Application Analysis of Cryptography in Blockchain

Haonan Jiang*[a]
[a]School of Information Science and Technology, HaiNan Normal University, Haikou, CN 570100
*Corresponding author: 201924120408@hainnu.edu.cn

ABSTRACT

The purpose of blockchain technology is to solve the trust problem between people or institutions and make the communication data and network communication of the Internet. In the past, cryptography lost money. Passwords are used to protect data, and the cost is relatively high. But with blockchain, cryptography becomes valuable. The formation of blockchain has made new contributions to cryptography and done something we could not do in the past. With blockchain, cryptography is "valuable". In fact, there are many cryptographic primitives used in blockchain, such as hash, digital signature, and etc. Moreover, digital signature not only uses standard digital signature, but also uses ring signature, connectable ring signature, one-time signature, borromer ring signature, multi signature, homomorphic encryption, homomorphic commitment, accumulator, zero knowledge proof, etc. As well as the recently popular password signature toss.As mentioned above, the popularity of blockchain technology will completely break the centralized pattern, indicating the advent of a new era in the future - Web3.0.This paper focuses on the application of encryption technology in blockchain, and expounds in detail the applications of such as hash function and ring signature in blockchain. This study analyzes the application of cryptography in blockchain and discusses to the development of encryption technology in the future.

Keywords: blockchain, cryptography, bitcoin, cryptography encryption technology, function

1. INTRODUCTION

The purpose of blockchain technology is to solve the trust problem between people or institutions and make the communication data and network communication of the Internet. In real, especially in some fields, the authenticity of data is very important. In daily life, data fraud is a problem that people are very worried about. For example, when a country elects a president, we should ensure that the data is not tampered with.

At present, there is no foolproof way. However, if the voting process is published on the blockchain, it can ensure that the data is true and reliable because the blockchain scheme directly isolates the tamperability of the data from the technical level. Everyone's voting records are open and traceable, saved into the blockchain, they cannot be modified. Through blockchain, This is the result we want, decentralization. We can make this truth in everyone's hands at the same time. Everyone can monitor and supervise the voting process. Everyone has saved a backup, so everyone directly becomes the maintainer and manager of data. Fate of these data will be decided by everyone. This is the core logic of blockchain decentralization.

As mentioned above, the popularity of blockchain technology will completely break the centralized pattern, indicating the advent of a new era in the future - Web3.0.

In Figure 1, each block consists of its hash, the hash of the previousblock, a timestamp and some other block fields.

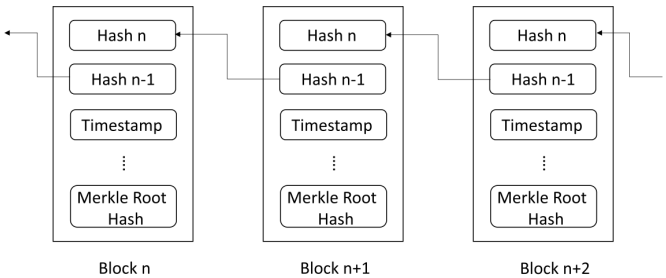

Figure 1. Basic blockchain structure[1].

Third International Symposium on Computer Engineering and Intelligent Communications (ISCEIC 2022), edited by Xianye Ben, Proc. of SPIE Vol. 12462, 1246216 · © The Authors. Published under a Creative Commons Attribution CC-BY 3.0 License · doi: 10.1117/12.2661094

In a brief history of security, blockchain is compared to a family tree. It's equivalent to holding a tweeter on the square when ispeak, and what i say has been heard by many people. When someone wants to repent, as long as there are enough people to prove the truth, no one can repent The core cryptographic primitives of bitcoin are signature algorithm (ECDSA) and hash algorithm (hash). In fact, there are many cryptographic primitives used in blockchain, such as hash, digital signature, etc.

Moreover, digital signature not only uses standard digital signature, but also uses ring signature, connectable ring signature, one-time signature, borromer ring signature, multi signature, homomorphic encryption, homomorphic commitment, accumulator, zero knowledge proof,etc. As well as the recently popular password signature toss.

2. RELATED CRYPTOGRAPHY

2.1 Hash function

Hash functions are among the cryptographic primitives, which typically don't encrypt or decrypt messages and can be used to ensure the data integrity [2].

A method to extract tiny digital "fingerprints" (also called as abstractions) from any type of data is the hash function, also known as hash function and hash algorithm. The hash function will produce a result with a set length and fixed format if data of any length and content are input, this result is comparable to the fingerprint of input data. The fingerprint will change as long as the input varies. For various contents, the hash function yields distinct fingerprints. Hash functions play an important role in blockchain security. Generally speaking, it is very safe. For example, if an attacker wants to crack a 256 bit private key, he must exhaust 2256 key possibilities. If a typical super computer that executes 1018 keys per second is used to crack such a system, it will take 3x1051 years to find the key [4]. The hash function has three main uses in the blockchain:

$$h: M \rightarrow \{0,1\}^n, with\ h(m) = \hat{m}$$

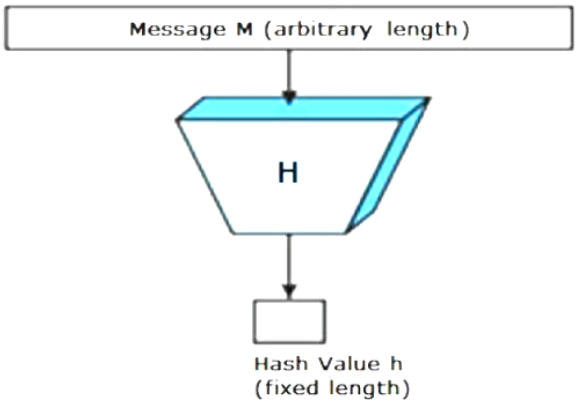

Figure 2. Image of a typical Hash Function [3].

a) Fast verification: The hash function generates summaries of various data in the blockchain. When comparing whether two data are equal, only need to compare theirsummaries. For instance, it is quick and easy to compare the hash values of two transactions to determine if they are equal.

b) Prevent tampering: To make sure that the data is not altered throughout the transfer process, just simply need to send the data's summary at the same time. In order to determine whether the transmitted summary and the created summary are equivalent, the recipient of the data will recreate the summary of the data. If they are equal, it implies that during the transmission procedure, the data was not altered.

c) Workload proof for Proof-of-Work (POW) consensus algorithm: This is mostly utilized in POW's consensus algorithm. In further detail, it is to provide a specific quantity of data before allowing to explore for additional data. Merging produces a hash value that is less than a specific threshold. Right now, POW consensus applies to both Bitcoin and Ethereum.

2.2 Evolution of hash function in blockchain

a) Sha256: A group of cryptographic hash functions known as Sha256, or secure hash algorithm, were created by the National Security Agency (NSA) and made public by the NationalInstitute of Standards and Technology (NIST). The sha-0, SHA-1,SHA-2,and Sha-3 series have all evolved there. Bitcoin adopts sha256 algorithm, which belongs to SHA-2 series. When Nakamoto invented bitcoin, it was one of the most advanced and secure algorithms.

Table 1. Fraction of SHA256d outputs with respective target value[1].

Target Value T	**Fraction of SHA256d outputs≤ T**
0x7 t1t2t3t4 ....t62t63 (63times)	$\frac{1}{2}$
0x0 t1t2t3t4 ....t62t63 (63times)	$\frac{1}{16}$
0x00...00t1t2t3t4 ....t47t48 (16times, 48times)	$\frac{1}{2^{64}}$

b) Scrypt: With the emergence of video card mining and mining pools, communities are worried about the concentration of computing power, which violates the principle of decentralization. Therefore, Wright coin proposed the script algorithm. In addition to this algorithm, other parts of Wright coin are completely fork bitcoin. Compared with sha256, this algorithm requires more memory and longer computing time, and can resist mining machines. However, this algorithm has not undergone strict security review and comprehensive demonstration.

c) Concatenation algorithm: The so-called concatenation algorithm is the same as the concatenation algorithm in our junior high school physics. It uses many kinds of hash algorithms for multiple rounds of operation, and the results of the previous round are used for the input of the next round of hash. X11, x13 and x15 on the market are such algorithms.

d) Parallel algorithm: The so-called parallel algorithm is also similar to the parallel algorithm in physics, that is, first solve the input with different hash functions, and then confuse the solution results to form the final hash algorithm results.

e) ETHASH: Ethash is a hash algorithm worth mentioning. It is the hash algorithm of POW used in Ethereum. The algorithm can resist mining machines, and basically can achieve ethash mining, which has nothing to do with CPU performance, but is proportional to memory size and memory bandwidth. The flow of the algorithm is as follows:

- For each block, a seed is first calculated, which is only related to the information of the current block.
- A 32m random data set (CACHE) is generated according to the seed.
- 1GB data set (DAG) is generated according to the cache. The DAG can be understood as a complete search space. The mining process is to randomly select elements from the DAG (similar to finding a suitable nonce in bitcoin mining) and then hash.

2.3 One time digital signature

In the blockchain version of bitcoin, digital signatures are used to protect data integrity throughout the system and to veri fy the identities of both parties to a transaction. A digital signature employs asymmetric encryption and digital digest tec hnology to guarantee the accuracy of the sender's identity and the integrity of the material being transmitted. Digital sum marization is to use hash function to change information of any length into information of fixed length. Hash function is

a one-way generation system, which generates input value to the generation through the generated hash value irreversibl y. In addition, hash function is a compression mapping, and the output is fixed length information.

Digital signature can mainly realize as below:

- The receiver can authenticate the identity of the sender through the sender's public key.
- Through private key signature, others cannot forge the signature of information.
- The sender also cannot deny the signature of the information through the private key signature.
- The integrity of data is ensured by digital summarization technology.
- The hash function also ensures that the data cannot be tampered with.

2.4 Ring Signature

Rivest et al[5]first introduced the ring signature algorithm, a type of digital signature scheme, in 2001. Ring signatures are a type of group signature that leaks information covertly, or a simpler group signature [6].

The ring signature lists only ring members, not management. The signer randomly selects the public keys of multiple ringmembers, combining their public and private keys, random integers, and other technologies [7], in order to complete a ring signature. The signature verifier can only confirm that the signature is part of the signature set; they are unable to determine who signed the signature. For submitting complaints, casting ballots in elections, using electronic money, and other purposes, ring signature works quite well. The blockchain offers cross-parent transactions, data privacy disclosure, and an open and transparent record ledger. To achieve complete anonymity of users and defend their right to privacy, the technique uses the ring signature transaction signing scheme [7].

Ring signature implementation includes the following rules:

- When the key is Generatekey pairs (public key PKI, private key ski) are generate for each member in the ring.
- To create a signature for message M, the signer utilizes both his private key and the public keys of any n ring members (including himself).
- Using the ring signature and message M, the verifier determines if the signature was actually signed by a member of the ring. It will be accepted if it is legitimate; else, it will be dismissed.

2.5 Multi signature and aggregate signature

Many signatures on a digital item are what is commonly referred to as "multiple signatures." Several signatures show that multiple persons may manage and control digital assets. This fund requires several private key signatures, which is referred to as multi-signature. Usually, a multisignature address or account will be used to hold this money or digital assets. It is comparable to a real-life document that must be signed by several departments in order to become enforceable.

Multi signature is an improvement to the digital signature that enables the use of blockchain-related technologies in various spheres of life. An actual operation technique allows for the association of a multisignature address with n private keys. When transfer and other operations are required, as long as m private keys are signed, the funds can be transferred, where m should be less than or equal to N, that is, m/n is less than 1, and can be 2/3, 3/5, etc., which should be determined when establishing this multi signature address.

If a couple needs to reserve a sum of money for their children to go to college. Before that, no one can move. Changing the signature mode to 2/2 not only limits the couple, but also increases the difficulty of hacker attacks. The design of multi signature makes it possible to decentralize various businesses.

2.6 Homomorphic encryption

By enabling a specific kind of calculation to be made on the ciphertext and producing an encrypted result that is also the ciphertext, homomorphic encryption facilitates the encryption process[8]. The operation that was carried out on the plaintext produced the result[8]. For instance, no one can determine the precise value of a single number by adding two encrypted numbers and waiting until the other person decrypts the result. This procedure is therefore quite secure. The application of privacy protection technology in blockchain is still in its early stage. For the process of realizing

homomorphic encryption of FISCO bcos chain:all data on the chain can be encrypted by calling the Paillier library, and the ciphertext data on the chain can realize homomorphic encryption of ciphertext by calling the Paillier precompiled contract. After the ciphertext is returned to the business layer, it can be decrypted by calling the Paillier library to get the execution result.

2.7 Homomorphic commitment

The function of accumulator is to construct ring signatures on the one hand, and directly use it in blockchain on the other hand.Monroe coins are useful.As for the accumulator, it is also translated into aggregator in China, which is a good concept.

It can compress many objects into one space, and the compressed space is almost as large as the original space of each object.

2.8 Zero knowledge proof

Early in the 1980s, S. Goldwasser, S. Micali, and C. Rackoff proposed the zero knowledge proof. It means that the verifier can influence the verifier to believe that a certain conclusion is accurate without giving the verifier any valuable information. Zero knowledge proof is simply a contract between two or more parties, or a set of actions that two or more parties must execute in order to complete a task. The certifier convinces the verifier that he understands or is the owner of a certain message by proving it to him, but the verifier cannot learn anything about the proven message throughout the certification process. Zero knowledge proof has been demonstrated to be extremely beneficial in cryptography by a huge number of facts.If zero knowledge proof can be used for verification, many problems can be effectively solved.

There are two types of zero-knowledge proof. First one is interactive zero-knowledge proof. It is the firstinvention and requires multiple messages between prover and verifier. The second one is non-interactivezero-knowledge proof. It requires less interaction between the prover and verifier[9].

Figure 3 shows the working principle of the whole zero knowledge proof.

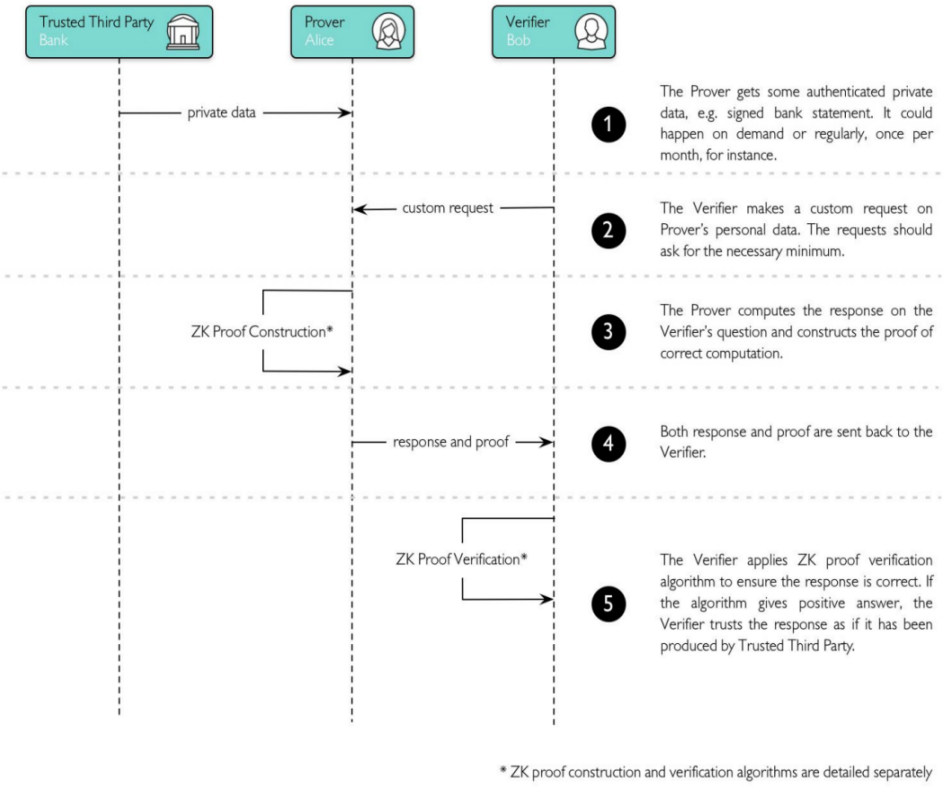

Figure 3. Zero-knowledge proof on blockchain explained in summary[10].

3. CONCLUSION

Blockchain is built with cryptographic algorithm. The chain of digital signatures ensures that the transaction is correct, and then the hash function ensures the integrity and tamperability, ensuring that the data can be verified and its credibility. The unidirectionality of hash function can be used to control the generation speed of money, which is one aspect. On the other hand, the formation of blockchain has made new contributions to cryptography and done something we could not do in the past.

With blockchain, cryptography is "valuable". In the past, cryptography lost money. Passwords are used to protect data, and the cost is relatively high. But with blockchain, cryptography becomes valuable. Because we generate hash codes that meet certain conditions, and after some cryptographic functions, the results become money. At the same time, with blockchain and applications such as bitcoin, these cryptographers suddenly seem to be able to eat, so cryptography is "valuable".

In the past, cryptography could not achieve non repudiation. After the blockchain came out, it became interesting. It will be found that the blockchain itself provides a platform for non repudiation, because blockchain is now a trusted third party, and everyone obeys it. What is said on the chain can naturally play a role in repudiation, which is also the double flower problem in bitcoin.

In fact, without the flexible and powerful security provided by public key encryption technology, e-commerce transactions relying on the Internet will be difficult to achieve. In the future, public key encryption technology will become an integral part of all kinds of information systems.

Cryptography can guarantee the security of all virtual networks. Security is the basis of all transactions. Blockchain networks cannot be separated from encryption algorithms. Moreover, with the rapid development of science and technology, our encryption algorithm will continue to improve.

REFERENCES

[1] Raikwar, Mayank & Gligoroski, Danilo & Kralevska, Katina. (2019). SoK of Used Cryptography in Blockchain. IEEE Access. 7. 1-1. 10.1109/ACCESS.2019.2946983.

[2] V. G. Martínez, L. Hernández-Álvarez, and L. H. Encinas, “Analysis of the cryptographic tools for blockchain and bitcoin,” Mathematics, vol. 8, no. 1, 2020, doi:10.3390/math8010131.

[3] Dilhara, Shashie. (2021). A Review on Application of Hash Functions and Digital signatures in the Blockchain Industry.

[4] K. T. Son, N. T. Thang, L. P. Do, and T. M. Dong, “Application of Blockchain Technology to Guarantee the Integrity and Transparency of Documents,” Int. J. Comput. Sci. Netw. Secur., vol. 18, no. 12, pp. 7–15, 2018.

[5] Rivest R L, Shamir A, Tauman Y. How to Leak a Secret[A]. Proc ASICRYPT’01[C]. Springer-Verlag, 2001.552-565.

[6] Chaum D, Heyst V E. Group Signatures[A]. Proc CROCRYP’91[C]. Springer-Verlag, 1991.257-265.

[7] Li, Xiaofang & Mei, Yurong & Gong, Jing & Xiang, Feng & Zhixin, Sun. (2020). A Blockchain Privacy Protection Scheme Based on Ring Signature. IEEE Access. PP. 1-1. 10.1109/ACCESS.2020.2987831.

[8] Ogburn, Monique & Turner, Claude & Dahal, Pushkar. (2013). Homomorphic Encryption. Procedia Computer Science. 20. 502-509. 10.1016/j.procs.2013.09.310.

[9] Çapraz, Seval & Ozsoy, Adnan. (2021). Personal Data Protection in Blockchain with Zero-Knowledge Proof. 10.1007/978-981-33-6470-7_7.

[10] Introduction to Zero Knowledge Proof. Ashish. 2018. The protocol of netx generation. Blockchain.https//medium.com/coinmonks/introduction-to-zero-knowledge-proof-the-protocol-of-next-generation-blockchain-305b2fc7f8e5.