the grid while broadcasting the information to all nodes in the network. These nodes then update the P’s disclosure using the monetary function \( f(x) \) based on the rules of the distributed electricity market trading system recording. Thus, the function \( f(x) \) is responsible for generating and then entering the decentralized market in which the currency algorithm is generated. In addition, the local substation S connected to P measures the total energy in the gap to produce \( t_p \) and total consumption \( t_c \). The substation then transfers the \( g(x,t_p,t_c) \) currency calculation results publicly to the users. \( g(x,t_p,t_c) \) is the production price function defined by the EMS. Therefore, the user P that injects energy x can acquire a certain amount of electronic money. And the amount of money received depends only on the functions \( f \) and \( g \) and is not associated with the monetary value on the market. At any given time period, P can join the exchange market to sell its electronic currency to convert the legal currency. Here we will elaborate on this power trading system using Nbitcoin for the realization of electricity transactions.

In the process of power transactions, each user can first meet his own needs using the energy that he produces, and then the excess energy can be sent to the grid. The information on local electricity production and consumption is sent to the power substation of the energy Internet operator via a smart meter, which is then used to determine the rate of return on the energy produced by the user, in order to motivate the agent to balance supply and demand by means of reducing production and consumption peak. For example, in low demand or high output period, the cost of energy consumption is very low. Similarly, low supply and high demand will also promote the price rise. Therefore, every 15 minutes, we use the following methods to determine energy consumption and productivity. The price function paid to the electricity producer forms a bell curve, defined as follows:

\[
g(x,t_p,t_c) = \frac{x \cdot q_{t_p=t_c}}{(t_p-t_c)^a} \cdot e^{-a} \tag{5}
\]

Where \( q_{t_p=t_c} \) is the maximum reward rate obtained by the power producer for the power of \( x \) when the total supply \( t_p \) is equal to the total demand \( t_c \) and is defined by EMS; \( a \) is zoom factor when \( t_p \neq t_c \).

When the total energy production is equal to the total consumption, the function reaches the peak, \( g = x \cdot q_{t_p=t_c} \). In other words, when \( t_p >> t_c \) or \( t_p << t_c \), the producer is almost unable to get any reward.

In the actual operation, according to the actual situation, if we assume that the maximum incentive rate of 5%, the scaling factor of 2000, the bell curve of price function with the total supply and aggregate demand will be shown in figure 4. If we change the maximum reward rate to 7%, and zoom factor remains unchanged, the price function will be shown in figure 5. If the maximum incentive rate remains unchanged, the zoom factor becomes 500, the price function drawn graph will be shown in figure 6. As can be seen in the figure, when the total power supply in the electricity market is far greater than the total demand for electricity, the price of the electricity unit paid to the electricity producers is almost zero. As the total demand for electricity in the market increases, the electricity price increases. When the total supply is equal to the aggregate demand, the price reaches the highest value, and if the total demand for electricity increases further, the electricity price will drop, which will cause the electricity producers to produce more electricity to maintain the balance between supply and demand to make their own energy production profit reach the maximum, which is the basic principles of electricity price function. Under this principle, through the role of price mechanism, the balance of power supply and demand is promoted and the stability of the electricity market is maintained. When the maximum incentive rate is changed, the electricity price will produce a positive
correlation. When the scaling factor is changed, the steepness of the curve changes, and with the decrease of the scaling factor, the steepness of the price curve becomes higher. That means that the smaller the scaling factor, the greater the impact of electricity prices on the market.

$h(\cdot)$ is the price function that consumers need to pay when they buy electricity:

$$h(y, t_p, t_c) = \frac{y \cdot \tau_{t_c > t_p} \cdot t_c}{t_c + t_p}$$

(6)

Figure 4. Price function bell curve. Figure 5. The bell curve after changing the maximum reward rate.

Figure 6. The bell curve after changing the scaling factor.

Figure 7. The bell curve of consumers’ payment.

Where $\tau_{t_c > t_p}$ is the highest cost that the buyer needs to pay when the energy supply is low. When $t_c = t_p$, the buyer should pay $\frac{y \cdot \tau_{t_c > t_p}}{2}$ per KW * h. When $t_c << t_p$, $h$ approaches 0, thus when the production is too much, the spending of the power consumers is almost 0, which can promote energy consumption to transfer over-production period to balanced period. The price function curve that consumers need to pay when they buy electricity is shown in figure 7.

Similar to the Bitcoin trading system, the Nbitcoin currency in the electricity trading market is based on the blockchain technology that is not controlled by any central authority in its monetary value. Furthermore, the bitcoin in this trading system is generated by injecting electrical energy into the
grid. The price function \( f(x) \) depends only on the amount \( x \) of renewable energy injected into the grid. This number is broadcast to the network, for each node in the network to track each transaction and earnings situation. But the actual transaction user information is not open, that is, all income and transactions are anonymous. Bitcoin is obtained by the function \( f(x) \), defined as follows:

\[
f(x) = b \cdot x
\]

(7)

Where \( b \) is a constant indicating the ratio of the bitcoin that can be obtained through injecting a certain amount of electricity \( x \) by the electricity producer.

4. Conclusion

In the context of the energy Internet, the emergence of a large number of energy productive consumers will create a new business model, which means that energy P2P transactions will spring up, and decentralized power trading models will also be a big change. Based on the development trend of power transaction in energy Internet, we analyze the basic concepts and characteristics of distributed energy system and blockchain. Then, considering the problems existing in the current electricity market transaction and the problems that may arise in the future, we put forward the framework of the distributed electricity market based on the blockchain technology.

References

[1] Munsing E, Mather J and Moura S 2017 Blockchains for decentralized optimization of energy resources in microgrid networks (Working Papers)
[2] Nakamoto S 2009 Bitcoin: A peer-to-peer electronic cashsystem (Consulted, 2008)
[3] Mattila J, Seppala T, Naucler C, Stahl R, Tikkanen M, Badenlid A and Seppala J 2016 Industrial blockchain platforms: An exercise in use case development in the energy industry Eta Working Papers 43 10-1
[4] Bahrami S and Sheikhi A 2016 From demand response in smart grid toward Integrated demand response in smart energy hub IEEE Transactions on Smart Grid 7 650-8
[5] Swan M 2015 Blockchain: Blueprint for a New Economy 1st ed (O’Reilly Media)
[6] Zhang Y and Wen J 2016 The IoT electric business model: Using blockchain technology for the internet of things Peer-to-Peer Networking and Applications 2016 1-12
[7] Tanaka K and Nagakubo K 2017 Blockchain-based electricity trading with Digitalgrid router IEEE International Conference on Consumer Electronics (Taiwan) pp 201-2
[8] Zhang Y and Wen J 2015 An LoT electric business model based on the protocol of bitcoin International Conference on Intelligence in Next Generation Networks pp 184-91
[9] Kosba A, Miller A, Shi E, Wen Z and Papamanthou C 2016 Hawk: The blockchain model of cryptography and privacy-preserving smart contracts Security & Privacy 2016 839-58
[10] Mihaylov M, Jurado S, Moffaert K V, Avellana N and Nowe A 2014 NRG-X-Change: A novel mechanism for trading of renewable energy in smart grids International Conference on Smart Grids & Green It Systems 2014 101-10
[11] Kilanc G P and Or I 2017 A decision support tool for the analysis of pricing, investment and regulatory processes in a decentralized electricity market Energy Policy 2008 36 3036-44
[12] Mihaylov M, Jurado S and Avellana N 2014 NRGcoin: Virtual Currency for Trading of Renewable Energy in Smart Grids European Energy Market 2014 1-6