

Blockchain And Its Impact On Information Security

Turdimurodov Jasur Ilkhomovich

Faculty of Construction Management
Samarkand State Architectural and Civil Engineering Institute
Samarkand, Uzbekistan

Abstract: *Our article is about blockchain technology, which is a hot topic today. We'll talk about what a blockchain is, what it does, and where it's used.*

Keywords— Blockchain, cryptocurrency, bitcoin, nebulis, guardian, Ethereum.

1. INTRODUCTION

Blockchain is a technology that allows system participants to reliably transfer assets to each other without an intermediary. For example, you can store records of money transfers in a blockchain. In cryptocurrencies, it is the blockchain that is used to record information about who, to whom, and how much virtual money has been transferred. However, other assets can also be stored in the blockchain. In general, what is possible to write on paper, it is possible to write all of those things in a blockchain, with only one difference - in a blockchain there is no possibility to exchange and falsify records. A shining example of the blockchain idea is Ethereum. It was founded by Vitaly Buterin, a 19-year-old programmer who was born in the Russian town of Kolomna and now lives in Canada. The platform is designed to create applications in the blockchain. Today, Ethereum is valued at \$ 703 billion.

2. MAIN PART

The structure of blockchain technology consists of the following principles:

1. Network integrity. Confidence arises within the system; it is not gained from the outside. Participants are honest in both word and deed, respect the interests of others, are willing to answer for the consequences of their actions, and their decisions are transparent. Integrity is coded at each stage of the process and distributed among all participants, meaning it does not belong to one person.

2. Load Distribution There is no single delete path. None of the participants can turn off the system. If the central authority blocks any person or group, the system will continue to operate. If about half of the network wants to gain control over the network, the rest will see what happens. The system treats all stakeholders equally. Satoshi Nikamoto, the app's programmer, programmed the app in such a way that those who contributed to the development of the app were encouraged. An active user of the network receives 50 bitcoins for each completed block after 4 years. After another 4 years - 25 bitcoins, then 12.5 and so on.

3. Security Every member of the Network must use encryption. Security measures are installed in the network. They ensure confidentiality and preservation of the original.

The user will have two keys: one to encrypt and one to decrypt. This method is called "public key infrastructure" (PKI).

4. Inviolability of Personal Information. People need to control their personal information. They must have the right to disseminate exactly what information belongs to them, when, how and to what extent.

5. Protection of rights The rights of owners are transparent and strengthened. Transaction time recording and PKI not only avoid double the cost, but also record the ownership of each bitcoin in the network. We will only be able to trade in things that belong to us. Apart from Bitcoin, this can be anything of value, including intellectual property rights.

6. Attraction The economy works better if it works for everyone. This means a reduction in access barriers. Anyone with a cell phone can participate in the market as a manufacturer or consumer. Satoshi proposed a "simplified verification of payments" method. So what are the capabilities of blockchain technology to ensure information security? We will try to answer this question in as much detail as possible below.

2.1 Blockchain and information security issues

New blockchain technologies are contributing to the revolution in information security. In addition, the launch of blockchain technologies will help protect data in personal messages, websites and apps that are popular in business and use. Blockchain's unique features have led to the emergence of several startups that specialize in blockchain technology, taking information security to a whole new level. Blockchain is a technology that helps encrypt actions performed on a file or object with code specific to the file. This encryption cannot be disabled, which makes the records of the files completely transparent: it is always known what transactions are made with it, when and by whom. Such a decentralized, autonomous approach to information security opens up long-awaited new opportunities in the field of Internet security in many areas, from business to social networks. First, and most importantly, the blockchain provides an opportunity to protect personal messages. Startups like Obsidian are designed to use blockchain technology to protect personal information on chats, messengers, and social networks. It is now well known that messengers are used not only for communication, but also for making payments. The vulnerabilities in Facebook,

Messenger, and WhatsApp are that they use sparse encryption and do not provide adequate protection for metadata, including the identity of the sender, his or her email address, and other credentials required to log in.

2.2 Protected messages

Obsidian Messenger plans to protect users' metadata using a blockchain. The user does not need to use email or any other authentication information to use the messenger. The metadata will be randomly distributed throughout the book and therefore will not be able to be collected at a single point where there is a possibility of distortion. This project is still in development, but other messengers can follow this scheme and protect their users' data in a similar way.

2.3 Protection from cyber attacks

Blockchain offers many opportunities to detect and repel organized hacking attacks on key websites on centralized servers. As a result of such attacks, users' access to the websites of PayPal, Twitter and Spotify has been blocked. The problem is that existing DNS servers lack security because they store the access key on a single server and place excessive reliance on caching. Startups like Guardian and Nebulis intend to change that by using a distributed network of blockchain-based keywords and keywords. Ultimately, blockchain protects servers from hacker attacks and ensures that they become an impregnable fortress. Blockchain is undoubtedly the most promising discovery in the field of information security in the last decade. This will revolutionize the development of information security systems and ensure a secure Internet for many years to come.

3. REFERENCES

- [1] Jacob William Blokchain: The simple Guide to everything you need to know. 2016 y.
- [2] Jeremy Clark Bitcoin, blockchain, cryptocurrency, cryptology and technical study of bitcoin, 499, 2016 y.
- [3] Roger Wattenhofer The science of blockchain. 2016 y.
- [4] Phil Champagne. The book of Satoshi ,, The Collected Writings of Bitcoin Creator Satoshi Nakamoto '' 396, 2014 y.
- [5] Melanie Swan. Blockchain: Blueprint for a New Economy. 2015 y.
- [6] Don Tapscott, Alex Tepscott. Blockchain revolution 2016 y.
- [7] Gulyamov SS, Abdullaev.A.M, Modern information systems and technologies in the economy. 2018
- [8] Генкин. Блокчейн: как это работает и что ждет нас завтра. 2018 592
- [9] Lapidus L.V Digital economy: management of electronic business and electronic commerce. INFRA-M 2017
- [10] Ayupov R. X. Baltabaeva GR Digital currency market, innovations and development prospects. 2018 y.