

Dmitry Bulgakov
V.I. Mieshkov, research supervisor
N.V. Poperechna, language adviser
SHEI “National Mining University”, Dniproperovsk

Problems of Using Digital Cryptocurrency Bitcoin

The problem of information security is being actively discussed worldwide. One of the questions in this topic is privacy protection in e-commerce. Currencies nowadays can not provide anonymity in financial transactions and there are no easy-accessible tools to change the situation.

The new wave of currencies, cryptocurrencies, is going to solve this problem. These currencies exist almost entirely in virtual realm and use cryptography to control their creation, administration and security. The most demanded cryptocurrency today is Bitcoin. In comparison with conventional currencies it has some fundamental differences. First of all, unlike hryvnia, Bitcoin is decentralized and there is no central bank to manage monetary policy. All functions such as Bitcoin issuance, transaction and verification are carried out jointly in P2P-network. It uses public key encryption for security. This means that when a new Bitcoin address is created, user's wallet software generates cryptographic key pair consisting of a public key and private key. After signing the transaction request with the private key of the address it is broadcast with public key to the network for verification. All transactions are conducted exclusively in a shared public transaction log known as “block chain”. This is done to confirm the party spending the Bitcoin really owns them, and prevent fraud and double-spending.

Total number of Bitcoins that will be issued is capped at 21 million. This limit protects its rate from devaluation. Nevertheless, each Bitcoin can be divided into Satoshis (1 BTC = 100,000,000 Satoshis). So this amount will be enough for everyone. And last but not least, Bitcoin as a decentralized currency is free from government interference and manipulation.

Despite the large number of Bitcoin advantages, it has some problems:

- Bitcoin does not have stable price making it difficult to access its real value and increasing the risk of losses for investors.
- BTC is a digital currency for paying online only.
- Electronic balances are not insured. In case of theft or loss of your digital wallet you will not have any ways to restore it. Currency balances, held at banks, on the other hand, are insured against certain events.
- Bitcoin is being prohibited in several countries now making it difficult to access there.
- The anonymity of Bitcoin makes it interesting for criminals.

Future of Bitcoin is still not clear because of a lot of problems and government prohibitions. To trust Bitcoin people need to find out if this system has a sufficient degree of security, and whether it can be used as money, i.e. whether it has the properties of money.