ALGORITHMS FOR ENSURING THE SECURITY OF RECEIVING AND TRANSMITTING TRANSACTION BLOCKS IN BLOCKCHAIN TECHNOLOGY

Raxmonova Visola Miraxmad qizi
2nd year master's degree at Tashkent University of Information Technologies named after Muhammad al-Khwarizmi.

Abstract. This article discusses about the possibilities of the blockchain, the transaction process and the stages of its integration into the blockchain. In addition, from algorithms for ensuring the security of receiving and transmitting blocks of transactions in blockchain technology, cryptographic algorithms, electronic digital signature, hashing functions, peer-to-peer network, proof-of-work processes were considered.

Keywords: blockchain, transaction, authentication, authorization, digital signature, hashing, peer-to-peer network, proof of work.

Introduction

Today, one of the technologies that provide reliable protection of information from the first source to the final recipient is the Blockchain Systems technology. Blockchain technology (Blockchain or chain of transaction blocks) immediately attracted a lot of attention in special and mass discussions from the day it was introduced. Some of his fans have even declared blockchain to be the greatest invention since the internet. The main proponents of blockchain believe that the benefits of blockchain lie in its integrity, reliability, and complete transparency of transactions. This technology is often suggested to be used for simple transactions. Smart contracts or smart contracts guarantee the execution of the transaction: records of transactions made in accordance with the contract are placed in a decentralized ledger of the blockchain, and all participants in the transaction can see any changes in it.

What is blockchain?

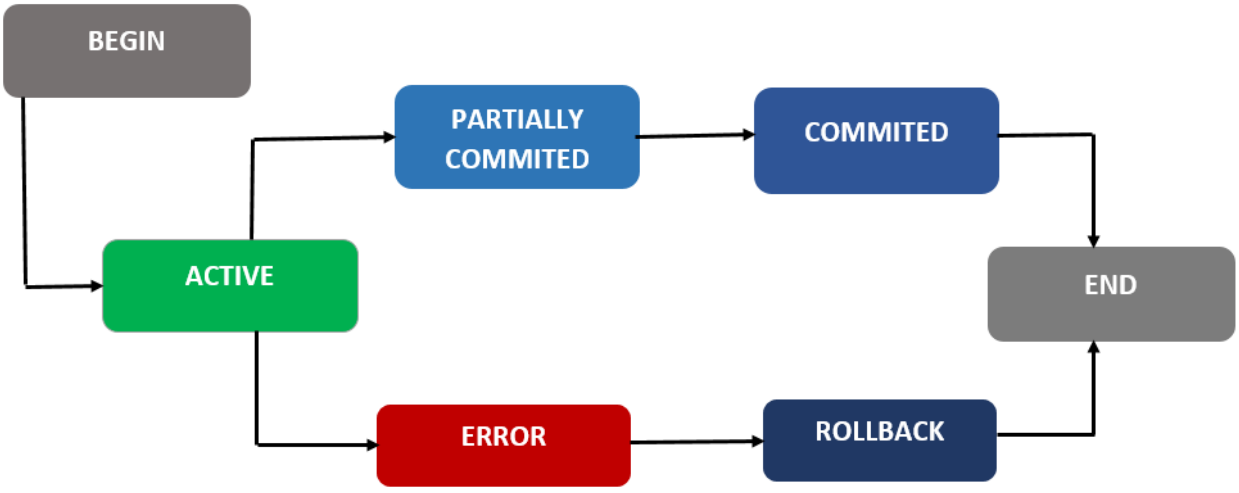
Blockchain is a chain of interconnected data that is recorded in blocks. It's convenient to think of it as an immutable singly linked list that is shared between the nodes of a computer network. As a database, the blockchain stores arbitrary (most often small) information in a digital format. To the general public, blockchain is best known for its important role in cryptocurrency systems to provide a secure and decentralized record of transactions. The innovation of the blockchain is that it guarantees the accuracy and security of data recording and inspires trust without the need for a trusted third party – so that the system can operate autonomously. The purpose of the

blockchain is to allow digital information to be recorded and distributed, but not edited. Thus, the blockchain is the basis of immutable ledgers or records of transactions that cannot be changed, deleted or destroyed. Blockchain offers the guarantee of a secure, distributed and transparent exchange of information of any kind between two parties. For example, in the case of cryptocurrencies, this information uniquely identifies a transaction between users - its author and recipient, thereby guaranteeing the security of the transaction itself.

Transaction and transaction states

A transaction is a sequence of operations performed on a database that takes it from one consistent state to another. When a database session occurs, a transaction begins. For example, we can bring the bank transfer process. The amount of 100 trillion soums will be transferred from the current account to the card account. The program withdraws the amount from the current account and then adds it to the card account. When the program is running, after making the first change, the power is turned off and the card counter does not increase. To avoid this situation, both teams must make a deal. If all commands in the transaction fail, the transaction is rolled back.

A transaction is considered as an atomic operation, but in reality it goes through a number of states during its lifetime. The transactions boundaries are specified by BEGIN-TRANSACTION and END-TRANSACTION statements. For recovery purpose (in case of data lost), the system needs to keep track of all these states.



Pic.1. Transaction States Diagram

As above image clearly depicts, transaction states are –

BEGIN: The database is in a consistent state before a transaction begins. The transaction on the database begins by the execution of the first statement of the transaction.

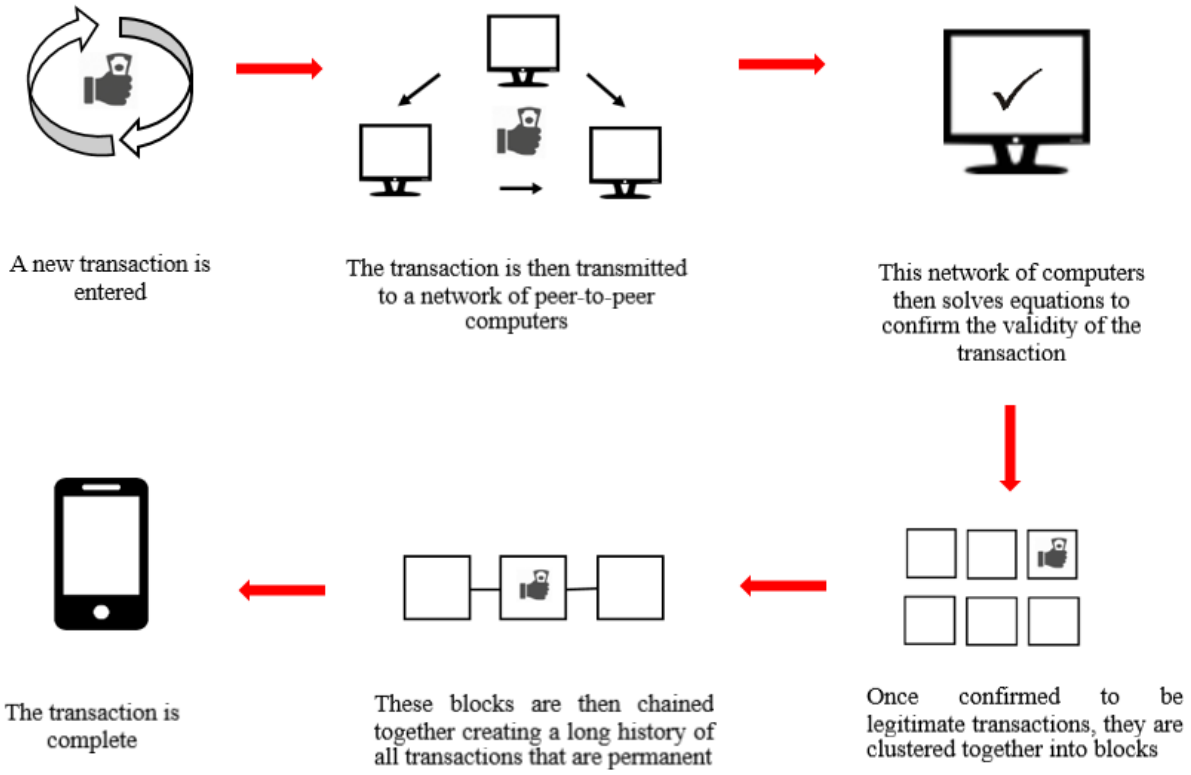
ACTIVE state, the transaction is modifying the state of the database. This means that the transaction performs write operations on the database items. At the end of the active state, the transaction enters one of three states: commit, abort or error.

COMMIT statement (complete execution) signals the successful completion of a transaction. It tells the transaction manager that the logical unit of work has successfully completed, the database is again (or will be after the execution of this statement) in a consistent state, and all queries and updates performed by this transaction can now be committed, i.e. made to database.

ROLLBACK statement is used when it is necessary to undo the changes made by a transaction and restore the database to its previous state. The operator informs the transaction manager that some kind of system failure has occurred, the database is in an inconsistent state, and all queries and updates performed during this transaction should be rolled back, i.e. they should be canceled, and the database returned to its original state.

How does a transaction get into the blockchain?

There are several key steps a transaction must go through before it is added to the blockchain. Before a transaction is added to the blockchain it must be authenticated and authorised.



Pic.2. Adding a transaction to the blockchain

Authentication. The blockchain was originally designed to operate without a central authority, but transactions still have to be authenticated. This is done with

cryptographic keys, a string of data (such as a password) that identifies the user and gives them access to their "account" or "wallet" on the system. Each user has their own private key and public key that everyone can see. Using both of them ensures that the user is authenticated with digital signatures and the transaction they want to make is done securely.

Authorization. Once a transaction is made between users, it must be approved or authorized before it can be added to a block in the chain. For a public blockchain, the decision to add a transaction to the chain is made by consensus. This means that the computers on the network must agree on the authenticity of the transaction. The people who own the computers in the network are encouraged to confirm transactions with rewards. This process is called "proof of work".

Blockchain Security Support Algorithms

As blockchain implementations grow in popularity, there are issues with the technology's security. Therefore, people are increasingly interested in understanding blockchain security algorithms. Blockchain technology uses the following algorithms to ensure security.

Cryptography algorithms. A blockchain is an ever-growing collection of records called blocks. With any other approach than today's blockchain, as the network grows, it would be difficult to ensure that all information on the blockchain is protected from any unwanted threats. Therefore, cryptography is one of the main requirements of the blockchain. In most applications in the modern world, cryptography is used to encrypt the transmission of data over insecure communication channels. A platform is proposed for setting up protocols and methods to avoid third parties interfering in accessing and obtaining information about data in personal messages in the communication process. If we look at the Bitcoin network, we will see that it does not use encryption. The Bitcoin blockchain is an open distributed database, so there is no need to encrypt it. All data is transmitted through the nodes in an unencrypted form, which allows strangers to interact through the Bitcoin network. In the case of blockchain, cryptography allows you to create a system in which changing old blocks by a group of attackers becomes virtually impossible.

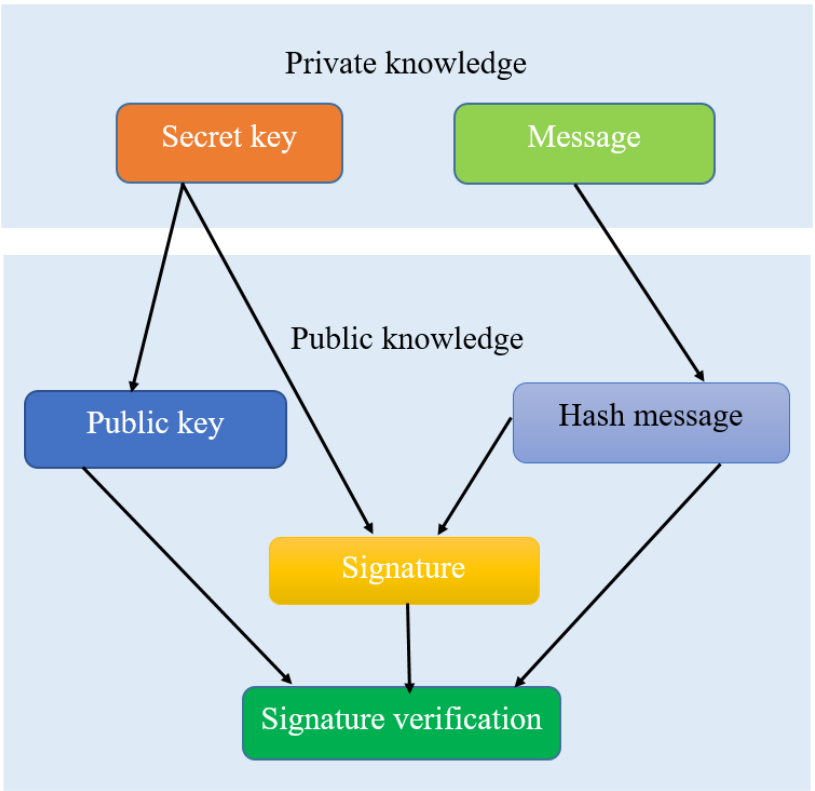
Digital signature. A digital signature is a cryptographic algorithm based on asymmetric encryption: using a private key, the author (who is also the sole owner of this key) can sign any message. The signature is most often performed on the hashed data contained in the message. Then, using the public key (which is made available to the public), any user can verify that it was the key holder who signed the message. In the case of blockchain, the user signs any transaction outgoing from him with his private key. The recipient, like any other network member, can decrypt the transaction to verify that the transaction really came from this sender, using the public key provided by the sender.

Due to digital signatures, it becomes impossible to spend the user's funds without his knowledge, because without his private key, the transaction will not receive the correct signature and, as a result, will not be accepted by the network of nodes participating in the blockchain. At the same time, the impossibility of forging a signature (in other words, selecting a private key) is ensured by the complexity of breaking the asynchronous encryption algorithm, which underlies the chosen signature method.

For example, Bitcoin implements the ECDSA (Elliptic Curve Digital Signature Algorithm) algorithm. ECDSA is a cryptographic scheme for creating digital signatures using public and private keys.

To generate a public key, you need to: generate a secret key → multiply the secret key by the generation point (point on the curve) → public key.

The multiplication operation is a point multiplication, which is different from the usual one. It is important to note that dot division is not calculable, so the public key cannot be used to derive the private key, which is what makes the ECDSA scheme so secure.



Pic.3. Digital signature structure

Hashing. Hashing is the process of converting an array of input data of arbitrary length into an (output) bit string of fixed length. Before transactions are combined into blocks, each transaction must be hashed. The hash added to the block is compiled based on the data recorded in this block. In addition to the hash of the block itself, the hash

of the previous block is added to it, due to which an associated sequence of blocks is created. The hashing algorithms used in the blockchain provide the so-called avalanche effect - even a small change in the hashed data leads to a significant change in the hash. Therefore, a change made in any transaction already in progress will generate a completely different hash, which will then change the hashes of all subsequent blocks.

Hash functions properties:

a) The output of a hash function is always deterministic, that is, when passing the same input data to the same hash function, the output will always be the same

b) The output of the hash function is a random one-way function

c) Two identical hash values cannot have two different messages

d) A small change in the input changes the hash value so much that the new and old values seem uncorrelated.

These properties determine the usefulness of hash functions. It is always possible to trace whether the file we are transferring has been surreptitiously changed. And also property (b) means that the input data cannot be predictably formed to obtain a certain output. This makes it possible to use certain information as confirmation without disclosing the information itself.

In Bitcoin, basically the hash function is SHA-256. The hash is a large number, and in order for a miner to submit a block to the network, the hash of that block must be below a certain threshold. Since hashing is a random process, a valid hash can only be found by intensive guessing.

Peer-to-peer network. In large corporations, a huge amount of personal user data is stored on individual devices, which increases the risk of data loss in the event of a hack, mishandling or loss of the system. Blockchain intends to eliminate this dependence on the central government. To do this, the blockchain works in such a way that the nodes in the blockchain system can validate the legitimacy of a transaction instead of a third party.

Transactions between clients, such as sending and receiving digital money, are transmitted to every node in the network. Nodes ensure the reliability of a transaction before it is documented as a block on the blockchain by verifying the sender's past transactions to ensure that he/she has not double-spent or spent more than they are acquiring.

Later, protocols of agreement, such as verification of work and confirmation of the bet, are sent by the miners. These protocols allow nodes to agree on the order and amount of transactions. When a transaction is verified, it is distributed as a block on the blockchain. User protection is enhanced by the decentralized nature of the blockchain and the absence of the need for a central authority.

Proof of work. Proof-of-work is data that allows any node to verify that whoever created that block has done a significant amount of computational work. In other words,

no node can create a valid block without doing an indeterminate but significant amount of work. The creation of any block requires a certain amount of processing power, and any other node can verify that this power was spent by the one who created the block.

Unlike transactions, the proof-of-work system required for each block allows us to find a convenient solution: since each block requires a certain amount of work, it is only natural that the only valid blockchain is the one with the most blocks. Think about it: if a Proof-of-Work system works because each block requires a certain amount of work (and time), the longest set of valid blocks is the hardest to break. If a malicious node or group of nodes tried to create a different set of valid blocks, always choosing the longest blockchain, they would always have to repeat more blocks (because each node points to the previous one, changing one block forcibly changes all blocks after it).

Conclusion

In conclusion, we note that it is quite difficult to find the best blockchain security algorithms. Algorithms are tailored to solve specific problems given certain inputs. Cryptographic algorithms such as digital signatures and hashing help protect information from third parties. Consensus algorithms help ensure the integrity of participants and transactions in the blockchain network.

Thus, it is quite difficult to choose a specific algorithm to protect security in the blockchain. While the blockchain is inherently secure, immutable and transparent, algorithms are needed to ensure all these characteristics.

References

1. J. Usmonov va A. Saidov, ELEKTRON HUKUMAT TIZIMLARIDA BLOKCHEYN TEXNOLOGIYALARINI QO‘LLASH ASOSLARI, O’quv qo’llanma, Toshkent, 2021.
2. Geroni, D. Blockchain Security Algorithms Used To Protect The Blockchain Security / D. Geroni, K. Amer, U.F. Muhammad. – : , 2021. – 14 c.
3. Бахвалова, Е.А. Исследование алгоритмов консенсуса для блокчейн-платформ / Е.А. Бахвалова, В.А. Судаков, U.F. Muhammad. – Москва : ИПМ им.М.В. Келдыша РАН, 2021. – 16 с.
4. https://ilyarm.ru/uz/upravlenie-tranzakciyami-vypolnyaetsya-tranzakciya-na-summu-chto-eto-sms.html
5. https://www.euromoney.com/learning/blockchain-explained/how-transactions-get-into-the-blockchain#:~:text=For%20a%20public%20blockchain%2C%20the,to%20verify%20transactions%20through%20rewards.
6. https://habr.com/ru/post/595621/