CRYPTOCURRENCIES

A VIRTUAL GOLD

Cryptocurrency **is a term not coincidentally made up of two elements: the prefix *crypto-* and the noun *currency.* Przemysław Kudłacik, PhD Eng. from the Institute of Computer Science of the University of Silesia explains that cryptocurrency is basically a means of settlement. However, it is not stored in the computer system of any bank, but rather maintained by thousands of computers scattered around the world. It is built on a technology called blockchain.**

A REVOLUTIONARY METHOD

Before there were cryptocurrencies, there was public key cryptography, or two-key cryptography. What is it? We are used to the principle that if something is encrypted, you need a password to decrypt it. But what's the use of encrypting something if we then have to somehow communicate the password to the person who wants to read the message? This is why asymmetric cryptography was invented: unlike symmetric cryptography, it is based on two passwords. The method was revolutionary because it allowed something to be encrypted with one password and decrypted with another. This solution is widely used today, e.g. in electronic banking, electronic signatures, the military, and cybersecurity. Cryptography is also the basis of cryptocurrency technology.

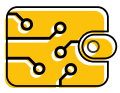
FREEDOM, ANONYMITY AND DECENTRALISATION

In 1982, American scientist and cryptographer David Chaum proposed using public key cryptography to create virtual, anonymously operated cash. That was a significant development because the basic carrier of IT media in operation at the time was magnetic tape, which provided more open access to online payments. His vision of digital currency included a fully anonymous system based on technology that did not quite resemble today's blockchain. Chaum's ideas became the foundations of the so-called cypherpunk movement born in 1992. People associated with this movement stood for total privacy, anonymity, and security through the use of cryptography.

In a way, it was a return to traditional currencies such as gold or silver. Before

Photo: panoramaphotos — Freepik.com

> Can something that does not physically exist have value?



the digital age, there was the bank note, which was a proof of ownership of gold or silver (the US dollar used to be backed by gold). David Chaum proposed to turn this bank note into digital currency, to which only those with a private key would have rights.

HOW ARE CRYPTOCURRENCIES CREATED?

Can something that does not physically exist have value? Gold and silver have value because not only do they physically exist, but it takes a specific amount of money, energy, resources, and human labour to produce them. In addition, there is a limited supply of these natural resources on Earth and it is impossible to mine more gold or silver than there is in nature. And how do you 'mine' cryptocurrencies?

Since the beginning of digital banking, people have been wondering how to secure databases, as hackers are constantly trying to break in. Often times, they also infect thousands of computers to simultaneously connect to a particular bank and put a strain on its servers that cannot handle such an onslaught of requests. These attacks are known as DDoS (Distributed Denial of Service) attacks. A way to protect against DDoS attacks was invented in the 1990s. The idea was born when working on countering email spam. Cynthia Dwork and Moni Naor proposed running a cryptographic task that would take up some of the computer's computing power. This puzzle of sorts involved having the computer solve a cryptographic task based on the content of the email before sending it. The result of the task, i.e. a specific number, was attached to the body of the email.

This solution was also used to implement the 'mining' of cryptocurrencies, and the process was called Proof of Work. The commitment of computer processing power is crucial. As mentioned earlier, in order for gold or silver to be acquired, expert knowledge, energy, or hardware must be involved. However, the same things are needed for cryptocurrencies to be created, only they are created in a digital form. In order to make it worthwhile for virtual 'miners' to support this distributed computing system, a competition has been introduced in which computers search for some special, rather complex number. The task is not easy and is dependent on the available computing power of the computer. The computer that finds the right number the fastest wins the right to add a new block to the chain and receives a reward in cryptocurrency, and so the race begins again. In bitcoin, it was assumed from the very beginning that a new page (new block) containing customer transactions in the database, or blockchain, would be added on average every 10 minutes. This has not changed to this day. An additional incentive for mining is earning commissions on approved transactions — you can get paid for mining cryptocurrency and for validating transactions.

SATOSHI NAKAMOTO

This is the nickname of the person (or group of people) who created bitcoin, the first cryptocurrency. It was they who came up with the idea of using the cryptographic puzzle process to create virtual gold. They announced it on 31 October 2008 in the manifesto entitled *Bitcoin: A Peer-to-Peer Electronic Cash System*.

On 3 January 2009, 30,000 lines of code were written in what is considered the beginning of the bitcoin network. From the start, it was assumed that there would be 21 million bitcoins (BTCs). Each BTC is divided into 100 million parts, known as satoshi, i.e. bitcoin 'pennies'. No one can add bitcoins to the system; the programme limits that the last BTC will be mined in about 100 years. It is worth mentioning that most bitcoins (around 19 million) have already been mined. Therefore, every four years the reward for the 'miners' is reduced by half, which is known as halving. On 5 October 2009, Satoshi Nakamoto 'mined' the first block and generated 50 BTC. After four years, the reward was already 25 bitcoins. Currently, it is equal to 6.25 BTC.

PROS AND CONS

The biggest advantages of cryptocurrencies certainly include the transparency of the system, decentralisation, and robust security. However, it has been noted that the competitive model can lead to huge energy consumption. Anonymity is also highly controversial. The lack of transparent information about users opens up opportunities for criminal activity.

Agnieszka Sikora, PhD

Przemysław Kudłacik, PhD Eng.
Institute of Computer Science
Faculty of Science and Technology
University of Silesia
przemyslaw.kudlacik@us.edu.pl