Application of Homomorphic Encryption in Blockchain Data Security*

Jingjing Chen†
Beijing Institute of Graphic Communication
Beijing China
921019511@qq.com

Fucheng You
Beijing Institute of Graphic Communication
Beijing China
youfucheng@bigc.edu.cn

ABSTRACT

With the continuous development of the Internet era, people's demand for network security is increasingly high, information is an essential component of the network, which implies numerous privacy, secrets, but also contains a large number of value, thus generating a multiparty trust issues of data security. Blockchain technology itself is still in the early stages of rapid development, the existing blockchain system in the design and implementation of the use of distributed systems, cryptography, game theory, network protocols and many other disciplines, for learning the principles and practical applications have brought considerable challenges. The blockchain, with its decentralized quality, quickly captures the attention of the public and solves many security problems derived from data security, thus attracting wide attention from people. In recent years, along with the increasing maturity of homomorphic encryption technology and push new, it is more and more people's favour and attention.

Homomorphic encryption is an encryption technology that provides the ability to perform various operations on data in an encrypted state without compromising its confidentiality. Its concern is the security of data processing. That is, others can process the encrypted data, but the process does not reveal any of the original content. Also, the user who has the Key decrypts the processed data and gets the result of the processing precisely.

The main encryption technique used in blockchain applications is the RSA encryption algorithm,[1] which is used to ensure that the user's private key is not compromised, but no project has been noticed about the homomorphic encryption method for smart contracts.[2] The purpose of this paper is to analyze the principle of homomorphic encryption and discuss its practical application in data security in combination with blockchain technology.

EITCE 2020, November 6–8, 2020, Xiamen, China

ACM ISBN 978-1-4503-8781-1/20/11…$15.00
https://doi.org/10.1145/3443467.3443754

CCS CONCEPTS

•Security and privacy ˜Cryptography

KEYWORDS

Homomorphic encryption, Blockchain technology, Data security

1 Introduction

With recent developments and updates, public-key ciphers, while becoming more mature, still have some problems to overcome. One wants to process data that has been encrypted and then implement decryption of the data so encrypted so that the result obtained is the same as a result obtained when the same process is performed on data that has not been encrypted, this is the problem of homomorphic encryption. By definition, it can be seen that the most important point of homomorphic encryption is that one can perform some specific operations, such as comparison and retrieval, without decrypting the encrypted data; at the same time, the result obtained after the operation is identical to the result obtained after decrypting the data and then manipulating it, which means that you can safely store your encrypted information in a third-party organization without affecting any of your own calls, because information data exists in the Cloud, but no one can encrypt it, and at the same time you can do anything with it without revealing the private key.

At this stage, in the global context, blockchain technology has shown rapid development momentum, the integrated application of blockchain technology plays an important role in new technological innovation and industrial change, we should take blockchain as an important breakthrough in independent innovation of core technologies, clarify the main direction, increase investment, focus on a number of key core technologies, and accelerate the development of blockchain technology and industrial innovation. Blockchain is not only a technology but also a way of thinking about social governance. Its core technologies including cryptography, distributed storage, smart contracts, consensus algorithms have received widespread attention, and these technologies have been applied to data processing, security

protection and other multiple fields. Blockchain has the qualities of decentralization, unalterable, full traceability, traceability, collective maintenance, openness and transparency, which are not found in many other technologies, providing more technical options for data security protection. Blockchain service to the real economy is increasingly becoming a social consensus, since the introduction of domestic, the formation of the blockchain and bitcoin isolated from the basic consensus, but its development in the privacy protection and data transmission of security vulnerabilities are also increasing, which is not conducive to better and faster development.

Therefore, the purpose of this paper is to study and analyze the principle of homomorphic encryption, combine the characteristics of blockchain technology, and apply homomorphic encryption technology to blockchain data security, so as to ensure the security of data.

2 Homomorphic encryption

In 2009, Craig Gentry, who proposed the first construction of a fully homomorphic encryption, gave the best and most intuitive definition: A way to delegate processing of your data, without giving away to it.[3]

We can define the homomorphic function, and if the function E can satisfy E(a)*E(b)=E(a*b), E(a)+E(b)=E(a+b), then it is fully homomorphic, if one of the conditions is satisfied, then it is semi-homomorphic; E function is a cryptographic function, and the decryption process is, if D(x)=a, and F(a)=x, then the entire decryption function D and encryption The function E is full homomorphic encryption; among them, there are other variables, such as the private Key, public Key, etc. The advantage of this function is that it implements the decryption of the result obtained when performing the operation on the secret F(x), so that we can get an accurate, detailed and comprehensive result of the original text from it.

Homomorphic encryption is defined as follows.

$$\forall m_1, m_2 \in \mathcal{M}, \quad E(m_1 \odot_{\mathcal{M}} m_2) \longleftarrow E(m_1) \odot_{\mathcal{C}} E(m_2) \tag{1}$$

Where M denotes the set of plaintexts, C denotes the set of secret texts and denotes that the left formula can be computed from the right formula.

In particular, there are,

$$\begin{aligned} \forall m_1, m_2 \in \mathcal{M}, \quad & E(m_1 +_{\mathcal{M}} m_2) \longleftarrow E(m_1) +_{\mathcal{C}} E(m_2), \\ & E(m_1 \times_{\mathcal{M}} m_2) \longleftarrow E(m_1) \times_{\mathcal{C}} E(m_2). \end{aligned} \tag{2}$$

They are additive isomorphism and multiplicative isomorphism, respectively.

Homomorphic encryption is a cryptographic technique based on the computational complexity theory of mathematical puzzles. [4] Processing homomorphically encrypted data to get an output, and decrypting this output gives the same result as processing the original unencrypted data in the same way to get an outcome. To send an encrypted thing to someone else, or to store something on a computer or other server, the Data is encrypted before the message is sent or stored. Only the user who has the key will be able to decrypt the encrypted message obtained and get the correct transmission. A user without the key cannot get any information about the original data from the encryption results. It is worth noting that in this process, the user cannot do any operation on the encryption result, but can only store or transmit it. Any manipulation of the encryption result will lead to wrong decryption result or even failure of decryption.

The most noteworthy aspect of the homomorphic encryption scheme is that it is concerned with the security of data processing. Homomorphic encryption provides a way to process the encrypted data. That is, others can process the encrypted data, but the processing does not reveal any of the original content. At the same time, the user who has the Key decrypts the processed data and gets exactly what the processing results in.

We can illustrate this process with a simple example, Alice user buys a piece of gold, she wants to have the gold processed by a worker, but the worker may steal the gold in the process, for the worker to process the gold and not steal the gold, she can do this.[5]

1.Alice locks the gold in an airtight box and attaches a pair of gloves to the chest.

2. the worker with this glove to work on the gold, the box is closed, the worker can't get to the gold nuggets, nor any gold fell during processing.

3. when the processing is complete, Alice takes the box back, opens the lock and gets the gold nugget after the processing is complete.

The correspondence inside this box is as follows.

1. Boxes: cryptographic algorithms.

2. The lock on the box: user keys.

3. Place the nugget inside the box and lock it with a lock: encrypt the data using homomorphic encryption methods.

4.Processing: using the characteristics of homomorphic encryption, direct data processing of encrypted results and inaccessibility of data.

5. Unlocking: decrypting the products and obtaining the processed results.

The most basic security of a homomorphic encryption scheme is semantic security, which means that the secret text does not reveal any information in plaintext. The following formula can express this.

The most basic security of a homomorphic encryption scheme is semantic security, which simply means that the secret text does not reveal any information in plaintext. This can be expressed by the following formula.

$$\forall m_0, m_1, \mathbf{Encrypt}(PK, m_0) \approx \mathbf{Encrypt}(PK, m_1) \tag{3}$$

A useful working homomorphic encryption model means that sensitive Data is less exposed, not only to external users trying to access the system but also to internal users. The identity of the data processor can be protected using a homomorphic encryption model. There is no way to see the details of the individual being processed, only the result of the processing. Businesses can feel more secure with the Data they collect, whether in the hands of team members within the organization or processors outside the organization who may need to perform some data tasks as

intermediaries due to holding more powerful tools or expertise. Cloud computing, in particular, can benefit from homomorphic encryption schemes, as they can run computations without having to access the original unencrypted data.

We can get a specific definition of homomorphic encryption in the context of cloud computing scenarios.

Alice's entire process of processing the data with Homomorphic Encryption, via Cloud, goes roughly like this.

1. Alice encrypts the data and sends the encrypted data to the Cloud.

2. The processing of data submitted to the Cloud by Alice, here represented by the function f.

3. Cloud processes the data under function f and sends the processed results to Alice.

4. Alice decrypted the data and obtained the results.

From this process, we can learn that a homomorphic encryption scheme should have the following functions.

1. the KeyGen function, key generation function. This function should be run by Alice to generate the key. The key was used to encrypt the data. Of course, there should be some public constants PP (Public Parameter).

2. the Encrypt function. This function, which should also be run by Alice, encrypts the user data. Data with Key to get the secret CT (Ciphertext).

3. Evaluate function: Evaluate function. This function is run by the Cloud, and operates on the secret text under the data processing method f given by the user so that the result is equivalent to the user encrypting f(Data) with the key.

4. decrypt function: decryption function. This function is run by Alice and is used to get the result of f(Data) processed by Cloud.

At the same time, the content can be encrypted in the operation process by using Cloud computing-related technologies according to different requirements, such as entrusting some less important data to a Cloud computing company for processing. However, once the important core and sensitive Data is involved, it can be encrypted by homomorphic encryption method. In the architecture of homomorphic encryption, although there are a variety of algorithm settings, the most fundamental relies on the mathematical matrix, number theory and other basic knowledge.

3 Blockchain

With the continuous development of the times, the amount of data in life is increasing, users with security requirements are also increasingly high, in different industries, in various fields, inter-industry communication will involve more data aggregation, these massive Data not only has great value but also implied a large number of personal privacy. With the development of blockchain technology, it appears in the sight of more people, its decentralized nature to solve the trust issues in many lives and industries, reducing many risks and accidents caused by data leakage, providing a certain guarantee for multiparty cooperation, providing platform support for data security, and promoting more efficient, orderly and safe multiparty cooperation.

In 2008, Satoshi Nakamoto described the concept of blockchain in "Bitcoin: A Peer-to-Peer Electronic Cash System"[6]. Blockchain has the following characteristics: decentralization, openness, independence, security, and anonymity, and because of these characteristics, blockchain has since received widespread attention from various sectors. In the book Block Data 3.0: The Orderly Internet and the Sovereign Blockchain, the author writes: Blockchain is based on super ledger technology, smart contract technology and cross-chain technology to establish a set of consensus and co-governance mechanism, which is programmed to solidify the data streams formed by the multi-dimensional overlay of time, space and moment to form a recordable, traceable, definitive, predictable and transactive technology Binding Power. [7] Blockchain is not only used in electronic currencies, financial institutions, and banks. Still, it has also been extensively and deeply researched in various fields such as information security, healthcare management, 5G applications, and AI.

Two main types of cryptographic algorithms, asymmetric cryptographic algorithms and hash algorithms, are used in blockchain to ensure the security and authentication needs of untrustworthy networks.[8]

The basic process of asymmetric encryption algorithm to realize the exchange of confidential information is: Party A generates a pair of keys and discloses one of them to other parties as a public key; Party B, who gets the public key, encrypts the confidential information with the key and then sends it to Party A; Party A decrypts the encrypted information with the other private key that it keeps. The strength of the non-stacking encryption algorithm is complex, and security depends on the algorithm and key. Still, due to the complexity of its algorithm, the encryption and decryption speed is not fast.

The RSA encryption algorithm, which is mainly used in blockchain, requires two keys: a public key and a private key. The public key and the private key are a pair, and if the Data is encrypted with the Public Key, it can only be decrypted with the corresponding private key.

Hash algorithms are used to generate precursor block addresses, record information summaries, interactor addresses, and construct Merkle tree data structures, and are the most widely used algorithms in blockchain, both for producing blocks and confirming the integrity of transactions. Hash algorithms are a class of functional mathematical algorithms that require three basic properties.

1. its input can be a string of any size

2. It produces a fixed size output

3. It is capable of performing efficient calculations, i.e., it can calculate the output value in a reasonable time.

Hash algorithms to achieve cryptographic security words, but also need to have collision resistance, stealth, puzzle friendly and other properties.

Blockchain itself has the advantages of decentralization, security, independence, etc.,[9] not only to achieve massive data storage but also real-time confidentiality of data, has excellent application prospects, will bring great changes to people's lives.

4 Practical applications of homomorphic encryption in blockchain security

At this stage, Baidu Netbook and 360 Netbook are cloud storage platforms, which will cause user data to be directly exposed in the central processor once it is attacked, and the user's private data will have no security at all. If the homomorphic encryption project is applied in cloud storage when users need to call their sensitive data, the system will only operate according to instructions, and the whole process system can't view the contents, so as to ensure security. With the development of science and technology, blockchain, with its unique technical characteristics, is gradually being widely studied in all walks of life, especially in the field of financial technology has become a popular technology, and in the number of users, also shows a rapid increase in the trend, the need to transmit more and more data, which has a positive effect on the protection and sharing of data.

The primary encryption technique used in blockchain applications is the RSA encryption algorithm, which is used to ensure that the user's private key is not corrupted. Still, no project has yet noted homomorphic encryption methods regarding smart contracts. Homomorphic encryption is a form of encryption that allows one to perform a specific way of algebraic operation on a secret text to get a result that is still encrypted, decrypting it yields the same effect as performing the same procedure on the plaintext. In other words, the technique allows one to perform operations such as retrieval, comparison, etc. on the encrypted data to obtain the correct result without having to decrypt the data during the entire process.

Homomorphic encryption was first used in cloud computing and big data, and it also complements blockchain technology well. Using homomorphic encryption technology, the smart contract running on the blockchain can process secret messages without knowing the real data, which significantly improves privacy security.

Due to the excellent practicality of homomorphic encryption technology, it has received widespread attention and use from all walks of life. The Huawei blockchain provides homomorphic encryption library, which encrypts and protects the user's transaction data with its public Key. The transactions are all in secret text operation, which is encrypted and saved in the final ledger. Fun chain Hyperchain implements encryption of transaction amounts and account balances in blocks through the encryption idea of homomorphic encryption (using the Paillier homomorphic encryption algorithm).[10] Its whitepaper claims that the verification time for a homomorphically encrypted transaction is about 10 microseconds, which can satisfy Hyperchain's need for tens of thousands of transactions per second.BCOS also uses the Paillier homomorphic encryption algorithm and has open-sourced the Additive Homomorphic Explanation of Use[11], as well as the Java version implementation of the Paillier homomorphic encryption algorithm. [12]

Along with the continuous improvement of the relevant technology, blockchain functions continue to increase, the number of users continues to grow, so the amount of data to be transmitted is also growing. These data, inevitably, there are some enterprise related secrets, now, relying solely on the blockchain's data transmission technology is difficult to fully ensure the security of data transmission, so it is necessary to use some external tools to carry out data encryption and processing,[13] and these tools, homomorphic encryption technology is the most considerable.

For blockchain network users who want to ensure the security performance of data submitted to the blockchain network, especially the security of critical and sensitive data,[14] malicious information leakage and tampering should be avoided. Homomorphic cryptography enables the user's confidential data to be secreted in a blockchain smart contract, rather than the traditional plaintext operation. The advantage of this is that the transaction data can be encrypted using a corresponding encryption algorithm before the user submits the transaction data to the blockchain network, the data exists in the form of a secret text, and even if an attacker accesses it, it will not reveal any private information of the user. In contrast, the results of the undercover text operation are consistent with the results of the plaintext operation.[15]

In an already operational blockchain network, homomorphic cryptography is combined with the principles of the blockchain mechanism in a more rational way, and the Data is stored in a purposefully distributed manner. Besides, individual nodes in the blockchain can also be targeted to the units that require independent computation and can be distributed reasonably. For those processes that require higher computing power, a method of homomorphic encryption technology is used to encrypt and decrypt the data. The specific steps of this method are as follows

generate a pair of homomorphic encryption keys, save the private key in a trusted third-party organization, please send it to the corresponding blockchain user, and use the corresponding homomorphic public key to implement encryption, thus better providing high privacy protection for the data security of the blockchain.

5 Conclusion

In summary, in recent years, the rapid development of blockchain technology, but the data transmission and processing process still has too much uncertainty, the security of the data transmission is not fundamentally guaranteed, people are also constantly exploring the technology, hoping to bring some new ideas, new changes, the use of homomorphic encryption technology can better solve the security problems of data transmission and processing. This paper analyzes the principle of homomorphic encryption technology, combines the essence of the blockchain, and proposes a scheme to apply homomorphic encryption method to the blockchain, to better provide privacy protections for the data security of the blockchain.

ACKNOWLEDGMENTS

This research is supported by Joint Funding Project of Beijing Municipal Commission of Education and Beijing Natural Science

Fund Committee (KZ201710015010), Initial funding for the Doctoral Program of BIGC (27170120003/022), BIGC Project (Ec202007) and BIGC Project (Eb202004).

REFERENCES

[1] Ron Rivest, Leonard Adleman, and Michael L. Dertouzos. On data banks and privacy homomorphisms. Foundations of Secure Computation, 1978.
[2] Tong Qinwei, Li Jie, Wang Jie, Hu Xinsen, Hu Kai. A full homomorphic encryption method based on smart contract[J]. Cyberspace Security, 2020, 11(09):32-38.
[3] Craig Gentry. Fully homomorphic encryption using ideal lattices. STOC 2009. Also, see "A fully homomorphic encryption scheme", PhD thesis, Stanford University, 2009. [LMSV10] Jake Loftus, Alexander May, Nigel P. Smart, and Frederik Vercauteren. On CCA-Secure Fully Homomorphic Encryption. Cryptology ePrint Archive 2010/560.
[4] Lin. Application of homomorphic encryption in data security of IoT blockchain[J]. Network Security Technology and Applications,2020(03):36-37.
[5] https://www.zhihu.com/question/27645858
[6] Nakamoto S. Bitcoin: A peer-to-peer electronic cash system[J]. Consulted, 2008.
[7] Block Data3.0: The Internet of Order and the Sovereign Blockchain [J]. Leadership Decision Information,2017(21):20-23.
[8] Yao Zhonghong, Ge Jingguo. An overview of the principles and applications of blockchain[J]. Research Information Technology and Application,2017,8(02):3-17.
[9] Leng Di. Blockchain-based dynamic data homomorphic encryption protection method[J]. Computer Products and Circulation,2020(04):147.
[10] Pascal Paillier. Public-Key Cryptosystems Based on Composite Degree Residuosity Classes. Eurocrypt 1999.
[11] https://github.com/bcosorg/bcos/blob/master/doc/manual/manual.md
[12] https://github.com/FISCO-BCOS/paillier-lib
[13] Sharples M, Domingue J. The Blockchain and Kudos: A Distributed System for Educational Record, Reputation and Reward[C]//European Conference on Technology Enhanced Learning. Springer International Publishing, 2016: 490-496.
[14] Biswas K, Muthukkumarasamy V. Securing Smart Cities Using Blockchain Technology[C]//High Performance Computing and Communications; IEEE 14th International Conference on Smart City; IEEE 2nd International Conference on Data Science and Systems (HPCC/ SmartCity/DSS), 2016 IEEE 18th International Conference on. IEEE, 2016: 1392-1393
[15] Craig Gentry and Shai Halevi. Implementing gentry's fully-homomorphic encryption scheme. Eurocrypt 2011.