УДК 336.743

Rozum V., Truhanenko M., Lukashevich K.
Cryptocurrency

Belarusian National Technical University
Minsk, Belarus

In the year of 2017, the following words were popular - bitcoin, blockchain and others. After that, it was reported that the bitcoin exchange rate has fallen 6 times. In view of recent events, for a couple of months many people have been hearing about new records for the value of the so-called MMM heir. However, this is all fine, but what the above words mean will be difficult to understand, even if you spend enough time studying Wikipedia, so we decided to try and explain the work of the "bubble", but for this we need you to define some concepts.

To ensure that the idea of all the written above can be grasped, we will begin with such a term as *blockchain*. In essence, that is a chain of blocks with information, where each other block, in addition to its unique information, contains information about all previous blocks. This method of storing information well prevents from its changing. In other words, to change the information in one block, you need to rewrite all the previous blocks, and their number is practically unlimited. This is also a disadvantage, because it is impossible to change the information in the middle of the chain [1].

Also, it should be added that all bitcoin owners store blocks with information about all transactions ever made with this currency and are constantly adding new blocks to the end. That is, this same chain is the same for everyone and is stored completely. The next term to be introduced is *miners* are those people who always add new blocks with information about

transactions and previous blocks. As a reward for their calculations, the miner receives bitcoins. That is, literally, the first line of the new block, the miner writes – "deposit 12.5 bitcoins to my wallet". Bitcoins for the reward are taken from nowhere, that is, mining is also the only way to create new bitcoins.

Moreover, the reward for creating a new block is constantly decreasing, namely, one can mine a limited number of bitcoins (21 million), as of 2017, more than 15 million bitcoins have already been issued. A permanent reduction in remuneration exists as a measure of protection against depreciation. So, initially, the creation of a new block was rewarded with 50 bitcoins, after a couple of years - 25, and et cetera.

The problem with this reward is that an infinite number of people can participate in the creation of a new block, and only the one who encrypts the information about the previous blocks in the new block itself will receive the reward. The solution to this problem is *mining pools*, services that unite miners and distribute the reward among all participants, depending on their contribution to the writing of a new block.

There is also such a thing as the complexity of mining, it grows in direct proportion to the number of new miners involved in writing new blocks. This information is worth understanding – so what exactly do the miners do? We understood that according to the rules of the blockchain, each block, in addition to information about transactions made with bitcoin in its block, must contain encrypted information about all transactions in all previous blocks. So miners are engaged in encrypting this information into a hash sum. It is a set of numbers and symbols obtained by complex mathematical calculations which are called *hash functions.*

For this reason, as we said previously, the reward will be received only by the one who encrypted this information in the

most beautiful form (usually the criteria for the beauty of the hash amount are zeros in the beginning). That is, if today the number of miners increased 100 times, then the hash sum of the new block would be 100 times "more beautiful" than yesterday, that is what complexity is. It is noteworthy that this also works in the opposite direction, namely, if all but one person on earth stops mining, this does not mean that this poor guy will have to recalculate the hash amount for millions of years to achieve the necessary “beauty”, the complexity of mining will fall by as much as it is necessary for this person to calculate the hash amount.

Now, a little bit more about the equipment for bitcoin mining. Bitcoin is mined with the help of so – called *“asics”* - narrowly focused computers needed to perform a specific task, the power of asics is much higher than the power of any other equipment used for mining cryptocurrency. The main characteristic that reflects the efficiency of mining equipment is hash per second (h/s).

Now, as mentioned earlier, the complexity increases in direct proportion to the number of mining operations, but now it can be formulated more exactly – the complexity increases in direct proportion to the total capacity of the new equipment. In the case of bitcoin, the appearance of “asics” greatly increased the complexity and yesterday's equipment was ineffective, and the purchase of expensive “asics” was not affordable for cryptocurrency enthusiasts. In this regard, I would like to touch upon the topic of other cryptocurrencies.

The most popular cryptocurrency after bitcoin is Ethereum (ether / ethereum, $ 1,913.10 as of 02.22.2021 [2]) precisely because of this cryptocurrency, people with any knowledge of computers hate miners.

A feature of this and other so-called altcoins (altcoin is an alternative coin (everything that is not bitcoin)) is that expensive ASICs are not used for its production, since the

algorithms for extracting ether allow it to be mined on ordinary computer video cards. This fact is the reason for the hatred of ordinary people towards miners. If it suddenly occurs to you to assemble / buy a ready-made computer capable of running something more demanding than a sapper, you will have enormous difficulties.

Ordinary people around the world bought up almost all existing video cards, which led not only to a shortage of these very video cards, but to another reason for the shortage of semiconductors in the world as a whole. Let me remind you that semiconductors are used in absolutely all digital products - smartphones, televisions, even cars. Therefore, in the digital field, the opinion about miners is not the best.

Another feature of the ether architecture is the presence of a dag file loaded directly into the memory of the video card, the dag file is essentially a data block, more than 1 GB in size, used to find a block solution in the blockchain network based on the Dagger Hashimoto algorithm (ether mining algorithm). The size of the DAG file increases by 8MB over time. This happens every 30,000 blocks (which is equivalent to 10.4 days) and is called a change of epochs. Because of this feature, 2 GB video cards stopped working on the Ethereum network in November-December 2016. Video cards with 3 GB memory completed their journey in ether mining at the end of 2018, and just a month ago, video cards with 4 GB were not suitable for mining.

References:

1. Большинство криптовалютных инвесторов не хочет продавать Биткоин по текущей цене. Что это значит? [Электронный ресурс]. Mode of access: https://2bitcoins.ru. - Date of access: 02.02.2021.