Summary of Foreign Research Progress and Application of Key Technology of Digital Currency

Guang Chen[1,a *], Xinda Li[1,b], Peidao Gao[2,c], Chaoyong Zhu[2,d] and Sirui Shi[2,e]

[1]State Grid Energy Research Institute Co. Ltd., Beijing 102209, China

[2]State Grid Yingda International Holdings co., LTD. Beijing, China

[a] chenguang@sgeri.sgcc.com.cn, [b] lixinda@sgeri.sgcc.com.cn, [c] peidao-gao@sgcc.com.cn

[d] chaoyong-zhu@sgcc.com.cn, [e] sirui-shi@sgcc.com.cn

*corresponding author

Keywords: Digital Currency; Trusted Cryptographic Technology; Blockchain; Smart Contract

Abstract: This paper provides a literature review on the foreign research progress and application of several key technologies that constitute digital currency. These key technologies mainly include trusted encryption technology, blockchain technology, smart contract technology, etc., which can help to provide auxiliary support for relevant personnel to carry out digital currency research.

Digital currency, simply put, is a value scale and circulation carrier based on digital technology, network transmission and non-physical form.Broad digital currency includes electronic currency, virtual currency, etc.In the narrow sense, digital currency specifically refers to the electronic cryptocurrencies created, issued, and circulated on the Internet based on cryptographic technology and blockchain technology.

Digital currency is the product of a combination of various technologies in the digital age.At present, the rapid development of digital currency is inseparable from the support of the research and application of key technologies. Key technologies for digital currency include: trusted encryption technology, blockchain technology, smart contract technology, etc.

1. Trusted Encryption Technology

At present, foreign digital currencies, such as Bitcoin, Letcoin, etc., are essentially electronic currencies applying cryptographic technology on the blockchain, so trusted encryption technology is the key basic realization technology. Since the idea of Diffie-Hellman public key cryptography was proposed in 1976 and marked the birth of modern cryptography, modern cryptography has been developed based on mathematics and alternately between encryption and decryption, attack and defense, spear and shield confrontation. From the perspective of mathematical algorithm, the cryptographic algorithm includes symmetric cryptographic algorithm, asymmetric cryptographic algorithm and hash algorithm. The development of modern cryptography and the evolution of cryptography algorithms have become an important realization basis of digital currency.

Generally speaking, the main applied cryptographic algorithm on the blockchain is the asymmetric encryption algorithm. Asymmetric cryptographic algorithm and symmetric algorithm correspond, refers to the transaction of the symmetric algorithm in two, to form a pair of key pairs. One key is disclosed for encryption, called a public key; the other key is a private and unique key, used for decryption, and is called a private key. In this way, the private key and public key are kept separately, and the security of both sides of the transaction is well guaranteed.

Based on the earliest Diffie-Hellman algorithm idea, the asymmetric cryptographic algorithm has, after decades of development, formed a variety of cryptographic algorithms, which can be roughly divided into three categories: large integer decomposition problem class, discrete logarithmic problem class, and elliptic curve class. In 1977, three scientists at the Massachusetts Institute of Technology proposed an asymmetric RSA algorithm based on the large integer factorization

problem. The algorithm uses the product of two large prime numbers as the encryption number. Because the emergence of prime numbers is irregular, the crack can only be found through continuous trial calculation, as a protection means of password security. RSA algorithm is the most widely studied asymmetric algorithm. It has been nearly 30 years since its proposal, and it has experienced various attacks, and is gradually accepted. It is widely considered to be one of the best asymmetric algorithm schemes, and it is widely used in various encryption verification scenarios. For example, the domestic Alipay is through the RSA algorithm to conduct signature verification. In addition to the commonly used RSA algorithm, in 1985 Tahilgeimer proposed the intractable ElGamal algorithm based on the discrete logarithms. The algorithm security depends on the difficult property of discrete logarithms in a finite domain, which is an internationally recognized and ideal asymmetric distributed encryption algorithm. In the process of encryption, it needs to carry out two modular exponential operations, and the length of transmitting ciphertext is twice the length of plaintext, which increases the amount of information in the process of transmitting ciphertext. Therefore, the encryption and decryption efficiency of this algorithm is slower compared with other algorithms, but its attack resistance is very good. Therefore, ElGamal algorithm is one of the more effective security algorithms for secure communication and digital signature on the network. In the same year that he proposed the ElGamal algorithm, Koblitz and Miller proposed the elliptic curve encryption algorithm, namely the ECC algorithm. The mathematical basis is the computational difficulty of forming the discrete logarithm of the ellipses on an Abel addition group by using the rational points on the elliptic curves. The ECC algorithm has certain application advantages over other algorithms, such as the RSA algorithm. First, the discrete log-solution of the ECC algorithm is more difficult to crack than the large integer decomposition. Secondly, the ECC has a smaller key length, and a lower requirement for storage space, when reaching the same crack difficulty of the RSA algorithm. Finally, the encryption and decryption speed is also faster due to the small key length. Thus, the ECC is widely considered to be the most powerful asymmetric algorithm given the key length, and would be very useful in connections with tight bandwidth requirements. At present, Bitcoin and other foreign digital currencies are widely used in ECC algorithms.

In addition to these cryptographic algorithms used for encryption or authentication, the hash algorithms used to ensure the integrity of the transaction content of the digital currency are also one of the priorities of the research. The Hash algorithm, also known as a safe hash function or a miscellaneous algorithm, also known as an information summary, is an algorithm that uses the HASH function to transform an arbitrary length of input into a fixed length of output. The hash algorithm is a generalized algorithm with many different implementation methods, but generally has two features. First, the hash algorithm is unidirectional, that is, the output can be obtained, and the output is irreversibly,; the output of the hash algorithm is deterministic, that is, when the value of the fixed length of the output is different, then the original input must be different. And the hash algorithm itself is a fast convergence algorithm, the computation speed is very fast, and the computational resource consumption is low. Therefore, the hash algorithm is widely used to guarantee the integrity of ciphertext in encryption technology. Currently commonly used hash algorithms include MD5 algorithm, SHA algorithm, etc.Digital currencies such as Bitcoin mostly use the SHA-256 algorithm to protect the integrity of the transaction content.

The use of trusted cryptography in blockchain is increasingly deep and extensive, and its importance is increasingly prominent. Its influence affects many fields of blockchain, and to a large extent affects the technological progress in these fields. It can be asserted that the trusted encryption technology of cryptography will be the battle of the future of the blockchain field.

2. Blockchain Technology

Blockchain is essentially a distributed storage system, and also a decentralized database.From the technical level, block chain is a string of associated using cryptography method of data block, each data block contains a currency network transaction information, used to verify the effectiveness of the information and generate the next block, the data block node without primary and secondary, through the consensus algorithm to determine the system stored data.From the

application level, blockchain is a decentralized and distributed shared ledger, with the characteristics of tamper-proof, whole-process trace, traceability, openness and transparency. These characteristics ensure the "honesty" and "transparency" of blockchain, laying the foundation for creating trust in blockchain.

On June 18,2019, Facebook released the Libra White Paper, which has significantly boosted the development of global blockchain technology. Since 2019, whether it is public chain or alliance chain, alliance chain, whether at home or abroad, whether which layer in the blockchain technology system framework, blockchain technology has developed, and there is no lack of highlights, blockchain technology has appeared all-round, high-quality development, and is in the ascendant.

At present, the development of global blockchain technology application has gone through three stages: blockchain stage 1.0 stage, namely the currency blockchain application stage. In this stage, the blockchain technology combines the core technologies such as distributed ledger, consensus mechanism, P2P technology and encryption algorithm, mainly to solve the decentralized management problem of digital currencies such as Bitcoin. Blockchain 2.0 stage, namely the programmable blockchain application stage.At this stage, examples of blockchain applications equipped with programmable technologies such as smart contracts have emerged. The combination of blockchain technology and smart contracts and other technologies can optimize the application of a wider range of scenarios and processes in the financial field, which can make more macro use of the entire Internet financial market. Not only the circulation of money, all financial transactions and digital assets can be transformed and used on the blockchain, using the blockchain technology to achieve the conversion of more digital assets, thus creating the value of digital assets. In the blockchain 3.0 stage, namely the blockchain governance stage, the application of blockchain technology goes beyond the financial field and becomes more extensive. This stage is the combination of blockchain technology with the real economy and the real industry. Echo with intelligent Internet of things era, because block chain technology can solve the problem of trust, improve the operation efficiency of the whole system, block chain technology applications will extend to all aspects of human life, provide decentralized solutions for various industries, in all kinds of social activities of information since the proof, namely no longer rely on a third person or institutions to obtain trust or establish trust, so as to achieve more extensive information sharing.

3. Smart Contract

Smart contracts are a computer protocol designed to disseminate, verify, or enforce contracts in an information manner, allowing trusted transactions that are traceable and traceable without third parties, secure and irreversible.

A Smart contract is actually a computer program that is written in a language that a computer or a target machine can understand. In addition, it includes agreements between the parties in the form of business logic. Another basic idea is that smart contracts are executed automatically when certain conditions are met. Smart contracts are enforceable, meaning that all contract terms are enforced as defined and expected.

Due to the backward technology and the lack of application scenarios, smart contracts did not receive attention from all parties. Later, smart contracts are further divided into smart contract code and smart legal contracts. As an example of how to automate using smart contracts, Grigg proposed a graph contract triad of "legal provisions, parameters and codes" in Ricardo contracts, which also affected the implementation of blockchain smart contracts later, but the application of smart contract technology has failed to make substantial progress.

It wasn't until nearly 20 years later that, with the emergence of Bitcoin and the development of blockchain technology, that the potential and advantages of smart contracts were truly recognized. Based on the Bitcoin Turing incomplete bytecode language OP-RETURN Bitcoin script is the earliest applied in the block chain smart contract, because the OP-RETURN computing power is very limited, does not support circular statements, can only realize the basic arithmetic, logic operation and verification encryption function, so the early smart contract usually cannot have complex logic. Moreover, blockchain also initially appeared as the underlying technology of

Bitcoin, and various blockchain forks led to great changes.So early smart contracts still didn't fit very well into Bitcoin's blockchain network.It wasn't until Ethereum appeared in 2013 that smart contracts actually landed for the first time. Ethereum, as the world's first public blockchain with a built-in Turing complete programming language and officially introduced the concept of smart contract block chain, is currently the most popular smart contract development platform. Ethereum smart contracts are written in a high-level language such as Solidity. Their core is Ethereum virtual machine (EVM) that can be encoded by any complex algorithm. All smart contracts deployed on Ethereum are compiled into EVM bytecode and executed in the EVM locally isolated by miners. As ethereum, the founder of ethereum Vitalik Buterin in ethereum white paper described for smart contracts, " smart contracts should not be considered to fulfill or comply with obligations, they are more like robots living in the EVM, when received external conditions (message or transaction) will automatically execute a specific code and modify the relevant address balance or other information." Etheric fang is equivalent to an underlying operating system, users can according to their own will on the ethereic fang platform efficiently and quickly developed a variety of smart contracts, including cryptocurrency and established on the smart contract of decentralized applications, the application once built, can implement automatic execution and without other intermediary agencies to participate in, accuracy and efficiency will be improved. The emergence of Ethereum has really changed the application pattern of blockchain and smart contracts, making it no longer limited to digital currency, and starting to have the opportunity to build a more macro financial system and apply it to other social areas.

For blockchain virtual machines, as an important part of the smart contract execution environment, with the development of technology, in addition to EVM virtual machines, WASM virtual machines, deterministic JVM, and even docker virtual machines (HyperLedger Fabric use) have all joined the big family of blockchain virtual machines, and thus can support more contract development languages beyond Solidity.In 2019, CKB-VM virtual machines based on RISC-V instruction sets emerged, Its fans argue that the RISC-V instruction set has the following advantages: open source, Any institution and individual can develop processors compatible with RISC-V instruction sets, Can be integrated into the RISC-V's hardware and software ecosystem; ripe, The core instruction set was finally confirmed, Future achievements all require backward compatibility; Instruction set streamlining, Easy and reliable implementation of virtual machines; Support for multiple development languages, Any language that can be compiled into a RISC-V instruction set can be used to develop smart contracts; The runtime overhead is clearly defined, No repeated adjustment of the GAS billing mechanism is required.

Smart contracts for other blockchain platforms are also evolving.For example, Hyperledger Fabric is a modular and open-source enterprise-level licensed distributed ledger technology platform for enterprise environments that provide capabilities such as supporting insertable implementations and creating channels for different components. Its highly modular and configurable architecture provides innovative, flexibility, and optimisability for industry use cases such as banking, finance, insurance, healthcare, human resources, supply chain, and even digital music delivery. EOS is a commercial blockchain underlying public chain operating system designed for distributed applications, aiming to solve the existing problems of low performance, poor security, high development difficulty, and excessive reliance on fees, and realize the performance expansion of distributed applications. EOS decentralized applications mainly include e-commerce, fintech and markets. The superledger does not use custom bytecode to realize the writing language of smart contracts, but runs the program code of a specific interface to realize smart contracts, supporting high-level languages including Golang, java, Nodejs and other languages, which greatly reduces the threshold of developing smart contracts.

Although the smart contract is still in the early research, there may be various challenges and problems, but anyway, smart contract for the underlying block chain data provides better than traditional contract programmable mechanism and flexible security algorithm, reduce other transaction costs related to the contract, and to build block chain 2.0 programmable financial system and block chain 3.0 programmable social system laid the foundation, is the most important

technology on the block chain.

Acknowledgments

This work was supported by the science and technology project of State Grid Corporation of China, called “Research on the applied technology of e-CNY in finance and its ecological operation mode (Project Code: 52580021N004)”.

References

[1], Li Weiming. Research on trusted encryption service platform technology [J]. Network Security Technology and Application, 2019 (11): 32-34.

[2] Shen Xin, Pei Qingqi, Liu Xuefeng. A Review of Blockchain Technology [J]. Journal of Network and Information Security, 2016,2 (11): 11-20.

[3] Xie Hui, Wang Jian. Blockchain Technology and its Application Research [J]. Information Network Security, 2016 (09): 192-195.

[4] Ouyang Liwei, Wang Shuai, Yuan Yong, Ni Xiaochun, Wang Feiyue. Smart Contracts: Architecture and Progress [J]. Journal of Automation, 2019,45(03): 445-457. DOI:10.16383/j.aas.c180586.

[5] He Haiwu, Yan'an, Chen Zehua. Summary of smart contract technology and applications based on blockchain [J]. Computer Research and Development, 2018,55 (11): 2452-2466.