УДК 004.42

P. Rąb, student (Lublin Catholic University, Poland);
P.P. Urbanovich, prof. (BSTU, Minsk, Belarus)

# METHODS, SOFTWARE AND HARDWARE TOOLS FOR CRYPTOCURRENCY TECHNOLOGIES

Cryptocurrency has been created and is managed by computer software and does not exist physically in any way. In other words, it is a currency used within software and created thanks to software as opposed to a specific physical currency [1].

The cryptocurrency market is growing stronger every year.

Bitcoin is one of the oldest and most popular cryptocurrencies. There is no owner or central control, here – all users are equal, in contrast to, for example, the general banking system, where there is a client-manager relationship. The source currency code is open and available to everyone.

Bitcoin is the first use of blockchain technology. The network is based on the digital record of transactions in the form of blocks of data, thus creating an identical database of transactions is distributed on many computers. Each computer that is a node in a peer-to-peer network (also referred to as P2P – can act as a client and server), has a copy of the collective transaction book in digital form. The verification consists in checking the value of the result with the value of input data by all network nodes and does not require as many resources as finding a solution that approves a given block containing transactions and attaches them to the block chain (fig. 1 [2]).

The idea behind the security of a distributed blockchain register is rewards in the form of cryptocurrencies for transaction authentication. The authentication process is also the process of assigning a new cryptocurrency to the owner and is called mining.

There are two types of algorithms for extracting cryptocurrencies: *Proof of Work* and *Proof of Stake*.

To present and analyze the basic methods of functioning of the most popular cryptocurrencies, based on blockchain technology, a web-application was created.

The site uses the most popular pattern for creating websites such as Model-View-Controller. The application consists of many functionalities such as: briefcase creation, adding new transactions, adding new network nodes and thus simulating the P2P network operation on which the Bitcoin cryptocurrency is based. To generate a wallet, we need a public and a private cryptographic keys [3-4].

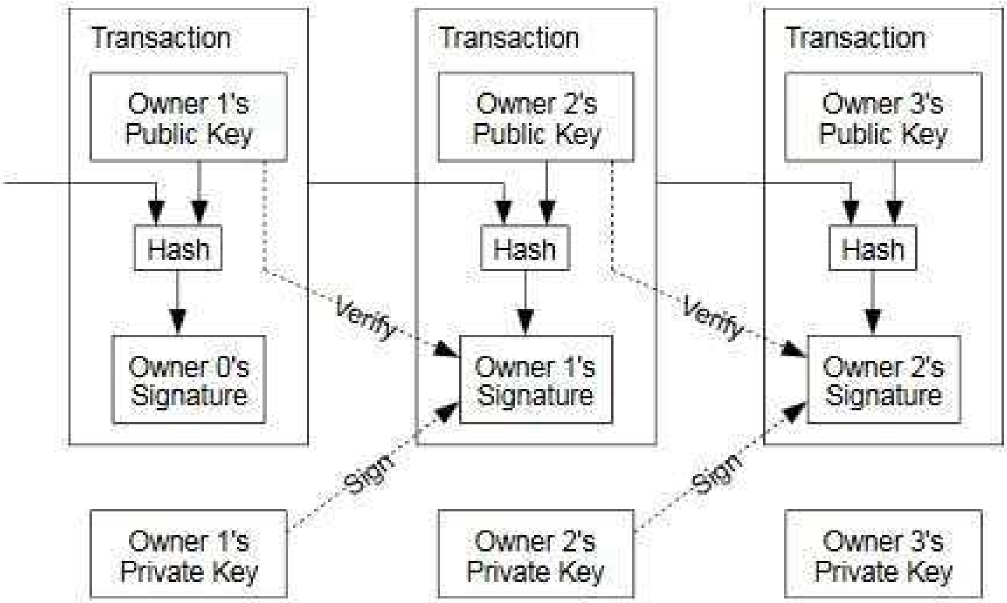
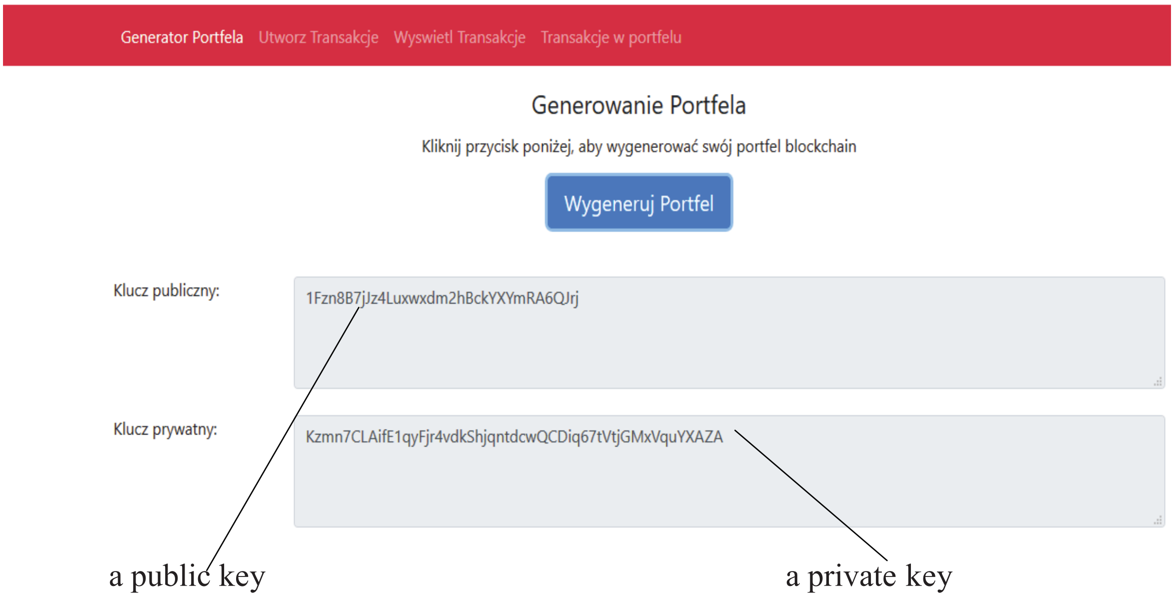


**Fig.1 The blockchain technology implementation scheme [2]**

When someone wants to send any cryptocurrency, they need a public key of the recipient, and more specifically a public address. Everyone can share it freely, because the only function that it fulfills is the ability to send funds from another wallet to it.



Generowanie Portfela

Kliknij przycisk poniżej, aby wygenerować swój portfel blockchain

Klucz publiczny: 1Fzn8B7jJz4Luxwxdm2hBckYXYmRA6QJrj

Klucz prywatny: Kzmn7CLAifE1qyFjr4vdkShjqntdcwQCDiq67tVtjGMxVquYXAZA

a public key

a private key

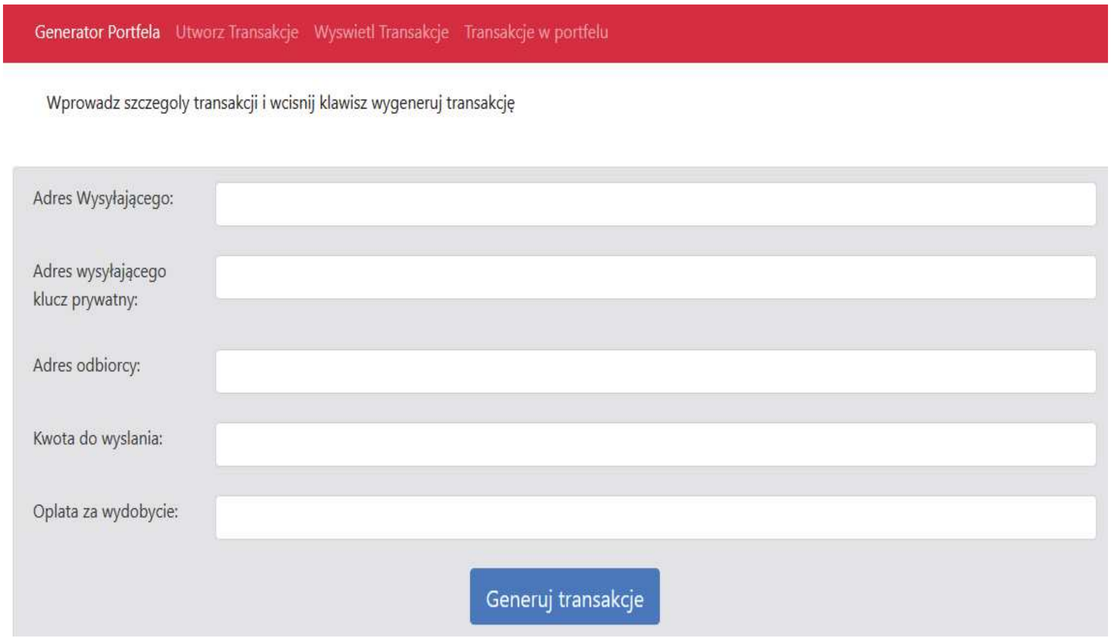
**Fig.2 The screenshot of «The Briefcase Generation»**

The private key, in addition to being our password, also serves to sign each transaction. Assuming that such a key should not be shared with anyone, the entire blockchain network is sure that the funds have been sent by the owner of a given wallet. Figure 2 shows the appearance of the wallet page view.

A RSA algorithm was used to generate a pair of keys [3]. Another functionality is creating transactions that are saved in a blockchain. If the user wants to send to another person, some amount must have the recipient's public key. In the transaction, he must also provide his own public and private key.

Fig. 3 presents the appearance of the page for creating transaction

The last important functionality is the ability to trace the entire register of all transactions that have been recorded in the entire network.



Wprowadz szczegoly transakcji i wcisnij klawisz wygeneruj transakcję

**Fig.3 The screenshot of «The transaction Generation»**

This register consists of the following information: recipient's address, sender's address, amount, transaction date, and block number.

## REFERENCES

1. [Electronic resource]: https://pl.dailyforex.com/forex-articles/ 2017/ 12/. – Access date: 20.02.2019.

2. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system/ S. Nakamoto. – [Electronic resource]: https://bitcoin.org/bitcoin.pdf. – Access date: 20.02.2019.

3. Urbanovich, P. P. Zashchita informatsii metodami kriptografii, steganografii i obfuskatsii/ P.P. Urbanovich: ucheb.-metod. posobiye dlya stud. – Minsk: BGTU, 2016. – 220 s.

4. Ochrona informacji w sieciach komputerowych / pod red. prof. P. Urbanowicza. – Lublin: KUL, 2004. – 150 s.