Application of Cryptographic Techniques in Blockchain Technology

Kalana .K.A.V.
IT20037260
Faculty of Computing
Department of Computer Systems Engineering
Sri Lanka Institute of Information Technology
New Kandy Rd, Malabe
10115, Sri Lanka
it20037260@my.sliit.lk

Rathnayake .R.M.K.G.
IT20128272
Faculty of Computing
Department of Computer Systems Engineering
Sri Lanka Institute of Information Technology
New Kandy Rd, Malabe
10115, Sri Lanka
it20128272@my.sliit.lk

Ilangarathna .D.N.
IT20180034
Faculty of Computing
Department of Computer Systems Engineering
Sri Lanka Institute of Information Technology
New Kandy Rd, Malabe
10115, Sri Lanka
it20180034@my.sliit.lk

Dilshan .D.R.G.K.B.
IT20219970
Faculty of Computing
Department of Computer Systems Engineering
Sri Lanka Institute of Information Technology
New Kandy Rd, Malabe
10115, Sri Lanka
it20219970@my.sliit.lk

***Abstract*— Cryptography is the science of writing secret code, and it has been used since ancient times. This art is a part of a system called cryptology which has two counterpart's cryptography and cryptanalysis. Since Cryptography is all about creating secret messages, known as ciphering, Cryptanalysis is about breaking those secret messages, known as deciphering. Cryptography consists of many schemas, and generally, they can be divided into three majors; symmetric, asymmetric, and hash functions. Blockchain is a technique of preserving information that makes it difficult to update, hack, or manipulate the system. A distributed ledger is a system that copies and distributes transactions throughout the blockchain's network of computers. Blockchain technology is a framework that maintains public transactional information, also known as blocks, in many databases connected by peer-to-peer nodes in a network. This type of storage is sometimes known as a 'digital ledger.' In blockchain technology, cryptographic schemas are used as essential components in the hash in a block structure, asymmetric schema in cryptocurrency, and digital signature in blockchain trading. Therefore, this study aims to understand what aspects of cryptography are used in blockchain technology, how these cryptographic principles are used in this technology, the primary use cases of cryptography in blockchain technology, and the limitations and problems faced by cryptographic functions in the blockchain.**

Keywords—Blockchain, Hash Functions, Symmetric cryptography, Asymmetric cryptography, Crypto wallet, Digital signature

I. INTRODUCTION

Since the introduction of Bitcoin in 2009 [1], public interest in cryptocurrencies has increased dramatically. As a result, banks and businesses increasingly accept cryptocurrency as a proper monitoring system. Most people incorrectly think blockchains and bitcoins are connected or integrated; nonetheless, bitcoins rely on blockchain security to execute transactions.

Blockchain technology was established to address issues resulting from growing online transactions with third-party apps, enabling transparent and efficient transactions while eliminating cumbersome processes. A blockchain block or node serves as a storage container for a record in the digital ledger, which is another term for blockchain [2].

Cryptography is used in blockchain to safeguard transactions between two nodes in a blockchain network. Cryptography and hashing are the two essential elements of blockchain technology. Cryptography encrypts messages in a peer-to-peer network, while hashing secures block information and connects blocks in a blockchain. Cryptography is primarily concerned with guaranteeing the security of participants, transactions, and measures against double-spending. It aids in the security of various transactions on the blockchain network. It assures that only the person supposed to receive, read, and process the transaction data may do so [3].

Blockchain is built using a variety of cryptographic principles. The advancement of cryptographic technology encourages limitations for the further growth of blockchain. Cryptography is primarily utilized in blockchain to safeguard user privacy and transaction information and assure data integrity [3]. Cryptography's leading technologies are symmetric encryption and asymmetric encryption. Asymmetric cryptography relies on digital signatures for verification. Every transaction recorded to the block is digitally signed by the sender, guaranteeing that the data is not altered. Cryptography is critical in keeping the public network safe, making it suitable for ensuring the integrity and security of blockchain [3].

II. ANALYSIS

Goal of Cryptography

Generally speaking, cryptography's main aims are information security and efficient utilization and manipulation. This goal can ensure availability, access control, non-repudiation, data integrity, confidentiality, and authentication.

III. CRYPTOGRAPHIC SCHEME

A. Symmetric Key Cryptography

It is an encryption technique where messages are encrypted and decrypted using the same public key by both the sender and the receiver. Symmetric vital systems are quick and easy, but the issue is that the sender and recipient must somehow securely exchange keys. The key advantages of this algorithm are its quick processing speed and minimal computational requirements. The two modes of this algorithm are block ciphers and stream ciphers. All data would be broken up into chunks or blocks using a block cipher, and the data would be provided for encryption based on the block size and key. Data is divided into bits in

a stream cipher, such as 0101010101, and then randomly generated when the encryption rule is applied. Symmetric is faster than the asymmetric algorithm. Data Encryption Technology is the most widely used symmetric key encryption system (DES). Other symmetric key encryption algorithms are Blowfish, RC5, 3DES, and AES [4] [5].

B. Asymmetric Key Cryptography

A key pair is employed in this system to encrypt and decrypt data. When encrypting data, a public key is used, and a private key is used when decrypting data. Private keys and public keys are distinct. Even if everyone is aware of the public key, only the intended recipient can decode it because only he is aware of the private key. Let us utilize the following scenario as an example: If the first key is intended for encryption publication, then system communication on unlocking user keys is secret from the public. The second requirement is that our system would act as an ID-based verification for document lock by the dealer of that private key if we published one unlock key decryption after that. This type of fundamental public approach is crucial because it can be applied to the over-shifting of encrypted keys or to provide data security when both users cannot agree on a secret key concerning the private key. Asymmetric vital algorithms include RSA, DSA, Diffie-Hellman, and El Gamal [4] [5].

C. Hash Functions

This algorithm makes no use of any keys. It is impossible to reconstruct the contents of plain text since a fixed-length hash value is computed based on plain text. Hash functions are widely used in operating systems to secure passwords [6].

IV. BLOCKCHAIN TECHNOLOGY

Blockchain is the underlying technology of world-famous cryptocurrency and non-fungible token (NFT), Which is a distributed database with decentralized, traceable, non-tampering, secure, and dependable features. Moreover, blockchain is integrated with technologies like peer-to-peer protocol, digital encryption, consensus, smart contract, and more. Three blockchains, public, private, and alliance, have expanded their ways to many industries and sectors [7].

Word' Chain' means the peer-to-peer (P2P) connection in-between blocks mathematically with the help of hash values and Merkle root [2]. Block consists of two parts, blockhead and block body. Blockhead consists of the previous block hash value, the version of the cryptocurrency, the timestamp, the difficulty of the target, cryptographic nonce (an arbitrary one-time number), and Merkle root value (the hash value of a hashed value), including blockhead elements and blocking the body altogether [8]. The Block body contains all transaction details, such as from whom and the amount. The Block header is used as documentation to identify the block as an entity separate from other blocks.

The advantages of using a system like a blockchain can be categorized as follows [9].

1) **Security**

Digital ledgers use the digital signature to identify user authentication, and hash functions help secure the transaction's data integrity and confidentiality.

2) **Decentralized infrastructure**

the mutual trust and cryptographic security of blocks result in smooth, safe, faster transactions rather than conventional ways, where the need for traditional regularities authorities such as banks and governments

3) **Automation**

The programmable nature of blockchains can generate events and actions triggered when certain conditions are met.

A. Cryptography in Blockchain

All transaction information in the blockchain is stored within itself; therefore, information security is a high requirement among all other non-functional requirements. Moreover, the Decentralized nature of blockchain does not have any conventional centralized node. Instead, it manages the whole chain using a mutually shared mode among nodes. Therefore information supervision among shared nodes is required to ensure the credibility and integrity of the transaction, where cryptography plays a significant role in blockchain technology.

B. Role of Cryptography in Blockchain

Cryptography plays a major role in blockchain technology to protect user privacy, transaction information, and the blockchain's consistency. Cryptographic techniques used in the blockchain are,

1. Asymmetric Key Algorithms in cryptocurrency
2. Hash in block structure

1) Asymmetric Key Algorithms in cryptocurrency

Asymmetric Key Cryptography, also known as Public Key Cryptography, is a critical component of the Blockchain network. It is utilized in multiple places to secure the integrity of messages produced by the system. The essential components of every currency, wallet generation, and transaction signing, rely primarily on asymmetric encryption. The Blockchain protocol uses the Elliptic Curve Digital Signature Algorithm (ECDSA) to generate a fresh set of private and associated public keys. The public key is then used with a hash function to generate the public address used by Bitcoin users to transmit and receive payments. The private key is kept private and is used to sign a digital transaction to ensure the transaction's legitimacy [10].

2) Hash in block structure

Hash function properties such as susceptibility, unidirectionality, collision resistance, and high sensitivity help blockchain technology secure data integrity in a dangerous environment. Furthermore, hash functions may validate the blockchain's block and transaction integrity. Each block's header contains the hash value of the preceding block's information, and any user may compare the computed hash value to the stored hash value. The integrity of the previous block's information is then determined. The hash function may also be used to produce public-private vital pairings. The most prevalent hash algorithms are SHA256 and RIPEMD160 [7].

The Merkle Tree is a hash binary tree used to verify the integrity of vast amounts of data swiftly. Typically, the Merkle tree comprises,

- the transaction database for the block,
- the root hash of the block header, and
- all branches along the underlying block data to the root hash.

Merkle tree operations are typically performed in groups. The data in the block adds the newly created hash value to the Merkle tree. It is eventually formed into a tree structure when the last root hash is left and stored as the Merkle root of the block header [7] [11].

a) Properties of Cryptographic Hash

- The hash value will fluctuate significantly with any small change in the input data.(Diffusion/Avalanche Effect)
- The hash function cannot be used to determine the input value.(Preimage Resistance)
- They are quick and effective because they mostly use bitwise operations.

b) Benefits of Hash function in Blockchain [3]

- Easy to verify the transaction
- Prevent any modifications to the data blocks
- Using hash reduce the bandwidth of the transaction
- Impossible to Reverse Engineer

c) Use of Cryptographic Hash Functions

Cryptography hashing the blockchain is open to the general public, it is crucial to safeguard data and protect user data from unauthorized modification [12].

C. Main usages of Cryptography in Blockchain

1) Blockchain wallet

A Bitcoin wallet is a file in the users' file system. It holds public and corresponding private key pairs and transactions from and to that wallet. Public keys are given to payers to identify recipients, and private keys are used to sign transaction messages. User preferences are also kept in wallet files that can and should be encrypted [13].

A Bitcoin address is a character identifier of 25-34 characters. The address usually starts with one and never contains the number 0 or the uppercase letter "O" or the lowercase "l" or "I" for better legibility. The address is removed from the public part of the Elliptic Curve Digital Signature Algorithms (ECDSA) key pair. After several hashing cycles with the RIPEMD-160 and SHA- 256 algorithms, a checksum for the address is added and encoded with a modified Base 58 coding from the mentioned format. The probability that an incorrect address is accepted as valid is over 4.29 billion. There is good protection against typing errors, although typing addresses for sending Bitcoins is probably a rare opportunity. The Bitcoin addresses and ECDSA key pairs are not part of the structure of the Bitcoin network and can be created safely offline after the hash and encoding rules described in the original design. The Bitcoin network will only know the address after its first use and a reported transaction. There is no way to use these parts again; they are lost forever [13].

The original Bitcoin client is written in C++ and is open-source. Several other programs are available to connect to the Bitcoin network. One can also use eWallet services to avoid downloading the ever-growing blockchain with all transactions, eliminate some checks on their Bitcoins, and eventually accept higher transaction fees [13].

2) Digital signatures in transactions

Digital signatures are electronic signatures that assure that a particular sender sent the message. While performing digital transactions, authenticity and integrity should be assured. Otherwise, the data can be altered, or someone can act as if he was the sender and expect a reply [14].

Signature algorithms like email programs create a one-way hash of the electronic data to be signed. The signing algorithm then encrypts the hash value using the private key (signature key). This encrypted hash, along with other information like the hashing algorithm, is the digital signature. Finally, this digital signature is appended with the data and sent to the verifier. A Verifier reads a digital signature and the public key (verification key) and generates some value. It then applies the same hash function on the received data and generates a hash value. If they are both equal, the digital signature is valid; otherwise, it is invalid [14].

D. Limitations of Cryptography in Blockchain

By analyzing the transaction records in the global catalog which is available publicly, store the transaction history at each node on the blockchain network, potential attackers may threaten the user's transaction privacy and identity privacy. An attacker can obtain valuable information by analyzing these transaction records [7].

The identity privacy threat means that the attacker can get the identity information of the trader. The mechanism of the crypto coin is easy to crack and cannot achieve the desired effect. Therefore, it is necessary to add a cryptographic mechanism to ensure the security of the mixed currency [7].

Data security and privacy protection in the blockchain are severely challenged, and advanced cryptography techniques can effectively solve such problems, but weak links remain. The private key is generated by the random number generator in the computer system, called pseudo-random, has certain regularity, and has the threat of being cracked. In future research, it is necessary to develop a coin-rich mechanism under the protection of cryptography mechanisms and to minimize the performance requirements [7].

V. Conclusion

Blockchain technology is based on cryptography concepts to shorten transaction times. However, this technology has made inroads into a variety of industrial industries. This paper examines three key topics: hash functions in a block structure, the asymmetric schema in cryptocurrencies, and digital signatures in transactions. The evolution of cryptographic technology encourages constraints for blockchain's future expansion. Cryptography is generally used in blockchain to protect user privacy and transaction information and ensure data integrity. The two most critical cryptographic technologies are symmetric encryption and asymmetric encryption. For verification, asymmetric cryptography uses digital signatures. Every transaction added to the block is digitally signed by the sender, ensuring that the data has not tampered with it. Because cryptography is essential in keeping the public network secure, it is appropriate for maintaining the integrity and security of blockchain.

Acknowledgment

Authors token appreciation toward lecture in charge of cryptography Mr. Kavinga Yapa for providing us this fantastic opportunity to initiate this project and would like to humble gratitude toward everyone for providing resources and ideas on completing this mini review paper in timely and meaningful way.

VI. References

[1] W. Duggan, "The History of Bitcoin, the First Cryptocurrency," 31 August 2022. [Online]. Available: https://money.usnews.com/investing/articles/the-history-of-bitcoin.

[2] Ege Tekiner, Abbas Acar, A. Selcuk Uluagac, Engin Kirda, Ali Aydin Selcuk, "SoK: Cryptojacking Malware," 2021.

[3] "Cryptography in Blockchain," geeksforgeeks, 20 September 2022. [Online]. Available: https://www.geeksforgeeks.org/cryptography-in-blockchain/. [Accessed 29 September 2022].

[4] "Cryptography and its Types," geeksforgeeks, 10 May 2022. [Online]. Available: https://www.geeksforgeeks.org/cryptography-and-its-types/. [Accessed 2 October 2022].

[5] Muhammad Aamir Panhwar, Sijjad Ali khuhro, Ghazala Panhwar, Kamran Ali memon, "SACA: A Study of Symmetric and Asymmetric Cryptographic Algorithms," *IJCSNS International Journal of Computer Science and Network Security*, vol. 19, no. 1, pp. 48 - 55, 2019.

[6] "Hash Functions and list/types of Hash functions," geeksforgeeks, 31 July 2022. [Online]. Available: https://www.geeksforgeeks.org/hash-functions-and-list-types-of-hash-functions/. [Accessed 30 September 2022].

[7] e. a. Sheping Zhai, "Research on the Application of Cryptography on," in *IOP Publishing*, 2018.

[8] J. FRANKENFIELD, "Block Header (Cryptocurrency)," Investopedia, 22 September 2021. [Online]. Available: https://www.investopedia.com/terms/b/block-header-cryptocurrency.asp#:~. [Accessed 29 September 2022].

[9] "What is Blockchain Technology? How Does Blockchain Work? [Updated]," simplilearn, 9 September 2022. [Online]. Available: https://www.simplilearn.com/tutorials/blockchain-tutorial/blockchain-technology#. [Accessed 2 October 2022].

[10] T. K. Sharma, "How Does Blockchain Use Public Key Cryptography?," Blockchain Council, 23 July 2018. [Online]. Available: https://www.blockchain-council.org/blockchain/how-does-blockchain-use-public-key-cryptography/. [Accessed 27 September 2022].

[11] M. D. Pierro, "What Is the Blockchain?," *Computing in Science & Engineering*, vol. 19, no. 5, pp. 92-95, 2017.

[12] Maoning Wang, Meijiao Duan, Jianming Zhu, "Research on the Security Criteria of Hash Functions in the Blockchain," Proceedings of the 2nd ACM Workshop on Blockchains, 2018.

[13] ER-RAJY LATIFA, EL KIRAM MY AHEMED, EL GHAZOUANI MOHAMED, ACHBAROU OMAR, "Blockchain: Bitcoin Wallet Cryptography Security, Challenges and Countermeasures," Journal of Internet Banking and Commerce.

[14] "Digital Signatures and Certificates," geeksforgeeks, 31 August 2021. [Online]. Available: https://www.geeksforgeeks.org/digital-signatures-certificates/. [Accessed 1 October 2022].