International Journal of Cryptology Research 11(2): 17 - 30 (2021)

CRYPTOGRAPHY IN BLOCKCHAIN TECHNOLOGY

Isma Norshahila Mohammad Shah*[1] and **Hazlin Abdul Rani**[2]

[1, 2]*Cryptography Development Department, CyberSecurity Malaysia*

E-mail: isma@cybersecurity.my
**Corresponding author*

ABSTRACT

Blockchain is a ground-breaking technology that, because of its transparency, decentralisation, and security features, has a significant impact on society today. Academics, business, and researchers have recently become more interested in researching several aspects of blockchain and smart contracts, such as the technology's possible applications and flaws. One of blockchain's backbone is cryptography technology. In this paper we will discuss the application of cryptography in various aspect of blockchain design.

Keywords: blockchain, cryptography, security

1 INTRODUCTION

Innovative and competitive technologies are frequently introduced with the goal of discovering new and better approaches to more effectively implementing software systems and products. Blockchain is one example of this technology, which has the potential to be implemented in a variety of use cases, including internet interaction systems, public services, the internet of things (IoT), and financial systems. Academics and industry have been paying close attention to blockchain technology and the use of cryptocurrencies (Wang et al. (2018)). Satoshi Nakamoto first introduced the concept of blockchain in 2008 (Nakamoto (2008)), which was later implemented in a digital currency system called Bitcoin in 2009. Following the introduction of Bitcoin, new blockchain ideas began to emerge and be implemented, resulting in the rapid development of this technology.

A blockchain is a distributed ledger that records all transactions and data exchanged since its inception. In other words, blockchain keeps a constantly growing list of records known as blocks. Each block contains a number of transactions and is linked to the previous block created all the way back to the first, genesis block. Its distributed and immutable nature makes it ideal for use in a variety of digital asset transactions, such as transferring property ownership, recording transactions, and tracking digital assets to ensure transparency, security, trust, and value. Blockchain is based on a protocol that combines three well-known and existing technologies, which are cryptography, peer-to-peer (P2P) computer networks, and game theory (Voshmgir (2019)). In this paper, we will focus on the cryptography protocol used in the blockchain technology.

2 CRYPTOGRAPHY

Cryptography is a means for designing strategies and protocols that prevent unauthorised parties from accessing and interpreting data contained in private communications during the communication process. The process of turning plaintext into ciphertext is a common representation of cryptography. Ciphertext is text that can only be decoded by the intended recipient. Encryption is the process of turning plaintext into ciphertext; decryption is the process of turning ciphertext back into plaintext. A cipher is a set of predetermined processes that can be used as a procedure to achieve encryption or decryption, also known as a cryptographic algorithm. A key is a small quantity of data required to generate the output of a cryptographic method.

It is crucial to first comprehend the different types of cryptography in order to understand the encryption used in blockchain. As indicated in Figure 1, there are three types of cryptographic algorithms: symmetric-key cryptography, asymmetric-key cryptography, and hash functions.

(a) Symmetric-key cryptography: This encryption technique uses a single key for encryption and decryption. This technique is also known as Secret-Key Cryptography.

(b) Asymmetric-key cryptography: This form of encryption utilises a pair of keys, the encryption key and the decryption key. A public key is used to refer to an encryption key, whereas a private key is used to refer to a decryption key. The same mathematical process is used to produce these key pairings. Additionally, this sort of cryptography is known as Public-Key cryptography.

(c) Hash Functions: No keys are used in the hash function. It uses a cipher to generate a hash value of a defined length from the plaintext. It is practically impossible to extract the plaintext's contents from the ciphertext.

A blockchain uses asymmetric-key cryptography and hash functions for encryption. Asymmetric-key cryptography is used to safeguard blockchain transactions between users. Simultaneously, hash functions are utilised to ensure the integrity of data in the blockchain.

3 BLOCKCHAIN ARCHITECTURE

Bitcoin (Nakamoto (2008)), Ethereum (Buterin (2014)) and Hyperledger (Foundation (2018)) are the most prevalent uses of blockchain technology. Although the implementations are distinct, the underlying design shares many similarities. Blockchain platform can be divided into five layers as shown in Figure 2.

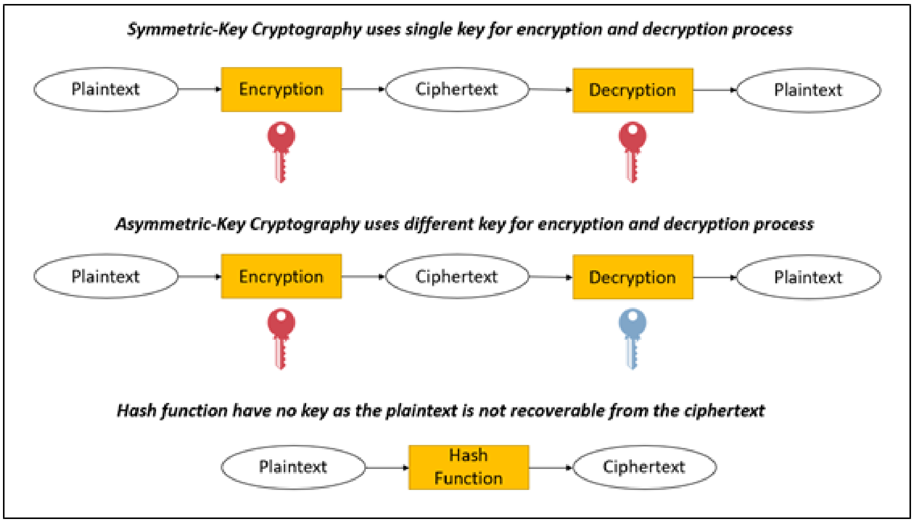
Symmetric-Key Cryptography uses single key for encryption and decryption process
Plaintext
Encryption
Ciphertext
Decryption
Plaintext
Asymmetric-Key Cryptography uses different key for encryption and decryption process
Plaintext
Encryption
Ciphertext
Decryption
Plaintext
Hash function have no key as the plaintext is not recoverable from the ciphertext
Plaintext
Hash Function
Ciphertext

Figure 1: Types of cryptography

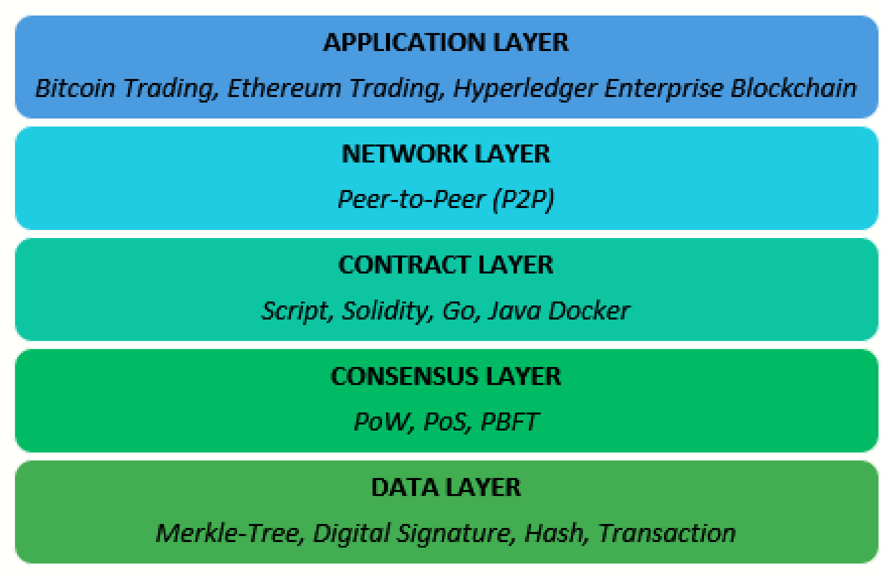
APPLICATION LAYER
Bitcoin Trading, Ethereum Trading, Hyperledger Enterprise Blockchain
NETWORK LAYER
Peer-to-Peer (P2P)
CONTRACT LAYER
Script, Solidity, Go, Java Docker
CONSENSUS LAYER
PoW, PoS, PBFT
DATA LAYER
Merkle-Tree, Digital Signature, Hash, Transaction

Figure 2: Blockchain layers

3.1 Data layer

The data layer relies mainly on the block data structure to assure the integrity of data storage. As the network grows, each node creates a new block of data linked to the longest primary blockchain, encapsulating all of the transactions it has received throughout that time. Block storage, chain structure, hash algorithm, Merkle tree, and timestamping are all included in this layer.

3.1.1 Consensus layer

The consensus layer is required for blockchain systems to function. The consensus layer primarily consists of a consensus mechanism that allows each node in the decentralized system to achieve a consensus on the validity of block data. The consensus layer is the most essential and required component of any blockchain, whether Ethereum, Hyperledger, or another. The consensus layer is responsible for verifying blocks, sorting them, and ensuring everyone agree. The consensus mechanism consists mainly of Proof of Work (PoW), Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), and Simplified Byzantine Fault Tolerance (SBFT).

3.2 Contract layer

The blockchain programmable feature is built on the smart contract, which is mostly featured in the contract layer. The blockchain stores the computerized software that may automatically execute the contract conditions in the form of code and data sets. Smart contracts, which are triggered by time or events, are distributedly performed by blockchain nodes. Signatures or other external data signals prompt the coding of all relevant phrases, which are automatically resolved.

3.3 Network layer

Various data transmission methods and verification procedures are included in the network layer. The network layer, also known as the P2P layer, is in charge of inter-node communication. In addition, the network layer handles discovery, transactions, and block propagation.

A peer-to-peer network is a computer network in which nodes are spread and share the network's workload to achieve a shared goal. This P2P layer guarantees that nodes can discover one another and interact, disseminate, and synchronize in order to maintain the blockchain network functioning properly.

3.4 Application layer

Bitcoin, Ethereum, and Hyperledger are examples of application layers. Bitcoin is mostly used for electronic monetary transactions. Ethereum introduces digital currency-based decentralized apps. Hyperledger is used mainly for enterprise-level blockchain applications and does not facilitate digital currency transactions.

4 HASH FUNCTION

Hash functions are crucial in connecting the blocks and maintaining the integrity of the data stored within each block. It is one of the fundamental building blocks of blockchain technology. The most important characteristic of a blockchain is immutability, which is made possible by hashing. Any change to the block data can produce inconsistency and hence invalidate the blockchain. This criterion is provided by the hash function property known as the 'avalanche effect.'

A blockchain is a shared ledger that records all transactions and data changes that have occurred since the ledger was initially recorded. This ledger is divided into blocks inside the blockchain. Each block records a particular amount of transaction information, which is then connected or chained with the preceding block using a cryptographic hash function up to the first block, known as the genesis block. Figure 3 depicts the data structure of the Bitcoin blockchain, which serves as the foundation for the data structure of subsequent chain blocks (Hu et al. (2021)).

Each block consists of a block header and a body block. The block header contains the hash value of the previous block H_{Prev}, the current consensus version number v, the current mining difficulty parameter d, a time stamp, t which stamps the current time in seconds according to universal time, the transaction hash value formed through the Merkle tree method H_{root} and nonce n_r. The body of the block consists of the transaction sent to the chain block Tx_j, where Tx is the transaction and j represents the number sequence of the transaction recorded by the block. All these transactions will be compiled using the Merkle tree method to calculate the H_{root} value which will then be the value stored in the block header.

The Merkle tree method is clearly illustrated in Figure 3 where every two adjacent transactions will be combined. The combined hash value of these two transactions is produced using cryptographic techniques to be used in the upper layer. This process is repeated until there is only one hash value (H_{root}) which is the top value in the Merkle tree. If there is only one transaction at the end of each layer, it will be duplicated and merged with itself, as shown in the path $H_5 \rightarrow H_{55} \rightarrow H_{555}$ in Figure 3. Merkle tree stores hash values for all transactions stored in a block.

The attributes of hash functions also provide other advantages such as access to ownership documentation without really disclosing the information, protection against unapproved changes to transactions and verification of a confirmed transaction without having full access to the block.

5 PUBLIC KEY CRYPTOGRAPHY

Asymmetric encryption is commonly used to confirm the authenticity of data using public-key cryptography. In classical computing, public-key cryptogra-

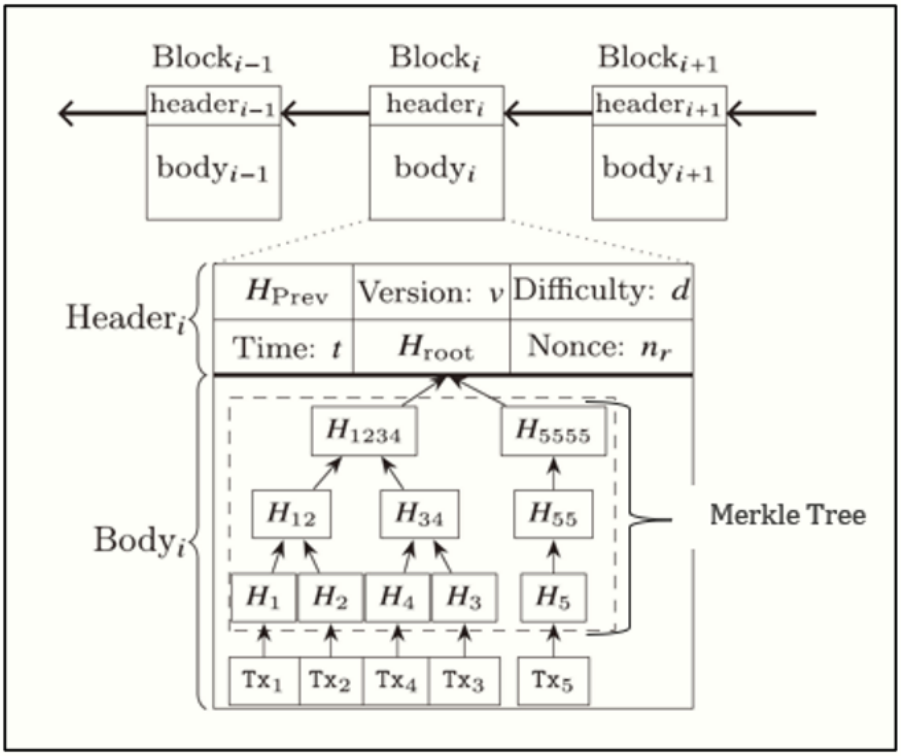

Figure 3: General block structure in blockchain (Hu et al., 2021)

phy was initially employed to encrypt and decrypt messages. In cryptocurrencies, the creation of wallets and the signature of transactions, which are necessary components of any currency, rely heavily on public key cryptography. The underlying technology of cryptocurrencies would be nearly hard to implement without public-key cryptography.

The secret of public key cryptography is the “trapdoor functions,” which are one-way mathematical functions that are easy to solve in one direction but nearly impossible to break in the opposite direction. While it is feasible, reverse engineering these functions would require a supercomputer and hundreds of years.

Each user’s address is computed using a hash function derived from the public key. These addresses are used to transfer and receive assets on the blockchain. The public key is globally available so all session participants can see it. Furthermore, because public keys include no personally identifiable information, they can be shared with other network users.

For example, in the Bitcoin cryptocurrency, the Elliptic Curve Digital Signature Algorithm (ECDSA) generates a fresh set of private and corresponding 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 funds. The private key is kept secret and is used to sign a digital transaction to confirm its legitimacy.

6 DIGITAL SIGNATURES

Blockchain applications use cryptography methods and encryption keys to utilise the idea of physical signatures. Advanced mathematical codes are used in cryptography techniques to store and transmit data values in secure formats. Because of this, it guarantees that only the people for whom the transaction or data is meant can acquire, read, and process the transaction or data, as well as confirm the legitimacy of the participants and the transaction.

Cryptocurrency trading, also known as "crypto trading," has grown in popularity over the past decade since Bitcoin's introduction on the internet. Crypto trading is the exchange of one form of cryptocurrency for another. These transactions are carried out through the use of user wallets and cryptocurrency exchanges. An example of digital signatures usage in blockchain is depicted in 4 below.

Private keys are used in blockchain networks to gain access to funds and private wallets. In the meantime, the usage of digital signatures in cryptocurrency trading protects user identification and security. Digital signatures are similar to physical signatures on documents. They aid in ensuring that the author of a transaction is, in fact, the person who possesses the private key.

The use of digital signatures ensures the process's validity; once com-

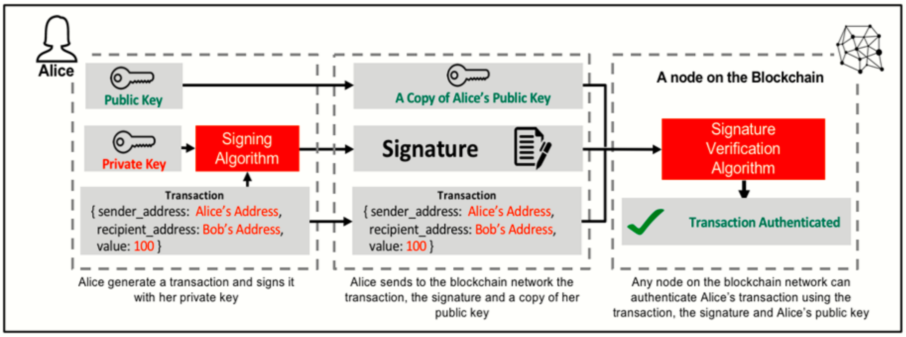
Alice
Public Key
Private Key
Signing Algorithm
Transaction
{ sender_address: Alice's Address, recipient_address: Bob's Address, value: 100 }
A Copy of Alice's Public Key
Signature
Transaction
{ sender_address: Alice's Address, recipient_address: Bob's Address, value: 100 }
A node on the Blockchain
Signature Verification Algorithm
Transaction Authenticated
Alice generate a transaction and signs it with her private key
Alice sends to the blockchain network the transaction, the signature and a copy of her public key
Any node on the blockchain network can authenticate Alice's transaction using the transaction, the signature and Alice's public key

Figure 4: Digital signature in blockchain

pleted, the results cannot be falsified and can't be changed. In addition, they are utilised for multi-signature contracts and digital wallets hosted on the blockchain to safely sign off on transactions (offline). Multiple (different) private key signatures are necessary in order to carry out any operation that falls under the terms of these multi-signature contracts and digital wallets. Therefore, digital signatures ensure that the data on a blockchain is accurate and that the blockchain itself maintains its integrity.

In Bitcoin crypto-trading, digital signatures serve as the backbone, with each transaction having a unique digital signature based on the user's private key. If you have the message, the user's public key, and the signature, it's not easy to figure out if the signature is real. More formally, digital signatures depend on two functions:

1. Sign (Message, Private Key) → Signature
   Given the message to sign and a private key, this function generates the message's unique digital signature

2. Verify (Message, Public Key, Signature) → True/False
   Given the message to verify, the signature, and the public key, this function returns a binary value indicating whether or not the signature is genuine.

Once the owner has signed the transaction, it is delivered to the memory pool, where miners will process it. Miners utilise the sender's public key to validate the digital signature, preventing hackers from spending user funds without their permission. If the ownership and digital signature are valid, the transaction is included in the following block and funds are transferred from one wallet to another.

7 CRYPTOGRAPHY APPLICATION IN BLOCKCHAIN CONSENSUS MECHANISM

Consensus is required to confirm transactions and update the ledger. Blockchain technology employs a consensus process to establish an agreement on a data value (transaction) without the intervention of a centralised authority. Proof Of Work (PoW) and Proof Of Stake (PoS) are two of the most well-known consensuses. There are numerous other consensus mechanisms in use at the moment, including Proof Of Identity, Proof Of Importance, and Proof Of Existence (Bhutta et al. (2021)).

The consensus mechanism ensures that all transactions in a block are confirmed and agreed upon before forming a new block. It is carried out by special nodes known as miners. Each blockchain platform has its own consensus protocol mechanism, such as Bitcoin, Ethereum, Hyperledger, and others.

A miner (or miner node) is a computer that performs the mining process in the blockchain in order to create and add new blocks to the existing network. Although mining is commonly connected with Bitcoin, mining is also used in other blockchain-based technologies. The mining process generates a hash value for each block that cannot be readily falsified and ensures the integrity of the entire block without the need for a centralized mechanism.

The Bitcoin protocol also extensively uses cryptography to compute the proof of work function. Miners use a large number of inputs to compute the "SHA256 Hash Function" until they locate the nonce for a certain block before adding it to the blockchain. The difficulty of mining is determined by how many zeroes the hash must begin with in order to be included to the network. This is a one-of-a-kind method in that it adjusts higher or lower based on how many people are mining at any given time. It also makes it computationally impossible for an attack vendor to go back and modify previously recorded transactions on the blockchain.

8 CRYPTOGRAPHY BENEFITS IN BLOCKCHAIN

There are a variety of advantages that cryptography brings to blockchain, some of which are listed below:

i Security
Blockchains use cryptographic hashing to store root hashes that securely encode each transaction. An entirely different hash will be generated at the root hash if someone attempts to alter any data in the blockchain. Other users can determine that the data has been compromised by comparing the hash value.

ii Immutability
This characteristic of cryptography is crucial for blockchain because it enables blocks to be securely linked by other blocks and ensures the dependability of the data stored there. It also makes sure that an attacker cannot use previous queries and their corresponding signatures to create a valid signature for newly posed queries.

iii Encryption
Cryptography makes use of asymmetric encryption to guarantee that transactions on their network does protect their data and communications from unauthorised disclosure and access.

iv Non-repudiation
The non-repudiation function offered by the digital signature protects against any denial of a communication sent by the sender. This advantage is related to the fact that there are no collisions between the messages delivered because each input value has a distinct hash function, making it simple to distinguish one message from the next.

v Irreversible
Reverse engineering is impossible using strong cryptographic algorithms

like hash functions; that is, we cannot generate the input by using the output and the hash function.

9 CONCLUSION

The technology of cryptography is the foundation on which blockchain is built. Cryptography's main uses revolve around ensuring that participants and transactions are secure, protected against double-spending, and preventing interference with central authority and operations. By utilising cryptographic techniques and encryption keys to offer the necessary security, blockchain technologies use the idea of real-world signatures to ensure data integrity.

REFERENCES

Bhutta, M. N. M., Khwaja, A. A., Nadeem, A., Ahmad, H. F., Khan, M. K., Hanif, M. A., Song, H., Alshamari, M., and Cao, Y. (2021). A Survey on Blockchain Technology: Evolution, Architecture and Security. *IEEE Access*, 9:61048–61073.

Buterin, V. (2014). Ethereum Whitepaper. *Ethereum*.

Foundation, H. (2018). An introduction to Hyperledger. *Linux Foundation: San Fransisco, CA, USA*, pages 299–348.

Hu, B., Zhang, Z., Liu, J., Liu, Y., Yin, J., Lu, R., and Lin, X. (2021). A comprehensive survey on smart contract construction and execution: paradigms, tools, and systems. *Patterns*, 2(2):100179.

Nakamoto, S. (2008). Bitcoin: A peer-to-peer electronic cash system. *Decentralized Business Review,*, (21260).

Voshmgir, S. (2019). *Token economy: How blockchains and smart contracts revolutionize the economy*. Shermin Voshmgir-BlockchainHub.

Wang, H., Zheng, Z., Xie, S., Dai, H. N., and Chen, X. (2018). Blockchain challenges and opportunities: a survey. *International Journal of Web and Grid Services*, 14(4):352.