ELECTRONIC PAYMENT SYSTEM AND BLOCKCHAIN AS ITS VITAL PART

Agzamova (Nuriddinova) Mokhinabonu Shahobiddin qiz,
Trainee teacher, Tashkent University of Information Technologies named after Muhammad al-Khwarizmi, Tashkent, 100200, Amir Temur street, 108, Uzbekistan, Tashkent

Key words: block chain, payment, electronic commerce, network, bitcoin, security, openness, information

Abstract

The proposed review article provides information on modern electronic payment systems, especially focusing on how the mechanism of bitcoin works, blockchain technology, also describes the scope of blockchain's application.

Introduction

During the last several decades electronic payment systems have reached a new stage of development providing people with the necessary infrastructure to facilitate payments. Today, due to the rapid growth of electronic commerce, EPS have become an integral part of trade and entrepreneurship[1].

The widespread virtual currency offers users a high level of anonymity, which is simply not possible in the case of credit and debit cards or traditional online payment systems.

Initially, the digital currency began to be used to purchase and sell virtual goods in various online communities: social networks, virtual worlds or online games. But to date, it is quite a profitable business, generating real income in the form of fiat currency.The range of blockchain technology applications is expanding, the so-called publicly available book of accounting, which is the basis for one of the types of EPS – cryptocurrency has become a topic of our actual work[2].

Electronic payment systems

Once Bill Gates in his book "The Road to the Future" predicted that in the near future money will cease to exist in a physical representation and will only be in circulation in the electronic form. The electronic equivalent of money, existing only in the form of information stored on a physical medium, has a number of advantages:

- the mechanism of payments is simplified (you can pay for the goods from any place);
- the procedure for repayment of debt is simplified;

- the difficulties with conversion from national currencies at bank rates disappear;
- the problems related to money transportation disappear, including through state borders;
- the safety of money is ensured.

The development of electronic payment systems will greatly simplify mutual settlements through the Internet.

Electronic payment systems (hereinafter - EPS) are organizations that issue digital currency, create and implement new methods for their distribution and provide all conditions for electronic financial transactions.[3] Any electronic payment system issues its own electronic finance corresponding to paper currency. Various EPS differ in levels of development, degrees of functionality, coverage, and intended purpose. Some are used around the world, some in only a few countries, and others do not leave the borders of their state at all.

Due to the advent and growth in the usage of EPS in the world, the concepts associated with this process begin to appear. One of these concepts, which was mentioned earlier, is electronic money.[4]

Electronic money, or otherwise digital currency, refers to the system of storing and transferring both traditional currencies and non-state private currencies. The circulation of electronic money can be carried out both according to the rules established or agreed with the state central banks and according to the own rules of non-state payment systems.[5]

A common misbelief is the identification of electronic money with no-cash money.

Typically, the circulation of electronic money occurs through computer networks, the Internet, payment cards, electronic wallets and devices that work with payment cards together with other financial instruments as bracelets, key chains, mobile phones and etc.[6]

There is a variety of electronic money classifications, but here we consider a few based on:

- smartcards;
- network.

Smart cards are linked directly to bank accounts and represent a certain amount of money that the card user manages. Such systems allow you to pay for Internet purchases, store money in several currencies and can be managed by telephone communication.

For an electronic system based on networks, you need to install a specific program. Such programs are free and with the development of the capabilities of mobile devices, mobile applications of such systems are also created. In general,

EPS based on networks are chosen by users dealing with earnings on the Internet, purchasing goods through online stores or by firms that wish to expand the forms of making payments for their services.

Bitcoin

An example of a completely independent cryptocurrency is bitcoin and most of other cryptocurrencies are based on the bitcoin, so we will consider it in detail.

In 2008, October 31, Satoshi Nakamoto published a paper “the Bitcoin: Peer-To-Peer Electronic Cash System”, which described bitcoin as a fully decentralized e-cash system that does not require a third-party trust. As a result, bitcoin was launched in 2009 and became the first decentralized convertible currency and the first cryptocurrency. Thus, bitcoin is such an electronic peering payment system that uses the same units for payments.[7]

There are bitcoins only in the form of records in the database (DB), where all transactions with the bitcoin addresses of sender / recipients are stored unencrypted, but without mentioning the information about the real owner of these addresses. In the database there are no separate records about the current number of bitcoins from any owner, that is, the addressee may have unidentified amoun of bitcoins. Only on the basis of transaction chains, the current number of bitcoins associated with a particular bitcoin-address becomes understandable. Calculations of how many virtual currencies are listed for the owner, automatically are made by client programs.

In cryptocurrencies, public and private keys are used to transfer currency from one person to another, and a cryptographic signature is required each time to complete a transfer.

It is known that each user of the system can generate an unlimited number of pairs. The size of the private key is 256 bits, and the corresponding public key is 512 bits.

The keys are needed to create a bitcoin address and confirm the legitimacy of the transaction formation, they can also be used for a digital signature or encryption in the correspondence..

The addresses are anonymous and are in form of a sequence of bytes obtained as a result of the conversion of the open key consisting of a text about 34 characters in length, using numbers and letters of the Latin alphabet. Bitcoin addresses can be represented in the form of QR-codes, as well as in the form of other two-dimensional bar codes, which are read by mobile devices.[8]

Bitcoins can be transferred to anyone who reports the correct bitcoin address or public key. The minimum transferred value of 10 - 8 bitcoins was called "Satoshi" (in honor of the creator Satoshi Nakamoto).

Transactions support an arbitrary number of "inputs" (links to previous transactions) and "outputs" (instructions for recipients). The values from all the "inputs" are summed, and the sum is distributed over the "outputs".

As shown in Figure 1, the operation of transactions looks like this:

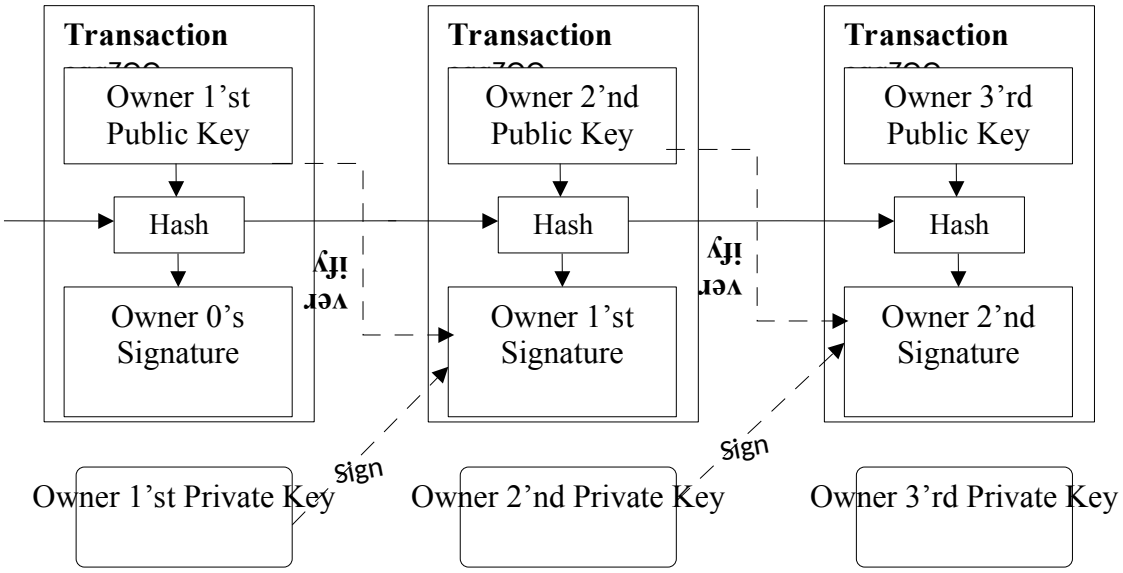

Figure 1. The operation of transactions

Blokchain

Blockchain is a chain of transaction blocks, which is built according to certain rules. A transaction block is a special structure for recording a group of transactions in the Bitcoin system and similar ones.[9]

Blockchain is, as it is not hard to guess from the title, a chain of data blocks, where each block is associated with the previous one. The block contains a set of records. And new blocks are always added strictly to the end of the chain.

This chain is built on three principles:

- distribution;
- openness;
- security.

All users of the block system form a network of computers, each of them contains a copy of the blockchain data. Usually this is a complete copy of all the blocks, but in principle you can store only the data you need on a particular computer.

All the blockchain data, blocks and their contents, are always open for everyone. The user can easily read any block and see all the records in this block, also look at the chain and track the change of information. Thus, all data in the blockchain are easily verifiable, which means that you do not need to trust other

network members, because you can always check them and get a guaranteed reliable answer.[10]

Owing to Encryption, users simultaneously receive openness and authenticity with a complete distrust to the other participants and, possibly, even their malicious intent.

A block in the blockchain consists of a header and a list of transactions. The master data is stored in the header, which includes its hash, hash of the previous block, as well as transaction hashes and additional overhead information.

Conclusion

So, the transfer of bitcoins reduces itself to specifying the conditions that are formed using public keys to further disposal of them. Having no intermediaries in its operations, it does not only reduces the likelihood of hacking, but also makes corruption impossible.

Probably, this idea sounds utopian, but nevertheless, the blockchain technology is developing quite rapidly, so it is possible to assume that blockchain will become one of the important components of not only the economy but other spheres of activity, including even politics, such as unforgeable election results.

References

1. Williamson, S., 2018. How Blockchain Technology Is Transforming Traditional Payment Methods. [Online]. Available through: < https://www.nasdaq.com/article/how-blockchaintechnology-is-transforming-traditional-payment-methods-cm1012647 >. Accessed on: [12th Jan’2019].

2. Zwanenburg, 2018. Invest in Blockchain. Available through :. Accessed on: [10th Jan’2019]. Faden, M., 2017. Coming in 2017: Live Blockchain Deployments promise to accelerate Payment processing services and Trade Finance. Available through: . Accessed on: [11th Jan’2019].

3. Medici, 2018. Blockchain –Overview, Tech, Application Areas and Use cases. Available through:. Accessed on: [15th Jan’2019].

4. Canellis, D., 2018. Deutsche Bank, HSBC, and IBM are testing Blockchain-powered bank transfers. Available through: https://thenextweb.com/hardfork/2018/07/03/blockchain-bank-ibm/ Accessed on: [12th Dec’2018].

5. Mulle, M., 2017. CIO Insights Reflections: Cryptocurrencies and Blockchain-their importance in feature. Available through: : downloads/newsdocs/ cio_insights_reflections_-_cryptocurrencies_and_blockchains_- _emea_- _client_ready.pdf> Accessed on: [8th Jan’2019].

6. Nikhilesh, D., 2017. Deutsche Bank: Blockchain opportunities are huge. Available through:https://www.coindesk.com/ford-lg-to-pilot-ibm-blockchain-in-fight-against-childlabor Accessed on: [14th Jan’2018].

7. Detrixhe, J., 2018. Big tech companies prefer the Federal Reserve over Blockchain. Available through :< https://qz.com/1499400/tech-giants-like-google-and-paypal-look-to-the-federalreserve-for-faster-payments/>. Accessed on: [16th Jan’2019].

8. Ebrahimi, A., 2018. The Complete Guide to Credit Card Processing Rates & Fees. [Online]. Available through: < https://www.merchantmaverick.com/the-complete-guide-to-credit-cardprocessing-rates>. Accessed on: [16th Jan’2019].

9. Mathieu, 2018. GRAFT is providing an alternative to Credit Card Networks via Real-time Authorizations and Service Provider Ecosystem on a Private Blockchain. [Online]. Available through :< https://ethereumworldnews.com/graft-is-providing-an-alternative-to-credit-cardnetworks-via-real-time-authorizations-and-service-provider-eco-system-on-a-privateblockchain/>. Accessed on: [12th Jan’2019].

10. Mintdice report, 2018. Mastercard vs. Visa blockchain projects. [Online]. Available through :< https://www.mintdice.com/blog/Mastercard-vs-visa-blockchain-projects>. Accessed on: [10th Jan’2019].