

THE BITCOINS

*Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь*

Egorov A. V.

Lazarenko A. M. – Senior Lecturer

Nowadays the world economy is extremely unstable. Crisis of the existing money system, high inflation and so on. All these difficulties in creating a stable economy have caused the appearance of a new independent alternative currency — bitcoin.

Bitcoin is an online payment system invented by group of people who were hiding behind a nickname: Satoshi Nakamoto, they published their invention in 2008, and released it as open-source software in 2009. The system is peer-to-peer; users can transact directly without needing an intermediary. Transactions are verified by network nodes and recorded in a public distributed ledger called the block chain. The ledger uses its own unit of account, also called bitcoin. The system works without a central repository or single administrator, which has led the US Treasury to categorize it as a decentralized virtual currency. Bitcoin is often called the first cryptocurrency. Bitcoin is more correctly described as the first decentralized digital currency. It is the largest of its kind in terms of total market value.

Bitcoins are created as a reward for payment processing work in which users offer their computing power to verify and record payments into the public ledger. This activity is called mining and is rewarded by transaction fees and newly created bitcoins. One of the features — is issue of new bitcoins. It is limited in volume and time and partly randomly distributed among those who want to use the computing power of their equipment to protect the payment system by proof-of-work from the respending. Maintenance activities of the system with the ability to receive compensation in the form issued by bitcoins and fees received the name of mining. Besides mining, bitcoins can be obtained in exchange for fiat money, products, and services. Hypothetically, there is a nonzero probability that the chain of blocks will be canceled and the system will be recognized as the main chain of the other blocks. The probability of such events dramatically decreases with increasing chain length. But if more than half of the control power throughout the computer network, such substitution is possible for any string that theoretically enables to realize double spending the same bitcoins. But in fact there is no possibility to concentrate this computing power in one hands, because in the entire network it is extremely high.

To generate a bitcoin, computers run specialized software. The basic element of the payment system is a client program with open source. With a network application layer protocol running on multiple computers clients are interconnected in an ad hoc network. Because of how complicated the math needed to generate a bitcoin is, BC-currency must be calculated with very powerful processors. These processors can be found in CPUs, graphics cards (GPU), or specialized machines called ASICs. People who use their computers to mine Bitcoin, are paid with a small percentage of the bitcoins they generate.

Bitcoin as a form of payment for products and services has grown, and merchants have an incentive to accept it because fees are lower than the 2–3% typically imposed by credit card processors. Despite a big increase in the number of merchants accepting bitcoin, the cryptocurrency doesn't have much momentum in retail transactions. Unlike credit cards, any fees are paid by the purchaser, not the vendor. The European Banking Authority and other sources have warned that bitcoin users are not protected by refund rights or chargebacks.

The use of bitcoin by criminals has attracted the attention of financial regulators, legislative bodies, law enforcement, and media. They listed money laundering, financing of illicit activities, theft, fraud, tax evasion, and use in black markets as possible. As of 2013, the criminal activities centered around theft and black markets. Officials in countries such as the United States also recognized that bitcoin can provide legitimate financial services to customers. But as bitcoins can't be traced, and the central banks of countries can't do anything with it, one of the largest owners of Bitcoin is the FBI. This organization has been able to focus in different ways on your wallet 174,000 Bitcoins. This is approximately equal to 3.15% of the total turnover of a cryptocurrency.

Thus Cryptocurrency Bitcoin is gaining popularity. And we can't ignore the advantages of using this currency. First of all, the transactions with Bitcoin are cheap: there are no intermediaries; banknotes can pass directly from one person to another with minimal expenditure of energy and time. Secondly, we do not host Bitcoin and dedicated server, it is completely decentralized. Thirdly, operations with BC-currency are made anonymously, being tied only to the abstract kriptoidentifikatoru (BC-address). This implies many practical benefits. Because of its low cost and free nature, Bitcoin is ideal for speculation and trade. It is impossible to tax. Nobody will be able to control what you spend your BC on: a book or a weapon. No one can impose your rules, and in case of failure to freeze or take your wallet as it happens periodically with Yandex.Money, PayPal, WebMoney and any other traditional payment systems. Summarizing everything we can see that Bitcoin is a perfect digital currency.

References:

1. Victor Fomin magazine. 2014 № 143. — pages: 82-87
2. Alex Fork — "Bitcoin: More than Money" — pages: 35-43