United Nations Educational, Scientific and Cultural Organization
联合国教育、科学及文化组织

International Knowledge Centre for Engineering Sciences and Technology under the Auspices of UNESCO
国际工程科技知识中心 由教科文组织支持

Energy Industry: Blockchain Technology (2021)

IKCEST General Platform Team

2022.04

IKCEST Sci-Tech Trend Report

http://ikcest.org/tidings_article-304898.htm

Energy Industry: Blockchain Technology

Institute of Blockchain Technology at Shanghai
Academy of Science and Technology

Shanghai Ruanzhong Information Technology Co., Ltd.

March 2022

Contents

I. Characteristics and Application Value of Blockchain Technology

1. Brief Introduction to Blockchain Technology

The Blockchain technology, also known as the Distributed Ledger Technology (DLT), generates and updates data using the Distributed Node Consensus Protocol (DNCP), guarantees the safety of data transmission and access using the cryptography, and programs and manipulates data using smart contracts composed of automation scripts and codes, featuring distributed storage, anti-counterfeiting, anti-tampering, transparency and authentication, and high reliability.

As a collective innovation technology integrating cryptography, game theory, network communication and other science and technology, the Blockchain has values in techniques, economics and social governance. From the perspective of techniques, multi-center trust can be realized by construction of a P2P network, orderly and tamper-proof shared ledger using cryptography and the DNCP. From the perspective of economics, the Blockchain has partially decentralized and distributed characteristics, which brings a new way of value transmission. Hence, participants can realize P2P value exchanges by greatly streamlining the intermediate links. From the perspective of social governance, the Blockchain can realize the orderly flow of data and values across

platforms, regions, systems, departments, businesses and borders, and can also support effective collaborative management and services. As one of the major impetuses to promote supply-side structural reform, the popularization and application of the Blockchain will create a brand-new business and service model, which is expected to build a new way of industrial cooperation, improving the efficiency of co-circulation to accelerate the process of social digitization.

1.1 The Birth of Blockchain

In 1980s, the Cypherpunk, an organization, initiated the cryptocurrency. One of the founders Timothy May put forward untraceable electronic money, the Crypto Credits, which is used to reward hackers who are committed to protecting people's privacy. In 1990, David Chaum proposed the Ecash, a cryptographic network payment system based on blind signatures, which pays attention to privacy security and is untraceable. In 1998, Dai Wei proposed the B-Money, an anonymous and distributed electronic cryptocurrency system. In 2005, Nick Szabo proposed the idea of the Bitgold. These early attempts of digital cryptocurrency failed without exception because consumers did not pay much attention to privacy and security on the Internet.

In 2008, the outbreak of the global financial crisis further promoted the R&D and experiment of distributed and P2P payment cryptocurrency.

On October 31, 2008, Satoshi Nakamoto released the whitepaper titled Bitcoin: A Peer-To-Peer Electronic Cash System. Its purpose is to explain a brand-new and decentralized P2P exchange system. The Blockchain is the basic technology to operate that system. Compared with the traditional centralized ledger technology, the operation of bitcoin network does not require any centralized organization. Instead, it constructs a Blockchain data structure that is difficult to be counterfeited, tampered with and traceable through P2P communication and transparent and credible rules, and manages distributed transaction processing. Its data is stored in blocks sequentially linked in a chain. The authenticity and integrity of data are guaranteed by digital signatures and integrity checks.

On January 3, 2009, the bitcoin system officially began to operate. Nakamoto successfully dug out the first batch of bitcoins (50 in total) from the foundation block. Bitcoin has become the first application based on the Blockchain technology. In 2010, the bitcoin exchange was born. On May 22, someone bought two pizzas with 10,000 bitcoins. This was the first time that people used bitcoin for physical transaction. Since then, the bitcoin has been circulated among a very small group. The Blockchain, as the underlying technology supporting the operation of bitcoin system, has also begun to enter the public’s view.

1.2 Development of Blockchain

The development of a technology must go through continuous updating and iteration. The development of Blockchain technology has gone through three stages: origin of technologies, Blockchain 1.0 and Blockchain 2.0. This section will mainly introduce these three stages and the development of Blockchain technology, as shown in Figure 1-1.

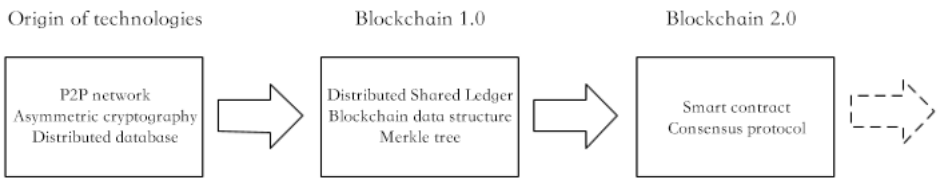

Figure 1-1 Development of Blockchain technology

1.2.1 Origin of Technologies

1) P2P (Peer To Peer) network

The P2P network, also known as P2P internet or P2P communication, is a decentralized networking technology connecting peer nodes compared with centralized network. It is the underlying network foundation of the Blockchain technology. Obviously different from the mode of centralized network central server serving the whole network, each node has equal importance in P2P network. Information or resources are transmitted amid the nodes through specific network protocols, as shown in Figure 1-2.

Figure 1-2 Network modes

2) Asymmetric cryptography

The asymmetric cryptography algorithm uses two keys to encrypt and decrypt messages. The keys refer to the Public Key and Private Key. The commonly used asymmetric cryptography algorithms include RSA, ECC and so on. The confidential process of asymmetric cryptography algorithm is shown in Figure 1-3. In a Blockchain, the Public Key and Private Key are usually used to create confidential communication amid peer nodes to ensure the authentication and verifiability of messages.

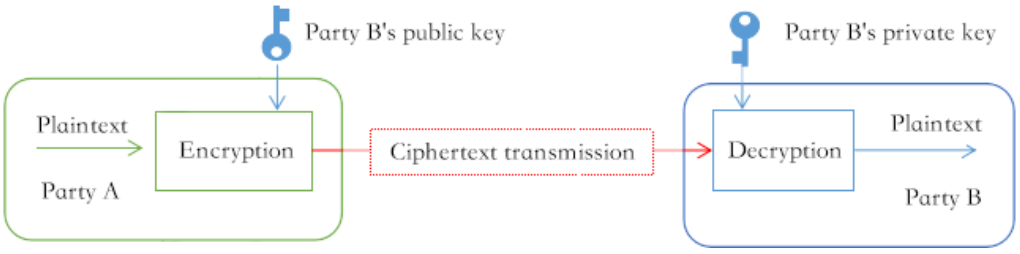

Figure 1-3 Decryption by asymmetric cryptography algorithm

3) Distributed database

A distributed database is a database in which data are stored across different physical locations. Logically speaking, the data belong to the same system and a physical location. But physically, they may be

dispersed over a network of interconnected computers. Therefore, a distributed database has two important characteristics: distribution and logical correlation. Based on the idea of distributed database, the Blockchain expands the scope of distribution, expanding the storage and maintenance of data from one physical location to multiple locations.

1.2.2 Blockchain 1.0

In January 2009, the official release of the Bitcoin marked the birth of Blockchain 1.0. Relying on the design of the Blockchain technology and the incentive mechanism, the Bitcoin can be successfully operated for more than 10 years in a completely distributed environment and without a single operation and maintenance management entity.

Basic technologies in Blockchain 1.0:

(1) Distributed Shared Ledger

The Distributed Shared Ledger refers to the distributed storage of the ledger on multiple servers. No matter where these servers are located, they can accurately and synchronously record every transaction that occurs in the entire network. Meanwhile, ledgers amid servers are synchronized through network communication. This is a data accounting method that does not need to be stored or confirmed by any centralized entity. All participants over the same network can obtain a unique, true copy of the ledger. Since ledgers are synchronized across the network,

arbitrary tampering in any ledger will be reflected in other immutable copies.

(2) Blockchain data structure

The Blockchain data structure is the structure of data storage in the underlying Blockchain of the Bitcoin, as shown in Figure 1-4. In the Bitcoin and other subsequently developed Blockchains, the smallest transaction unit recorded in the Blockchain is “Transaction” which represents financial activities such as transfers, payments, and exchanges initiated by users on the chain. A block is a transaction set consisting of one or more transactions by a specific node. Its storage structure is divided into two parts: the block header and the block body. The block body contains all the transactions of this block organized and stored in the form of the Merkle Trees. The block header contains the previous block hash, version, timestamp, difficulty target, nonce and the Merkle Tree Root. Since the block header contains the hash value of the previous block processed by the cryptographic hash function (CHF), a Blockchain storage structure with a totally ordered sequence of events is logically formed.

In a Blockchain, the CHF plays an important role. It is a one-way function and collision resistance, so it is quick to compute the hash value for any given message and infeasible to reverse the process that generated the given hash value. In addition, a small change to a string should

change the hash value so extensively that a new hash value appears uncorrelated with the old hash value. Due to this nature and the Blockchain storage structure, the attacker will be in great difficulty in tampering transaction messages in old blocks. Once the message in an old block is tampered with, the hash value of the block will change. This will cause the hash values of all blocks after the block to change. The attacker must craft the hash values of the block and beyond to change the transaction messages.

(3) Merkle Tree

A Merkle Tree is one of basic components of the Blockchain, as shown in Figure 1-4. Taking the Bitcoin as an example, a Merkle Tree Root in a block body is a unique hash created by hashing all the transaction hashes together in pairs.

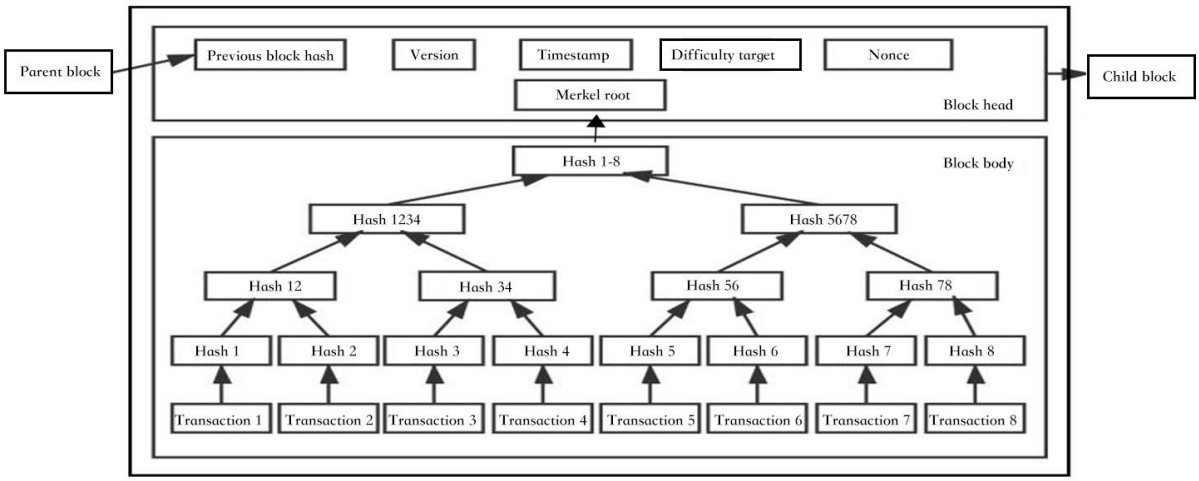

Figure 1-4 Data storage structure in Blockchain 1.0

The Merkle tree, named after its creator Ralph Merkle, is a tree in which every “leaf” (node) is labelled with the cryptographic hash of a

data block and is a generalization of a hash list and a hash chain. In a Blockchain, a transaction is a block, which is a leaf node of a Merkle Tree. As shown in Figure 1-6, blocks are grouped in pairs from bottom to top. A new data structure containing the hash pointer of each block for each group is built until a single hash pointer is created, namely the root hash. Under such a mechanism, the root hash pointer can be traced back to any data block, ensuring that the original transaction has not been tampered with. Once an attacker tampers with data blocks at the bottom of the Merkle Tree, the hash pointers of the previous hash will not match. So, any tampering behavior will be detected.

(4) Proof Of Work (PoW)

A consensus protocol describes the process in which each node in the system participates in the decision-making to reach a consensus. In a Blockchain, the distributed system, it is necessary to establish a trust mechanism amid nodes that do not trust each other in order to verify and confirm each transaction, and establish a self-trusting network amid nodes through technical endorsement.

The PoW is the consensus protocol of the Bitcoin in the Blockchain 1.0. Bitcoin has two incentive mechanisms to encourage nodes to keep records. One is the block incentive, namely the “mining”. The accounting node that creates a block can add a special transaction to the block. This transaction is a coinage transaction. The node creating the block can get

the income. The other is the transaction fee, i.e., a part of the Bitcoin transaction fee is paid to the accounting node as the incentive. Since the Bitcoin has been recognized for its value by some countries and commercial institutions, the design of its incentive mechanism enables all accounting nodes that operate and maintain the Bitcoin system to have incentives to keep records honestly and maintain the normal operation of the system.

1.2.3 Blockchain 2.0

In order to solve the problems of limited application development, low throughput performance and high energy consumption in the Blockchain 1.0, the technical structure of the Blockchain is being further adjusted and improved. The birth of the Ethereum in July 2015 marked the entry of Blockchain 2.0. The Ethereum introduces the concept of smart contracts. It supports Turing Complete programming language Solidity to write smart contracts and distributed applications. With the support of the smart contract system, the Blockchain begins to extend from a single accounting field to finance, people’s livelihood and other fields related to contract functions. In addition, with the birth of the Hyperledger Fabric, IBM's hyperledger project and a consortium Blockchain, the application of Blockchain has been further expanded to a wide range of scenarios including finance, government affairs and medical care that require higher regulatory compliance, data security and

performance. This also indicates that application of the Blockchain technology has gradually developed from programmable money to programmable finance.

The Blockchain 2.0 has the following key characteristics:

1) Smart contract

The smart contract is a typical feature of Blockchain 2.0. In 1995, Nick Szabo, a cross-disciplinary legal scholar, proposed the concept of smart contract which refers to “a set of promises, specified in digital form, including protocols within which the parties perform on these promises”. However, due to the lack of a trusted operating environment in the early days, the smart contract was not actually applied. Since the birth of the Bitcoin, people have realized that the Blockchain, the underpinning technology of the Bitcoin, can naturally provide a trusted operating environment for smart contract. Thus, the smart contract becomes a computer program on the Blockchain. When the conditions in the contract are met, it will automatically trigger the execution of the contract content.

2) Diversity of consensus protocol

With the increasing Blockchain application scenarios, consensus protocols adapted to different scenarios have been created successively, including the Practical Byzantine Fault Tolerance (PBFT) commonly used in the consortium Blockchain and the Delegated Proof Of Stake

(Dpos) commonly used in the public Blockchain.

The PBFT can well solve the node downtime and transmission errors in distributed systems. But due to the early Byzantine algorithm was extremely complex, the application range was limited. It was not until the PBFT was proposed in 1999 that the complexity was reduced to the polynomial level, leading to wider application.

In the PBFT, there is a concept of the View. In each View, all nodes run under the same configuration, and there is only one master node and other backup nodes. The master node is responsible for sorting the client's requests and sending them to the backup node in order. The backup node will check whether there is any exception in the order sorted by the master node. If an exception occurs, the View Change mechanism will be triggered, the next node being the master node. A new View will be created.

In the PBFT, the process from a client sending a request to receiving a reply is shown in Figure 1-5. Information exchanges occur amid servers three times. The whole process includes five stages:

(1) Request: The client sends a request to the master node in the format of the <REQUEST, O, T, C>, where O is the action executed, T is the local time, and C is the client number;

(2) Pre-Prepare: The master node receiving the request records it and numbers it, and then broadcasts a Pre-Prepare message to other backup

nodes in the format of <PRE-PREPARE, V, N, D>. Among which, V is the View where the request is located, N is the request number given by the master node, and D is the Digest number. If the backup node is located in the same View as V, and has never received the Pre-Prepare message with the same N number but different Digest number in the same View, the message is accepted and enters the Prepare stage;

(3) Prepare: The backup node entering this stage will broadcast a Prepare message and receive Prepare messages sent by other nodes in the format of <PREPARE, V, N, D, I>, where I is the number of the backup node. If the node receives 2f (F is the maximum number of nodes that can allow errors in the system) Prepare messages and their V, N and D are the same, the node will enter the Commit stage;

(4) Commit: The backup node entering this stage will broadcast a Commit message and receive Commit messages sent by other nodes in the format of <COMMIT, V, N, I>. After receiving 2f+1 (including the node itself) Commit messages with the same V and N, the node can execute the request after other smaller-numbered requests being executed;

(5) Reply: The node replies to the client in the format of <REPLY, V, T, C, I, R>, where V is the View where the request is located, T is the timestamp corresponding to the request, I is the number of the reply node and R is the execution result. When the client receives the replies from F+1 nodes, and the time stamp and execution result corresponding to the

request are the same, it is considered that the request has been recorded and processed by the system. If the client does not receive enough replies due to network delays, etc., the request is repeated to the server. If the request has already been executed, the server simply sends the reply message repeatedly.

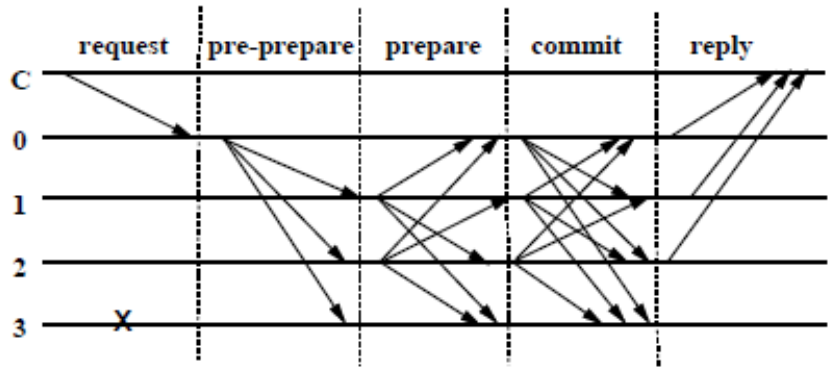

Figure1-5 Execution process of the PBFT

In addition, after the node executes the request, it needs to perform garbage collection to clear the previously recorded messages of the request. Otherwise, it will occupy system resources. However, due to network delay and other reasons, different nodes may be in different states, and it is necessary to reach a consensus over the network before clearing the records. Therefore, a Check Point protocol is also designed in the PBFT.

1.2.4 Exploration on Frontiers of Technology

With the Blockchain 2.0, the application of the Blockchain is not only limited to the financial field, but extending to the social governance and intelligence, including the Internet of Things, public welfare, medical

care, education, auditing, notarization, judicial arbitration and other fields. However, with the increasing expansion of the application of the Blockchain, the commercial requirements for the underpinning technology of the Blockchain are also increasing. The Blockchain technology after the 2.0 stage begins to explore how to improve the performance, optimize the structure, and realize cross-chain interoperability and other functions.

(1) The Impossible Triangle of Blockchain

Vitalik Buterin, the founder of the Ethereum, proposed the "Impossible Triangle" of the Blockchain in Shardingfaq, as shown in Figure 1-6. What proposed is that Blockchain system cannot simultaneously combine decentralization, performance and security. Among which, performance is defined as being able to process on-chain transaction, namely the number of transactions per second (TPS). Since the three angles cannot be satisfied at the same time, the design of the Blockchain can only choose two. For example, the Bitcoin chooses to sacrifice some performance for the sake of decentralization and security. The consortium Blockchain is essentially a compromise of "partial centralization" or "multi-centralization" for the sake of security and performance. Faced with such technical bottleneck, the development of Blockchain technology can only constantly think about how to balance the relationship between the three.

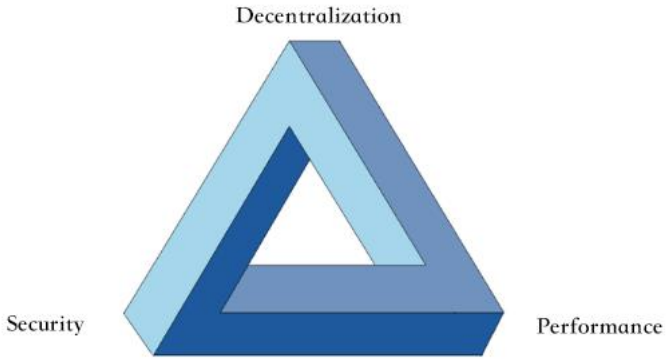

Figure 1-6 The Impossible Triangle of Blockchain

(2) Directed Acyclic Graph

The Directed Acyclic Graph (DAG) is a data structure in the computer field. Its unique topology is often applied to the dynamic programming (DP), data compression and other algorithmic scenarios.

Since the traditional single-chain structure of the Blockchain determines that the packaged blocks cannot be executed simultaneously, which greatly restricts the performance of transaction processing, some people propose to use the DAG to store transactions on the Blockchain. This changes the traditional Blockchain structure into mesh topology, solving the performance of Blockchain. Some scholars pointed out that, compared with the traditional chain structure of the Blockchain, the DAG Blockchain can package N blocks simultaneously when the block packaging time remains unchanged, and the transaction volume over the network can accommodate N times, as shown in the figure 1-7.

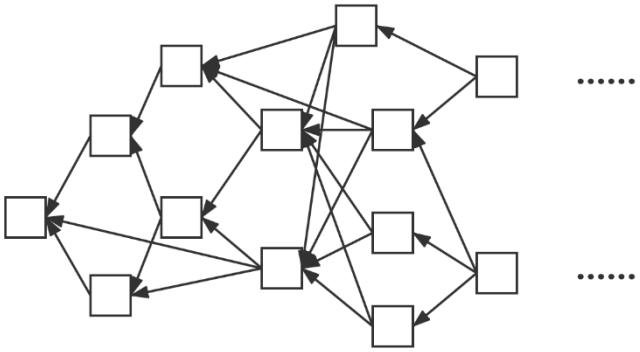

Figure 1-7 DAG structure

The Hashgraph, developed by the computer scientist Leemon Baird, uses the DAG to organize transactions in a chronological order. The transactions in the DAG do not require miners to verify and abandon the transaction in the traditional Blockchain in the form of block connection. It means that the transaction processing speed is faster than that of the traditional Blockchain.

(3) Sharding

In traditional Blockchains, only one block is usually generated in a period of time. The nodes participating in the consensus over the entire network will compete for the only accounting right, or reach a consensus on a newly generated block. In order to seek higher scalability, expansion can be accomplished by increasing the block production speed or increasing the block size. However, these two methods will bring about frequent forks or network delays. The sharding provides another solution for Blockchain expansion, which increases throughput by changing the way blocks are verified in the network.

The sharding in Blockchain is inspired by that in the traditional database which refers to dividing data into multiple parts and distributing them to different servers. For sharding in Blockchain, nodes in the network will be divided into different shards, and transactions in the network will also be assigned to different shards for processing. Therefore, the original logic of processing all transactions in the entire network by consensus nodes in the Blockchain has become that each node only processes a small portion of transmitted transactions, and that nodes in different sharded networks will execute simultaneously. This way of sharding increases the transactions that can be processed and verified on the Blockchain at the same time, achieving the purpose of expanding the throughput of the Blockchain. At present, there are three main sharding methods: Network Sharding, Transaction Sharding and State Sharding.

(4) Cross-chain technology

If the consensus protocol is the soul of Blockchain, the cross-chain technology is the bridge to realize the Internet of Value, and a good solution to save the consortium chain from the scattered islands.

Cross-chain is to allow digital assets, valuable information, services, resources and other “values” on the Blockchain to cross the gap amid chains for direct transmission. Essentially, there is no way to directly transfer value between two unrelated Blockchains. But for a user, the

assets stored by the user on one Blockchain can be exchanged for those on another Blockchain in some form. This is the cross-chain of value. When one Blockchain can trigger relevant responses based on transactions on another Blockchain, it is the cross-chain of information.

At present, the main cross-chain technologies include: Notary Schemes, Sidechains/Relays, Hash-Locking, and Distributed Control Rights Management (DCRM) technology. For example, the main concept of the Notary Mechanism is to find a third party trusted by both chains to declare a specific transaction that occurs on each chain. The third party is the notary, which can be an organization or a Blockchain. Compared with the Sidechains, the Relays is more advanced. It can make all the participating Blockchains interoperable through a specific protocol, realizing the cross-chain of the entire Blockchain ecosystem.

(5) Privacy protection

Although multi-party accounting in Blockchains make the ledger open and transparent among them, the security and privacy of users' transmitted data must be protected. At present, there are some solutions to protect user privacy and security through cryptography, secure multi-party computing, and data partitioning mechanisms. These technologies can be used to protect data privacy, signer privacy, address privacy and other privacy. However, the means of protecting privacy and security are far more than that. With the rapid development of

cryptography and Blockchain technology, more new technologies will emerge. At the same time, it should be realized that no single technology can realize complete protection, and multiple technologies need to be combined to effectively protect user privacy. The following will take the Zero-Knowledge Proof as an example to introduce relevant methods of Blockchain privacy protection.

The Zero-Knowledge Proof was proposed by S. Goldwasser, S. Micali and C. Rackoff in the early 1980s. It refers that the prover can convince the verifier that an assertion is correct without providing any valid information to the verifier. The Zero-Knowledge Proof in early times requires the prover and the verifier to complete the verification by exchanging messages. This process is called “Interactive Zero-Knowledge Proof”. In the late 1980s, Blum et al. proposed to use a common reference string (CRS) to realize Zero-Knowledge Proof. Only if the prover sends a message once, the verifier can verify the correctness of the message without interacting with the prover. The process is called “Non-Interactive Zero-Knowledge Proof”, which is known as the “Zero-Knowledge Proof” in Blockchain system.

1.3 Types of Blockchain

According to the access restrictions of Blockchain system, there are three types of Blockchain networks including public Blockchains,

consortium Blockchains and private Blockchains. They are applied to different scenarios.

1.3.1 Public Blockchain

As the name implies, a public Blockchain is accessed to the whole society, but does not belong to any individual or organization, such as the Bitcoin Blockchain and the Ethereum Blockchain. It has absolutely no access restrictions. Each node can freely join and withdraw from the network, and participate in the reading and writing process of data on the Blockchain. Initially, the Blockchain was in the form of a public Blockchain, and almost had no access restriction. As long as you have a computer that can be connected to the Internet, you can access to the public Blockchain system, and join or withdraw from it freely. In the public Blockchain, any transaction behavior of each user will be hashed and disclosed to the nodes of the entire network. The nodes can verify the authenticity of the transaction records over the entire network, participate in the consensus protocol of each transaction in the system, and initiate their own transactions.

Acting maliciously in the public Blockchain network needs extremely high costs. As a highly distributed system, the nodes in the public Blockchain will back up a local ledger. If someone wants to maliciously tamper with a certain data, it is necessary to tamper with the

data in other nodes and record them to the longest chain. In addition, the data linked through cryptography in the Blockchain is naturally difficult to be tampered with, which makes tampering with data technologically difficult and economically impractical in the public Blockchain network. For example, in the Bitcoin network, only with at least 51% of the computing power over the entire network can the longest chain be tampered with, which needs extremely high costs.

1.3.2 Private Blockchain

The private Blockchain is a relatively closed or centrally controlled Blockchain network. If the public Blockchain is compared to the Internet, the private Blockchain is like a local area network only allowing specific users to join. The reading and writing permission of each node is controlled by the organization. Users are authorized by the organization, so they can not only enjoy the advantages of information traceability and not easy to lose brought by Blockchain technology, but also do not have to worry about the access of unrelated personnel, resulting in information leakage.

The private Blockchain is a highly centralized system. Users need permission to access, only some of whom can rewrite data and participate in accounting. Compared with the public Blockchain and the consortium Blockchain, the control of the private chain is more centralized. The

reason is that the nodes are usually less, and that a complicated consensus process is not required. So, a certain or a few nodes may determine the result of the ledger accounting. Relatively speaking, all nodes of relatively centralized private Blockchains are controllable and have a relatively high degree of trust, which can improve their performance to a certain extent. Also, because not all nodes need to participate in the consensus protocol of every transaction, the transaction costs on a private Blockchain are relatively low.

A private Blockchain also has advantages and applicable scenarios. It can prevent the malicious destruction of data by a single node in the system. Even if there is an error, it can be quickly checked and repaired. Many large-scale financial enterprises will utilize private Blockchain technology in internal database management and auditing. Some public sectors also utilize the technology in the budgets, statistics and scenarios including registered by the government, but the public has the right to supervise.

1.3.3 Consortium Blockchain

The unrestricted permission of the public Blockchain and the overly strict permission the private Blockchain are not applicable to many business scenarios. The consortium Blockchain was created therefore. The degree of permission for the consortium Blockchain is between the

public Blockchain and the private Blockchain. It is only open to a specific group related to the business. The relationship among the members of the group is not so close, so it is impossible to use a private Blockchain network to share all the information. A consortium Blockchain is usually formed by enterprises with common interests or by related institutions, forming a consortium to join the network. Each node on the consortium Blockchain usually has a corresponding entity or organization, which can only join or withdraw from the network with authorization and verification. Compared with the private Blockchain and the public Blockchain, the consortium chain has a wider range of commercial applications, such as the well-known Hyperledger Fabric, the R3 consortium and the FISCO.

In addition, the data on a consortium Blockchain can be partially opened to the public, and limited API interfaces can be provided for execution. So, some non-core users can also use the consortium Blockchain system to meet their needs, access to data and collaborate conveniently. This can ensure that the transaction information and data are updated in real time and shared with all users in the consortium Blockchain.

In conclusion, following Chart 1-1 shows the comparisons amid above three Blockchains:

Chart 1-1 Comparisons amid three Blockchains

Item	Public Blockchain	Consortium Blockchain	Private Blockchain
Participant	Anyone	Authorized corporation and organization	An individual or individuals within an organization
Accounting	Anyone	Coordinated aid participants	Determined in the system
Authority	Decentralization	Multi-party centralization	Centralization
Advantages	Self-trust	High performance and low transaction costs	Transparent and traceable
Examples	Bitcoin	Liquidating	Auditing
Transaction speed	7~1000 times/s	10000+ times/s	1000+ times/s

1.4 Uses and Characteristics of Blockchain

1.4.1 Uses of Blockchain

A Blockchain, an integrated innovative technology, is a fusion of many scientific technologies such as cryptography, game theory and network communication, with the characteristics of decentralization, transparency, openness, immutability, and privacy. It is considered as the most disruptive technological innovation since invention of the Internet. Because the nature of the Blockchain is consistent with the characteristics of the information society, including the weak control, distributed centers,

autonomous mechanism, network architecture and coupling connection, the Blockchain can perfectly solve the problem of reconstructing social trust. If the artificial intelligence is a productivity revolution, Blockchain is a revolution in production relations, realizing the transmission from the Internet of Information to the Internet of Value. The value system of the entire society will also be reconstructed.

Blockchain is not only oriented to specific application scenarios such as digital asset exchange, judicial arbitration, and the Internet of Things, but will also serve as the infrastructure for future distributed commercial Blockchain interconnection, promoting cross-industry, cross-institution, and cross-region exchanges and interconnection.

1.4.2 Characteristics of Blockchain

(1) Decentralization

Decentralization means that there is no centralized node or management organization in the Blockchain network. Each node is highly autonomous and has equal rights and status. In the Internet era, the centralized organization of application software has won the absolute trust of the public. But once the organization fails due to human management negligence or hackers' attack, it is prone to occurring single points of failure. The Blockchain system has the advantages of high fault tolerance and attack resistance due to its distributed storage. The

“decentralization” of the Blockchain does not advocate non-central management and non-supervisory control, but distributed shared storage, which enables P2P transactions.

(2) Transparency

The transparency of the Blockchain means that, for the entire network nodes, the addition and update operations of data on the Blockchain are transparent, which will be recorded over the entire network. Also, the Blockchain actively adopts open source, open rules and high social participation, the entire network nodes can censor and trace relevant records. It should be noted that transparency and privacy are not in conflict. To be specific, “transparency” does not mean that any party on the Blockchain can see the transaction content and data over the entire network, resulting in privacy leakage. The Blockchain utilizes cryptography, multi-party secure computing and other technologies to protect the privacy of data. This is the trustworthy foundation of the Blockchain system.

(3) Openness

The openness of Blockchain is mainly reflected in three aspects: openness of data, organizational structure and ecology. Openness of data means that stakeholders can jointly store and maintain data. The openness of the organizational structure is reflected in the fact that the Blockchain system allows new stakeholders to join it more easily, which is conducive

to the expansion of business scale. The openness of the ecology means that various industries and businesses can be more closely linked through the Blockchain.

(4) Immutability

There are two sets of encryption mechanisms in the Blockchain to prevent tampering with records. One is to use Merkle Tree to encrypt transaction records. When the underlying data changes, the Merkle Tree Root will be changed. The other is that the fresh block includes the hash value of the previous one, so there forming linking relationship between blocks. If you want to change the transaction data of the previous block, you must reconstruct the transaction records and hash values of all previous blocks. This is extremely difficult. So, the stability and reliability of data on the Blockchain is extremely high.

(5) Privacy

Although all data records and update operations in the Blockchain are open to the consensus nodes over the entire network, transactions are executed anonymously. In order to further protect transaction data and the counterparty’s information, cryptographic methods such as mixed signature, ring signature, homomorphic encryption, and Zero-Knowledge Proof can be adopted, and data controllability can also be improved by means of data isolation and authorized access.

2. Application Value of Blockchain in Energy Industry

Energy Internet is a networked physical system that directly or indirectly connects the production, transmission, utility, storage and conversion devices of various primary and secondary energy with their information, communication, control and protection devices, taking the electrical grid as the backbone and platform. It is the deep integration and development of a new generation of energy system and Internet technology, and also the focus and innovation frontier of the current academic and industrial circles at home and abroad. As an information technology, Blockchain deeply integrates the information flow with the value flow of the Energy Internet through the revolution of information collection, transmission, storage, use and authentication, realizing the Internet of Value. Also, it has profoundly changed the energy flow through the reorganization of the information flow, which has a very important role and significance.

The information and data in the Energy Internet is widely recognized as the first productivity. The Energy Internet can be described from the following five perspectives: device, communication, data, application and business.

Device: It is not only the infrastructure of energy production, delivery and consumption, but the information perception network, including various equipment and components required for information

collection, relay transmission and exchange during the operation of the entire Energy Internet.

Communication: It is the nervous system for the entire Energy Internet system. It can connect various devices in the Device into an overall information system facilitated by the communication network. Also, it can effectively cooperate with the private line network and the public network. While ensuring the stable operation of the network channel for information transmission, it is supplemented by certain security protection strategies.

Data: All kinds of information and data accumulated during the entire operation of the Energy Internet are stored in the Data. Different from the Device and the Communication, the Data is not necessarily a specific item. It can not only be a specific large-scale data center, but also be a local cloud composed of dynamically networked IoT devices.

Application: It is the interface between the users of the Internet Energy (including the consumers, producers and managers) and various applications as well as systems for the Internet Energy. Its functions are directly provided for the users on the basis of the Device, Communication and Data, completing all kinds of work that users want to on the Internet.

Business: It is established on the basis of the Application and collects various application on a platform. It provides commercial services for users, including but not limited to accounts, payment,

transaction, management and social communication. But, the Business is not necessary for all Energy Internet system.

2.1 Guarantee for the Authenticity and Reliability of Information on the Energy Internet

The energy industry has the characteristics of a long industrial chain, many participants, complex operation process and many transaction settlements, which is highly similar with the Blockchain for its decentralized (distributed) data storage, credibility, traceability, immutability, and smart-contract function. So, the energy industry and the Blockchain may integrate with each other.

The application of Blockchain in the Energy Internet will create following values for the development of energy industry.

The first value is to guarantee the authenticity of information. Energy transaction participants can write the transaction method and other commercial terms in the contract by codes into the transaction service with the Blockchain as the core. Therefore, the system will automatically conduct relevant transactions according to the content of the contract agreed and authorized by both parties. Neither the service provider nor the consumer needs to worry that the transaction operation mechanism will be changed at will due to human factors. This ensures that the information will not be tampered with and the authenticity of the

transaction information.

The second value is to guarantee the reliability, forming secure and reliable shared ledger. Since the Blockchain technology permanently records all transaction behaviors of participants in the form of accounting and breaks the independent accounting model of different energy participating institutions in the past, this avoids many restrictions on confirming transaction records. Participants can check the transaction records authorized to be checked on the shared ledger system to ensure the transparency, openness and authenticity of transaction records.

The third value is to effectively protect privacy of traders. Although Blockchain technology will automatically record all transaction data of transaction participants, the participants do not need to bundle personal data with the transaction information, and can specify which transaction information can be authorized to check. This cannot only effectively protect privacy of traders, but also meet the application needs of various businesses for data.

The third value is to facilitate the formation of transaction consensus. Regardless of a participant joining the Blockchain anonymously or publicly and initiating a transaction, all the other participants will receive the transaction information simultaneously. At the same time, the information will be verified via the consensus algorithm applied to Blockchain technology, avoiding human interference.

The fifth value is to eradicate key problems in procedures of energy industry. At present, efficiency bottleneck, transaction delay and operation risk commonly exist in business procedures, which may be solved via Blockchain technology to a large extent. For example, the manual operation, manual verification and approval may be automated processed via the Blockchain. The paper contract may be replaced by the smart contract. Losses will not occur in the transaction due to system faults anymore.

2.2 Guarantee for the Security of Energy Data

Blockchain technology is significant for security of network and operation. With the development of the IoT, energy enterprises worldwide are strengthening the integration of energy assets and information technologies. More and more devices for data collection, processing and transmission are installed to provide enterprises with services on information management and control systems. The centralized management for data is relatively vulnerable to external attacks. Once it is successfully attacked, electricity and energy security for the society will be greatly threatened. To make it worse, it will cause fundamental influence to the national security. These issues may be solved by the immutability of Blockchains, which can monitor the regulation of pipeline network and other infrastructure, and the integrity of operation

systems. If the systems occur potential security issues, automated warnings will be released. This will avoid human errors and better guarantee the security of infrastructure.

Take the safety production scenario on the Blockchain technology applied to the State Grid as an example. Based on the Blockchain-based evidence including the safety supervision, network security and other device information, defense information and warning mechanisms, the check on the Blockchain may achieve full-state diagnosis of the operation network. This will ensure that the security events can be monitored and traced. In the field of the network security defense, the State Grid Electronic Commerce Company has stored millions of log data on security devices and systems, creating the warning system. Once the log data are tampered with, the system will release warnings immediately to reduce potential security risks.

2.3 Fundamental Guarantee for P2P Transactions

In the distributed energy operation, distributed database and accounting mechanism distributed in each node are created utilizing the distributed algorithm in the Blockchain. This will achieve data synchronization over the entire network via the Internet, and maximumly match characteristics of the distributed energy system through perspectives of functions, objects and attributes. Also, it will solve

technological bottlenecks in transaction pricing, risk measurement, consumption assessment, scheduling strategies and settlements.

The Blockchain for the distributed energy operation can store data from all nodes and key parameters of network, such as power/electricity flow data, scheduling data and settlement data.

A Blockchain can assist in executing the decentralized decision-making of electricity distribution. The decision-making depends on the coordination of each node and scheduling module in the distributed energy system, which can ensure that the system is always operating at an efficient level. It also realizes multi-module collaborative autonomy, where the decision-making data is recorded based on the Blockchain, and the decision-making mechanism is given by the artificial intelligence machine and executed through operation devices in the physical network.

The energy transactions on a Blockchain do not interfere with the common counterparts, so to a large extent it solves the trust issue, reduces the credit risk and improves credibility of the transaction subject. The energy transactions on a Blockchain form all kinds of “energy blocks” which record data including the flow data, scheduling data, and data for the billing settlement and the assessment for nodes trust. Those data are uniformly packaged, distributed and recorded on a Blockchain where the data are immutable, traceable and asymmetrically encrypted.

2.4 Trust Basis for Carbon Transactions

In the carbon market, the authenticity and transparency of carbon-controlling enterprises' carbon emission data, quotas along with the quantity, price and data of CCER is the most important. The central server cannot guarantee the data security, while institutions and individuals are not able to really participate in due to the non-transparency of information. To make it worse, the average development process of traditional carbon assets is over one year, which is a quite long period. The process interferes with the carbon-controlling enterprises, governmental regulators, exchanges for carbon assets, and third-party verification and certification organizations, each of which exists delivery of many documents. It is prone to errors and affects accuracy of subsequent structures.

A Blockchain has the characteristics of decentralization, self-trust, open, transparency, immutability, collective maintenance and privacy. Based on technologies including the distributed data store, consensus protocol and smart contract, it ensures the safety storage and interaction of transaction data and regulates behaviors of the participants during the process of a carbon transaction, which promote fair, safe and effective operation of a carbon-transaction market. It is proposed to establish the Blockchain network for carbon transactions as well as a Blockchain-based full-process management and protection mechanism of

“right conformation-transaction-right protection-punishment”.

Clear the “unique DNA” for a user’s identity. Based on its own type of node in the Blockchain network for a carbon transaction, the user submits carbon quotas and other information to register. After the verification of a third-party CA agency with the authority, the user will be issued with the digital certificate as its unified mark for identity.

Facilitate effective and transparent transaction quotas. The transaction nodes submit the quota quantity and transaction quotation to the Blockchain network for carbon transactions. By utilizing the Blockchain technology, rules for carbon transactions will be programmed into smart contracts. The contracts will be automatedly executed if the transaction information is matched, and will update the transaction records into the Blockchain. The Blockchain-based carbon transaction has following advantages. The anonymous transaction will protect users’ privacy and security; the collective maintenance for transaction data will make the transaction fair and transparent, which is convenient for participants and regulators to verify; and the decentralized P2P transaction will reduce time and trust costs.

Improve the prevention mechanism for breach of contract and right protection. For participants failing to perform the contract in a carbon transaction, the Blockchain can trace the transaction, store the data and rate the credit to support users and supervisory and judicial organs to

protect their rights. The timestamps and hash values can ensure the authenticity, relevance and legality of digital data, which will ensure the admissibility and probative power of evidence when presenting evidence for right protection, reducing relevant costs. Moreover, the asymmetric encryption technology can guarantee the transmission security. It is proposed to establish a consortium Blockchain for a carbon transaction where the transaction users, carbon exchanges, regulators, industry management organs, Internet courts and arbitration institutions serve as the nodes. This can share the digital data and transaction procedures to establish an effective right protection mechanism. Also, it is recommended to introduce a credit rating system. To be specific, the default information will be recorded in the Blockchain, which will influence the credit rating and further the transaction priority. This system will force the transaction participants to have credible transactions in order to reduce the negative effects of defaults.

Enhance the deterrence of transaction penalties. In the Blockchain network for a carbon transaction, each node not only includes the basic transaction information, but a proportioned deposit. The deposit will be automatically transferred if a transaction default occurs. Otherwise, the accounts of relevant users will be frozen and cancelled. In the annual settlement, the carbon-controlling enterprise with greater carbon emission than the quota settlement will be penalized based on the smart contract.

The “Blockchain + carbon transaction” is conducive to the fair and effective development of the carbon market, which will reduce false transactions and datum frauds. Moreover, the artificial intelligence, big data, cloud computing and other technologies can also provide services for carbon transactions to achieve a healthy and sustainable development.

II. Status and Analysis of Blockchain Application in Energy and Power Industry

Blockchain technology has become a hot technology to promote the digitalization of the energy and power industry, and a large part of the Blockchain projects are related to renewable energy. According to the report titled the “Blockchain-Innovation Landscape Brief” released by the International Renewable Energy Agency (IRENA) in 2019, more than 46% of the world’s energy Blockchain companies are located in Europe. And, the power industry worldwide has launched a total of 234 Blockchain projects where more than half (58.5%) are related to three areas: energy trading platforms, energy project financing and green certificate issuance. The application areas of the remaining projects include payment solutions, data management, charging facilities for electric vehicles, distributed energy platforms and other areas. The IRENA has classified recent Blockchain projects in the power industry as aforementioned, identifying several major application areas such as power trading, electrical grid

management and system operation, financing for renewable energy projects and green certificate management.

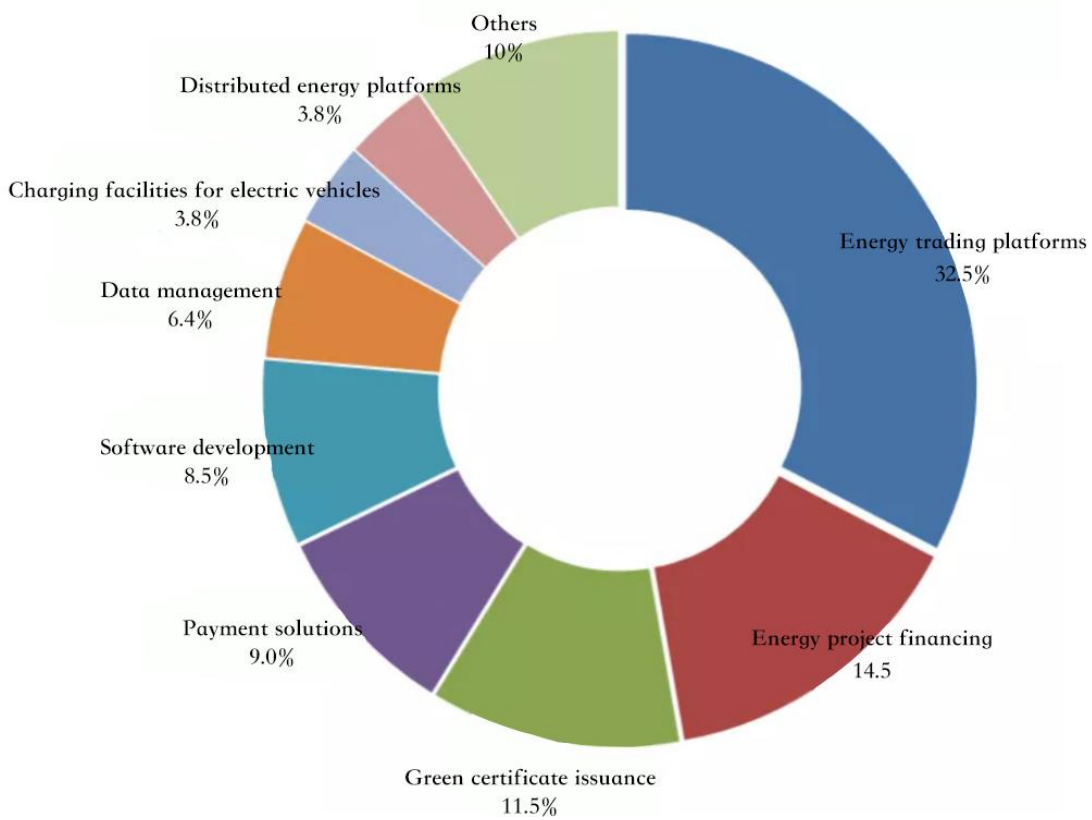

Figure 2-1 Blockchain applications in energy and power industry

1. Blockchain-based Green Power Traceability Platform for Beijing Winter Olympics

In order to fully implement the ecological civilization proposed by President Xi Jinping and the Winter Olympic concept of “green, sharing, openness and integrity”, and to respond to the idea of “carbon peaking and carbon neutrality”, the Blockchain technology is applied to the green power traceability for the Beijing Winter Olympics to make it an important platform and window to demonstrate China’s green development idea by leveraging the technology.

Based on Blockchain technology, the efforts extend to connecting the full chain of information flow of green power production, transmission, transaction and consumption, creating a credible and efficient management and control platform for green power traceability, and realizing that the whole process is visible, controllable and traceable. Aiming at relevant government authorities, regulatory agencies and related enterprises, the platform can effectively monitor the Blockchain for the key process of green power of the Winter Olympics from production to consumption so as to reduce the risk of data transmission loss and tampering. It also provides credible proof on 100% green power coverage for the Winter Olympics venues to achieve a real-time, visual and multi-dimensional perception of the Beijing Green Winter Olympics by the government, the people, and the Olympic Organizing Committee, improving the credibility of the public and the world for the low-carbon Beijing Winter Olympics. By making full use of the Blockchain consensus protocol, distributed ledgers, smart contracts and other technical characteristics, this platform is constructed on the public Blockchain service platform “State Grid Chain” of the State Grid. It has realized cross-chain interoperability with the Beijing ChainMaker platform, and will realize cross-chain interoperability with platforms such as the national Blockchain infrastructure “Xinghuo Chain Network”, the Tianping Chain for the Internet Court, and the e-commerce consortium

Blockchain for the Chinese central State-owned enterprises, forming a large-scale and industry-leading Blockchain group.

The green power traceability platform for Beijing Winter Olympics is constructed based on the Blockchain technology. The platform includes the base layer, platform layer, data layer, service layer and display layer. It obtains the business data by integrating with the external systems, conducts data calculation by the algorithm analysis and outputs results on the visual interface through the figures and real-time data. Based on the services provided by the State Grid Chain that the interface call for basic slaves and Blockchain-based evidence for the green power data of the Beijing Winter Olympics, the platform layer encapsulates the data exchange services. The integration, extraction and quality management for the green data are completed in the data exchange platform. The data layer includes data modelling, data cleaning, data assets and relationship analysis. The service layer includes on-chain service, traceability, data analysis, data development and data interface. The display layer displays the whole process of the green power of the generation, transmission, transaction settlement and consumption in the form of an urban sand table, realizing a dynamic and real-time perception of the public and the Olympic Organizing Committee for the whole process.

The platform, featuring the trusted on-chain source data, 100% green power proof, intelligent warning for the power margin, zero carbon

perception, cross-chain data sharing and visual display, provides a large-scale, reliable, convenient, and feasible Blockchain-based services for green power traceability to comprehensively realized the national goal of “dual carbon”. The key data and information of power generation, transmission, transaction and consumption on the whole green power chain are the block-chain based evidence, which can effectively promote the standardized development of power transaction market. They cannot be tampered with based on the Blockchain-based technologies such as timestamps, cryptographic hash algorithm, and multi-party joint maintenance. This improves the efficiency of power consumption along with the authenticity and transparency of transaction information, and proves that the Beijing Winter Olympics completely utilizes the renewable power energy.

2. Green Power Certificate of China Southern Power Grid

In recent years, China Southern Power Grid (CSG) has insisted on promoting the innovation on key technologies and business models, such as the application of Blockchain technology in the energy field. CSG has established a transaction platform pilot with Blockchain-based green power certificate (green power certificate) in Zhuhai, Guangdong. So, CSG is equipped with practical and promotion capabilities in terms of technology and platform. The green power certificate is an electronic

certificate with a unique code issued by the State to the power generation subject for the on-grid energy of renewable energy except for the water energy per megawatt-hour. In the smart energy pilot project “Internet+” with the National Energy Administration (NEA) who supports the energy consumption revolution, CSG has established a Blockchain-based transaction platform with green power certificate which generates distributed ledgers. This realizes the accounting information recording, transaction information storage, traceability of the information transmission and transparent monitoring process. Also, it guarantees a credible and effective operation of green power certificate transaction, avoiding human tampering and other illegal events.

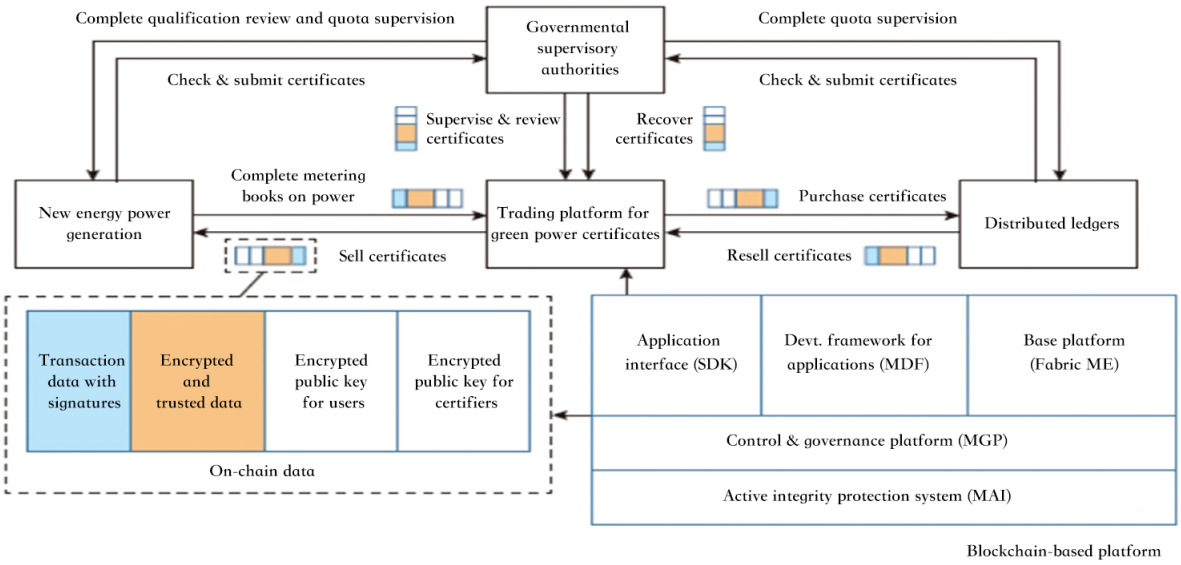

Figure 2-2 Circulation system of green power certificate based on Blockchain (CAI Yuanji, GU Yuxuan, LUO Gang, ZHANG Xuan, CHEN Qixin，2020[1])

3. Blockchain-based New Energy Cloud Platform for State Grid

The Blockchain-based new energy cloud platform takes the electrical

grid as the hub. By integrating the resources of the whole chain for the new energy industry, the platform uploads the business data related to the site construction consultation from users, evaluation for construction plans, equipment procurement, operation and maintenance, financial services, settlement, subsidies, and parallel power connection to the chain so as to realize ubiquitous connection of multiple links such as power supply end and user end. It also has established the new energy cloud service integrating “technology + service + finance” based on the management system of “horizontal coordination and vertical connection”. At present, pilot applications have been carried out in many regions such as State Grid Ningxia Electric Power Co., Ltd. On the one hand, it effectively optimizes business processes and improves the efficiency of multi-party collaboration. On the other hand, it optimizes the energy business environment and promotes higher-quality development of the energy industry. Meanwhile, it will help to increase the energy consumption proportion of new energy through digital management to truly optimize the energy consumption structure.

A Blockchain whose technical design is highly similar with the construction of ubiquitous power Interne of Things proposed by the State Grid. It can promote mutual trust between upstream and downstream industries, realize efficient data sharing, improve risk prevention capabilities, and effectively solve problems such as data integration,

network security, and multi-agent collaboration existed in the process of construction of ubiquitous power Internet of Things.

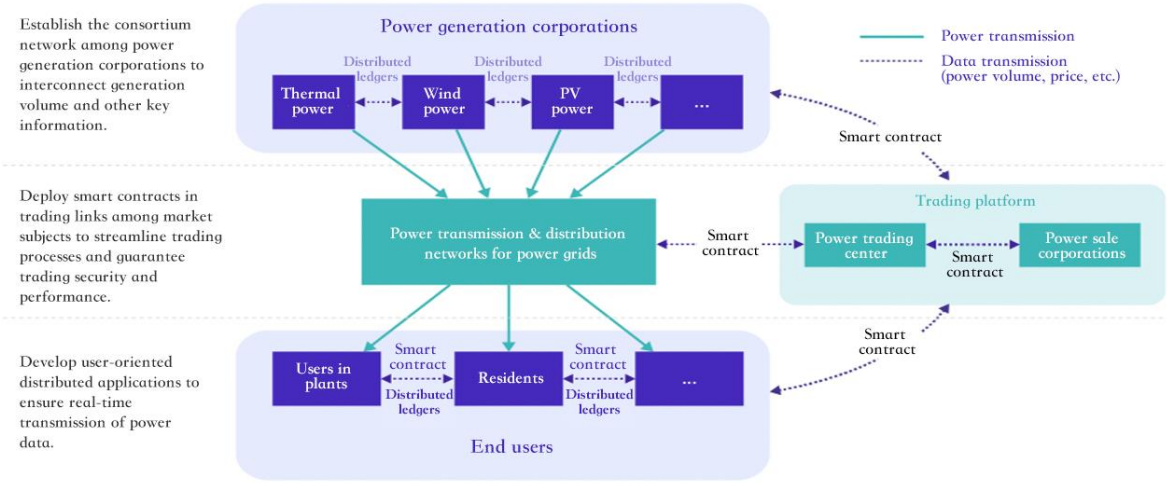

Figure 2-3 New energy cloud platform (TokenInsight，2019[2])

4. Enerchain - the European Energy Trading Platform

In the energy trading cycle, the first step of trading is usually provided by third parties online. Because the third parties always know the market conditions and transaction information, it not only brings about a large amount of agency fees, but lowers the efficiency. Enerchain is a P2P trading platform established by European energy trading corporations in the wholesale energy market based on the Blockchain technology. They transfer the entire P2P transaction process to Blockchains applied in the Enerchain where an anonymous trading organization utilizes cryptography to send decentralized orders to the other party who can review the orders. At present, there are more than 30 European energy trading corporations support the platform, including

ENEL (Italy) and RWE (Germany). They conducted a series of pilot transactions on electric power, which reduced costs. Besides, Vattenfall AB (Germany), Tennet Holding BV (Holland) and other electric grid corporations also utilize the platform.

5. Eloncity - the Decentralized Energy Management Platform

Eloncity, a decentralized green energy project based on the Blockchain, adopts the mode of power supply by decentralized renewable energy plus decentralized intelligent energy storage devices. Also, it deploys an intelligent network based on an efficient storage system to provide renewable power storage and a transmission and distribution platform for community micro-smart grid. By establishing community power infrastructure, Eloncity has gradually completed the networking and grid connection for the community micro-smart grid to establish a decentralized community electric power system. In this system, the combination of production and consumption of renewable energy as well as the integration of energy resources and users' demands make optimized resource utilization.

The Blockchain technology can synchronize the real-time price of grid services and the phasor real-time control system to balance the operation of microgrids and the access of distributed power generation systems, controlling the operation of grids more effectively. And, smart

contracts can instruct systems to initiate transactions. According to the pre-defined rules and conditions, the Blockchain-based platform will automatically manage the flow of the electric power system to balance supply and demand. For example, if the supply is higher than the demand, the smart contract will automatically store the remaining power. Also, the Blockchain technology can reduce the complexity of power distribution by automatically collecting and recording data from various meters and sensors.

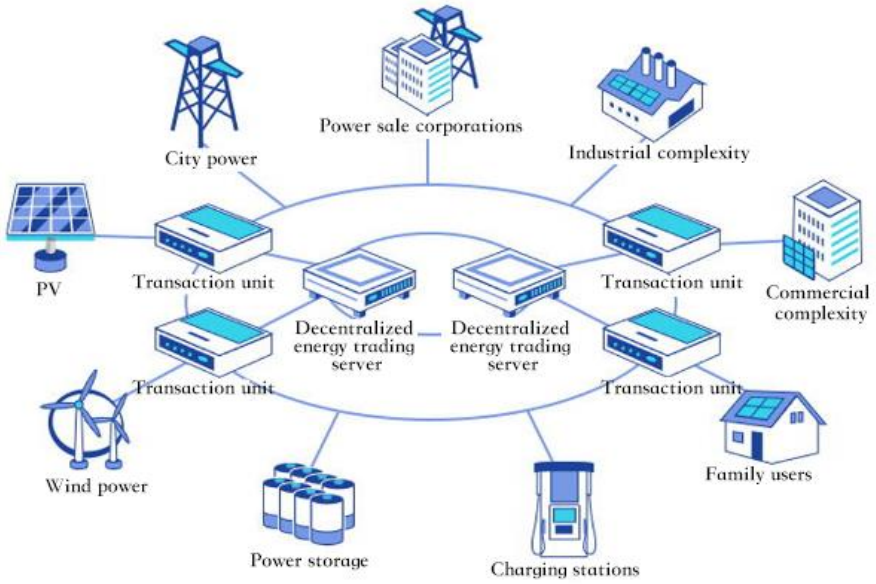

Figure 2-5 Decentralized energy

6. Brooklyn Microgrid - Trading Platform

In April 2016, LO3, an energy corporation in the USA, Siemens Digital Grid and Consensus Systems co-founded the Brooklyn Microgrid. It is the first Blockchain-based energy project worldwide that realizes P2P power transactions among residents in the community. Also, it allows

users to timely obtain data on power generation and consumption through smart meters, and to trade power energy with others via the Blockchain. This means that the users can complete power energy transactions without public power companies or the central grid. In addition, companies with energy production qualifications including producing solar panels can sell the unused energy to the community via the micro-smart grid.

The LO3 establishes its Exergy platform from the following perspectives: encrypted distributed ledger technology to securely store all data in a tamper-proof way; scalable smart contracts to automate all transaction processes; on-chain micro-smart grid control system to effectively manage its current and transaction flow. Suppliers providing PV systems for building rooftops can feed excess electric power back to grids in Brooklyn by combining the Blockchain and the micro-smart grid, and directly receive payments from purchasers. The Blockchain technology allows transparent and efficient transactions amid various involved systems and stakeholders, and includes particular demands for networks. In New York, fees for wires and substation maintenance and other utilities are quite high. These fees are generally paid by users for their electric power consumption. Generally speaking, the electricity fees are calculated by the net consumption in traditional grids where consumers have no choice. However, the fees are much cheaper in the

P2P energy sales compared with purchasing electricity from the central grid. And, consumers, such as ones installing solar panels on their roofs, can sell their own excess energy through the Blockchain. Brooklyn, as a pilot for the project, will enable producers and consumers for electric power in the community to conduct Blockchain-based energy transactions there, which can balance the production and consumption. Centrica, Braemar Energy Ventures, the British multinational utility, and Siemens in Germany have invested in the LO3.

7. WePower - Renewable Energy Trading Platform Based on the Blockchain

Wepower, a Blockchain-based green energy auction platform, allows manufacturers for renewable energy to issue their own tokens for energy to collect money where 0.9% is allocated to WPR token holders. The holders enjoy many priorities in the platform. On the one hand, they can have priority access to sales and auctions of new energy tokens. On the other hand, the more WPR tokens they have, the more energy they will be distributed. After the manufacturers have established the energy, the token holders can either consume the amounts of energy represented by the tokens or reinvest the tokens in the platform.

WePower not only solves funds issues for developers on the renewable energy, but directly provides opportunities for end consumers,

any investor and energy market creators to invest in profitable projects. This is realized by smart contracts on the Blockchain in a quick and transparent way. The developers can sell the up-front energy that will be produced in the future. In order to make it fast, global and transparent, it will be marked. Moreover, each power purchase agreement is a smart contract, which ensures the liquidity. And, the end consumers, investors and energy market creators can purchase the future energy in a discount so as to lower the cost. Or, the energy can be produced at a certain price in a certain time.

In addition, WePower has connected with the energy infrastructure and energy trading markets to record Blockchain-based data. If there is not enough demand in the platform, it may bring the energy transactions and sales to the market. Based on this model, it can accurately record types of energy produced, promote the liquidity of green energy in the market and bring transparency, which will reduce the pollution caused by the carbon dioxide. According to the estimate of Organization for Economic Co-operation and Development (OECD), the pollution at least costs 35 euros per ton or 1.13 trillion USD per year. In countries those have Wepower, the renewable energy is much cheaper than the traditional one. Wepower has provided a sustainable economic incentives path for the globe to develop the renewable energy.

8. Power Ledger - Blockchain-based P2P Electric Power Trading System in Perth

Power Ledger is founded in Perth, Australia by Ledger Assets, an Australian Blockchain-based software corporation. It is a P2P trading system for surplus solar energy based on the Blockchain and adopts POS (Proof of Stake) mechanism. In addition, the Blockchain developed by Ledger Assets is called Ecochain. The application of the Blockchain technology enables the system to determine the power owner when the power is being produced. Then, the owner completes transactions with the consumer through a series of agreements. To be specific, the owner can directly sell the excess power to other residents at the price that higher than that directly sell to the power corporation. Therefore, the producer for the power obtains more profits while the consumer gets lower price for power consumption.

Power Ledger profits from P2P power trading business model and its software. In the first half of 2017, it launched the official version of trading system covering 80 households in Perth urban areas. This is the first P2P power trading system put into use. Although Power Ledger has piloted the power trading for three times, it generally is in pilot stage as its stability has not been certified yet. It is known that the entire power network is an extremely complex value chain from generation, transmission, distribution to sale, consumption, storage, production and

immediate consumption. Besides, due to the very special nature of the power industry that is difficult to store in real time, all links in the entire value chain are interlinked. Also, the energy flow, capital flow and information flow are interconnected. The trading system established by Power Ledger is the first inseparable system. Its complexity and addition of trading costs are exponential. The system is an effective path for utilizing the decentralized energy and a great attempt for power trading.

III. Development and Vision

As a leap-forward upgrade of the traditional power system, the new power system based on new energy is green and low-carbon, safe and controllable, flexible and effective, intelligent and friendly as well as open and interactive. It strengthens its regulation performance and innovates development model for grids by focusing on innovations on science and technology, management and business models. The construction of the system will be promoted by Blockchain technology in intelligence, adapting to the market mechanism and serving “dual carbon” goal.

Improve the intelligent level of the new power system. In the new power system, the power source, power grid, load and power storage should be connected and coordinated more closely to achieve a high degree of intelligent operation control. The Blockchain technology should

extend its innovation application scenarios including the predication for operation risks and two-way interaction of new loads on the basis of deepening the existing applications, and improve the resilience of power grids via technical means. Besides, the Blockchain should be applied to microgrids, virtual power plants and new energy storage with the emergence of power producers and consumers. Also, it will realize flexibility by focusing on improving the adjustment capability of the power system and get the value of power big data by integrating the digital technologies. Therefore, it can realize the intelligent dispatch of the power system by enhancing the digitalization, informatization and networking of it.

Help the new power system adapting to market mechanism changes. With continuous development of high-proportion new energy consumption, carbon trade, coordination between the power and carbon market and other fields, the combination of the Blockchain and the new power system should match the transformation of the power market. To be specific, it should on the basis of continuing to build a trust mechanism for the power market deepen the model innovation for the spot power trading and long and medium term trading of the new energy, and propose a Blockchain solution for connecting the power and carbon market. Also, it should actively participate in establishing a unified national power market to perfect policies and market tools including the

power market, carbon market and power price mechanism, greatly improving innovations in energy, power, carbon and other markets. Driven by the Blockchain, a digital ecosystem for new energy will be established to improve the compatibility in the power market.

Facilitate the new power system serving the "dual carbon" goal. The large scale and high proportion of new energy units connected to the new power system will continuously increase the processing requirements for high-load intelligent bilateral trading scenarios including green power trading and the consumption of new energy. Although the Blockchain has already have mature solutions in those scenarios, its computing and processing performance and storage capacity will become a key node in restricting large-scale transactions in a short term. Therefore, its optimization in hybrid storage, multi-level cache, built-in contract, hierarchical consensus, and cross-chain technology will become an important path for the new power system to serve the "dual carbon" goal. Also, the Blockchain should give full play to its advantage of trust transmission to fully integrate into carbon emission service systems such as the intelligent monitoring and accurate measurement, strengthen data traceability and access as well as support carbon monitoring, carbon finance and other functions. The innovative Blockchain-based solution for the "dual carbon" goal has effectively enhanced environmental benefits of the new power system.

Bibliography

[1] CAI Yuanji, GU Yuxuan, LUO Gang, ZHANG Xuan, CHEN Qixin. Blockchain-based Transaction Platform with Green Power Certificate: Concept and Practice[J]. Automation of Electric Power Systems, 2020,44 (15):7(in Chinese)

[2] TokenInsight. Preliminary Research on Electric Grid Powered by Blockchain [EB/OL]. [2019-02-14]. https://blog.csdn.net/TokenInsight/article/details/87943491.