BLOCKCHAIN CRYPTOGRAPHY AND SECURITY ISSUES

Mohamed Abdelrahman

Pre-Masters of Software Engineering, College of Statistical Studies and Research,
Cairo University, Egypt.

ABSTRACT

Transaction records and other user information are stored in blocks that form a distributed ledger called blockchain. For blockchain to gain widespread adoption, it is crucial that user and transaction data be kept safe. This technology provides cryptographically safe and anonymous financial transactions among the user nodes of the network allowing the transactions to be evaluated and authorized by all the users in a transparent environment.

In this paper, we provide a comprehensive overview and classification scheme for all cryptographic ideas currently used in blockchain. Moreover, the current security issues of blockchain are shown, and a future research objective is predicted.

KEYWORDS

Blockchain, cryptography, hash function, proof-of-work, consensus, signature, encryption.

1. INTRODUCTION

A Blockchain is a distributed ledger that runs on a peer-to-peer architecture network. Blockchain gets its name from the fact that it is a decentralized ledger consisting of a sequence of "blocks." Since Satoshi Nakamoto devised and introduced the core idea of bitcoin [1]. There are several types of blockchain platforms, such as public chain, private chain, and alliance chain. Alliance chains are controlled cooperatively by several participating institutions, whereas private chains severely restrict qualification of participating nodes. To ensure the safety of all user transaction data, blockchain must function to a very high standard. Each node may operate independently of every other, and there is no one authority figure or hub. Therefore, blockchain transactions must protect the confidentiality of information sent through insecure networks and guarantee the authenticity of all transactions. There's no doubt about it: cryptography is the backbone of the blockchain. Protecting user data and transaction records, as well as ensuring data integrity, etc., are primary uses for cryptography in blockchain [2]. Various cryptographic methods, including hash algorithms, asymmetric encryption algorithms, and digital signatures, are introduced briefly in this paper. Also paper provides a thorough breakdown of how cryptographic technologies safeguard personal information and the integrity of ongoing transactions. In addition, there are already vulnerabilities in the blockchain's security system.

2. TYPES OF BLOCKCHAIN

2.1.Public Blockchains

A public blockchain is a blockchain that is open-source, freely accessible to anybody who wants to utilize it. There is no central authority in charge of the network; instead, anybody may join it and see, alter, or audit the blockchain at any time [3].

2.2.Private Blockchains

Private blockchains are permissioned blockchains that are administered and operated by a single entity. Who may participate as a node in a private blockchain network is decided by the network's administrator. It's also possible that the central authority may not provide every node the same access to resources or powers. Since the general public does not have access to private blockchains, they are only semi-decentralized. Ripple, a network for exchanging virtual currencies between businesses, and Hyperledger, an umbrella project for open-source blockchain applications [4] are both instances of private blockchains.

2.3.Consortium Blockchains

When compared to the private blockchain, which is controlled by a single corporation, the consortium blockchain is regulated by a collection of companies. Therefore, consortium blockchains provide more decentralization than private blockchains, which leads to greater security. However, establishing consortiums calls for collaboration across several institutions [5].

2.4.Hybrid Blockchains

When the public blockchain and the private blockchain are combined, we get a hybrid blockchain. Because some transaction validations need both the secrecy afforded by private blockchains and the transparency afforded by public blockchains, a hybrid blockchain incorporates the best features of each [4].

3. BLOCKCHAIN INFRASTRUCTURES

There have been two distinct eras in the development of blockchain technology; the first, represented by Bitcoin, was an era of multi-technology portfolio innovation called blockchain 1.0; the second, characterized by the transfer of digital assets called blockchain 2.0, is exemplified by Ethereum. Bitcoin, Ethereum, Hyperledgers, etc., are some of the most well-known implementations of blockchain technology. There are significant architectural similarities even though the implementations are unique. According to Data Table 1.

Table 1. Blockchain architecture.

	Bitcoin	Ethereum	Hyperledger
Application layer	Bitcoin trading	Ethereum trading	Enterprise blockchain
Network layer	TCP-based P2P	TCP-based P2P	HTTP/2-based P2P
Contract layer	Script	Solidity/Script EVM	Go/Java Docker
Consensus layer	PoW	PoW/PoS	PBFT/SBFT
Data layer	Merkle tree	Merkle patricia tree	Merkle Bocket tree

Keeping data safe is a top priority for the data layer, and it relies heavily on the block data structure to do it. Each network node collects the time-stamped transaction data it has received over a certain period of time into a data block, and then attaches this block to the longest running main blockchain. Block storage, chain structure, hash algorithm, Merkle tree, time stamp, and so on are all part of this layer's repertoire of essential tools, as shown in Figure. 1 [6].

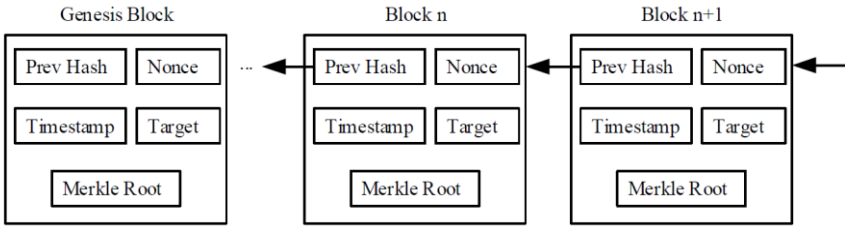

Figure 1. A sequence of blockchain showing block structure [6].

4. Blockchain Cryptographic

4.1.Hash Functions

The importance of cryptographic primitives like hash functions has grown in recent years. A hash function is a function that takes a block of binary data and outputs another block of binary data of the same size [7]. The term "hash" or "digest" is used to describe the outcome of such a process.
As with other cryptographic hash functions, SHA was developed and released by NIST. The SHA256 algorithm, a subset of the SHA-2 family of hashing algorithms, produces a message digest with 256 bits of data. There are two steps in the algorithm's computation process: message preprocessing and the main loop. In the message preprocessing stage, data of any length is subjected to binary bit filling and message length filling, and the resulting message is then split into multiple 512-bit message blocks. Each message block goes through a compression function in the main loop phase. This compression function takes as input the result of the previous compression function, and the final compression function takes as input the hash value of the original message.

For blockchain, Hash functions may be used to ensure the authenticity of each block and each transaction. Each block in a blockchain records a hash value based on the data in the prior block's header, and any user may verify the validity of a transaction by comparing the two values. Finally, the preceding block's data is checked for integrity. The hash function may also be used to produce public-private key pairings.

The hash pointer is a special kind of data structure that stores not just pointers but also the encrypted versions of the data and any related passwords. To check whether data has been altered, a hash pointer may be compared to a previous value stored in the same location, which is done with a regular pointer [8], as shown in Figure 1.

4.2.Public Key System

Symmetric encryption and asymmetric cryptography are the backbone technologies of the field. The issue of premature key distribution in symmetric encryption may be satisfactorily addressed by using an asymmetric method of encryption known as public key encryption. Asymmetric encryption algorithms use two separate keys—a public key and a private key—to encrypt and decode data. A random number algorithm is often used to produce the private key, whereas an irreversible technique is used to determine the public key.

Common public key encryption algorithms include those based on elliptic curves. The level of safety is proportional to the complexity of the discrete logarithm problem for elliptic curves [9]. In the blockchain, secp256k1 is utilized as the elliptic curve public key encryption technique. For secp256k1, an elliptic curve over a finite field was chosen as the basis cryptographic structure. Because of its unique design, its optimal implementation may provide a 30% gain in performance

compared to other curves. Secp256k1's constant is able to successfully prevent backdoors.
For blockchain, Bitcoin uses a pair of keys, a private one and a public one that is completely different from every other Bitcoin user's. Public key encryption is used to create the key pair. An individual's public key serves as their address in the payment link of bitcoin transactions; this address is known as the bitcoin address [10], as shown in Figure 2.

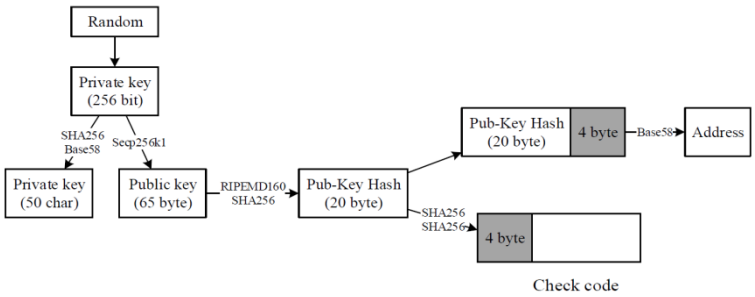

Figure 2. Bitcoin address generation process [10].

4.3.Digital Signature

Signature algorithms and verification algorithms are the two main components of a digital signature system. When a communication is digitally signed, the signature algorithm is used to create the signature and the signature key is used to govern the signature. Both the signature algorithm and the signature key are kept secret and are within the signer's control. The digital signature of the message may be checked using the verification algorithm, and the message itself can be validated using the signature. The verification algorithm is typically under the control of the verification key, but both the algorithm and the key are freely available to anybody who needs to verify the signature.

When using blockchain, a digital currency's current owner hashes both the content of the previous transaction order and the address of the next owner. After the list of transactions has been transmitted, the data digitally signed with its own private key is attached. The receiver is responsible for verifying the prior owner's details and the transaction's true owner. In the blockchain, the present owner, the prior owner, and the future owner are all recorded for each transaction. Therefore, all monetary transactions can be tracked back to their origin, eliminating the possibility of duplicate payment or other problems [11], as shown in Figure 3.

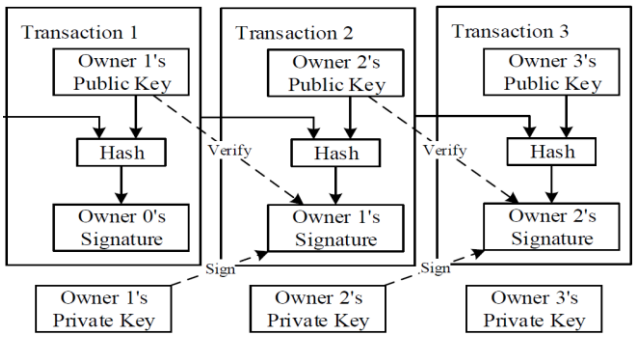

Figure 3. Blockchain transactions [11].

The payer typically completes the signature portion of the transaction authentication procedure.

The payer of the transaction first calculates the hash value by hashing the data from the preceding transaction. By utilizing its own secret key, the payer encodes the hash. During the same transmission of the digital signature and the prior transaction data, the encrypted data is also delivered to the receiver. In order to ensure the legitimacy of the transaction, the receiving party will use the same hash algorithm used in the preceding phase to generate a hash summary from the data it has received. Finally, the extra digital signature from the previous phase is decrypted using the payer's public key to produce a new hash digest. Order reliability may be checked by comparing the two summaries. The receiver may verify the legitimacy of the order by comparing the contents of the two.

4.4.Consensus Algorithm

By validating transaction data and identifying the accounting nodes in the blockchain network, the consensus Algorithm. guarantees that each block's contents is consistent. An early form of the Bitcoin network relied on an algorithm called Proof of Work to validate transactions (PoW). This Algorithm significantly utilizes the processing capacity of each node to guarantee accurate distributed accounting throughout the Bitcoin network. To guarantee the integrity and privacy of all blockchain data throughout the whole network, the PoW Algorithm depends on a competition of computer power between dispersed nodes. The SHA256 hash value of the original data in the block header must be less than the setting value of the difficulty goal in the block header, and each node must depend on its own resources to solve this calculation issue by determining a sufficient random number, or Nonce. As a result, some implementations will switch to a proof-of-stake scheme rather than a proof-of-work one. In Proof of Stake, the node with the largest stake is chosen to create the next block. If a node has a lot at risk, it is less likely to broadcast a malicious block. No way would they take such a risk. There is a huge time and energy savings when switching from Proof of Work to Proof of Stake. This is why many people include proof of stake into their model [12], as shown in Figure 4.

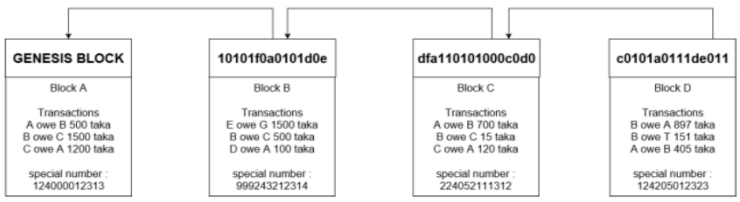

Figure 4. Proof of Stake blockchain [12].

5. BLOCKCHAIN SECURITY ISSUES

5.1. Vulnerabilities at Blockchain Endpoints

Despite blockchain's reputation for security, most blockchain transactions include intermediaries whose security can't compare to that of the blockchain itself. For instance, a "hot wallet," also known as a "virtual savings account," may receive a big quantity of bitcoin as a consequence of bitcoin trading or investment. It's possible that wallet accounts are not as secure as the blockchain blocks themselves against tampering.

Several outside businesses may be used to ease the process of doing blockchain-based transactions. Technology such as payment processors, smart contracts, and blockchain-based payment systems are all good examples. Hackers might find easy pickings in the applications and websites of these third-party blockchain businesses.

5.2. Public Blockchains Scalability Issues

We are already working with the biggest blockchains ever created, and that size will only increase as blockchain technology gains traction. Some industry insiders are apprehensive because these enterprise-level blockchains have yet to be put through their paces. Some people worry that as the blockchain ecosystem develops, more flaws may be found and exploited, or that the underlying technological infrastructure will become more prone to basic errors.

5.3. Public Blockchains Regulation Issues

Additionally, the lack of well-defined regulatory norms is a problem for blockchain security. Due to the lack of uniformity in the blockchain space, it is difficult.

5.4. Public Blockchains Insufficient Testing

As a last point, it's important to note that blockchain technology is finding expanding use outside of the realm of bitcoin exchanges. Hackers may be able to uncover and exploit flaws in non-cryptocurrency apps since their code is often untested and very experimental.

6. CONCLUSION AND FUTURE WORK

This paper provides an overview of the most prominent cryptographic use cases on the blockchain and provides an examination of the current issues facing this technology. The Types OF blockchain are presented first, followed by the blockchain architecture, and then the cryptographic technology that is used to develop the blockchain. This brings us to our last topic: the blockchain's current security flaws. The results prove that digital encryption technology is fundamental to the blockchain infrastructure. This study foresees the future research trajectory of blockchain technology, highlighting the vital role that cryptography studies play in the system's evolution.

In future research, is to design a coin-rich system that is secure thanks to cryptographic safeguards while also reducing the required computing power. The security of the blockchain might be enhanced with the use of a more robust and trustworthy cryptographic encryption technique.

ACKNOWLEDGEMENTS

The authors would like to thank DR. Ahmed Hamza, Department of Computer Science, College of Statistical Studies and Research, Cairo University, Egypt.

REFERENCES

[1] Bitcoin: A Peer-to-Peer Electronic Cash System, S Squarepants, 2008.
[2] Research on the construction of accounting information audit quality control system based on blockchain, J Wang, 2022.
[3] “Different Types of Blockchains are There” - Dragonchain, https://dragonchain.com/blog/differences-between-public-private-blockchains.
[4] “Different Types Of Blockchains In The Market And Why We Need Them”, https://coinsutra.com/different-types-blockchains.
[5] Voting System for Handicapped People using Blockchain System, Aishwarya Gade, Vaishnavi Pawar, Safiya Shaikh, Samiksha Mali, Prof. Mrs. S. P. Kakade, 2022.

[6] A survey on security and privacy issues of blockchain technology, A Prashanth Joshi, , M Han, Y Wang, 2018.
[7] Review of understanding cryptography S Moulick, 2014.
[8] Cryptography in Blockchain. Journal of Nanjing University of Posts and Telecommunications, Wang, H.Q., Wu, T., 2017.
[9] An Area Efficient Approach to Design Self-Timed Cryptosystems Combatting DPA Attack, D LEE, 2005.
[10] Blockchain technology and its application, H Dikariev, M Miłosz, 2018.
[11] Application of Technologies of Distributed Ledgers (Blockchain) in the Management of A Decentralized Autonomous Organization (DAO), A Burkov, 2020.
[12] Secure Replication in Distributed System using RSA & SHA1 algorithm, 2017.

Author

Mohamed Abdelrahman Pre-Masters of Software Engineering, College of Statistical Studies and Research, Cairo University, Egypt Post graduate diploma of Statistical Data Science, College of Statistical Studies and Research, Cairo University, Egypt BSc Computer Science & information Cisco Certified Network Associate (Cert. No.:424424171213BMCI) Microsoft Certified Systems Administrator (Cert. No.:I371-8995) Microsoft Certified Professional (Cert. No.:I371-8988) Microsoft Office Specialist (Cert. No.:C077-9810) International Computer Driving Licence (Cert. No.:UN05072003)