Conference Paper

Electronic Payment Systems and Blockchain as a Constituent Part

Lukina E. E. and Dolgachev M. V.

Pacific State University. Faculty of Computer and Fundamental Sciences. Tihookeanskaya St,, 136, Khabarovsk; Russia

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.

Corresponding Author:
Dolgachev M. V.
007428@pnu.edu.ru

Received: 11 December 2017
Accepted: 20 January 2018
Published: 13 February 2018

Publishing services provided by Knowledge E

Selection and Peer-review under the responsibility of the FinTech and RegTech: Possibilities, Threats and Risks of Financial Technologies Conference Committee.

1. Introduction

Every year electronic payment systems reach a new stage of development. The issue of payment through open networks has become important due to the rapid growth of electronic commerce in the last decade. Electronic payment systems should provide people with the necessary infrastructure to facilitate payments. Today EPS have become an integral part of trade and entrepreneurship.

In a world full of Internet technologies and new inventions the popularity of virtual or digital currency has been increasing for the last few years. It should be noted that these expressions are used as a synonym. This interpretation is followed by the European Central Bank, and the Financial Crimes Enforcement Network (FinCEN) and the FBI in their official documents use the term "virtual currency" as a common and the only one, so we will continue to treat these concepts as synonymous.

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.

There are also more and more options for improving the principles of the operation of EPS. 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.

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. Frequently, EPS are a part of large Internet companies, being an element of their business activity (for example, a currency of social networks, the Yandex.Money system, etc.).

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.

Different electronic payment systems issue their own types of currency. 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.

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.

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. Other payment instruments are also used: bracelets, key chains, mobile phones and other devices equipped with a special payment chip.

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

- smart cards;
- 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 you can use telephone communication to manage this system.

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.

As shown in Table 1, the types of electronic payment systems may be considered.

There is another concept such as cryptocurrencies or decentralized virtual currencies. The work of these systems is carried out using a distributed open-source computer network that does not have a central administrator, and there is no centralized control or supervision, and cryptographic methods are used as protection.

3. 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.

Table 1: Types of EPS.

Network-based		Based on smart cards
Fiat	Non-Fiat	Fiat
PayPal	EasyPay	Visa Cash
African payment system M-Pesa	QIWI	Mondex
	Yandex money	Hong Kong card system "Octopus"
	RBK Money	Dutch system Chipknip
	Cryptocurrency	

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.

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. Also in the database there are no separate records about the current number of bitcoins from any owner, that is, it is not known how many bitcoins the given addressee has. 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 transfer a cryptocurrency.

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 transactions formation, they can also be used for a digital signature or encryption in the correspondence.

Creating a new key pair is autonomous and does not require a connection to the network or the Internet. The key store is the wallet.dat file located on the computer.

The user comes up with a password only to access information from the file "wallet.dat", that is, to access his key pairs. In most cases, it will be sufficient to somehow obtain a private key, therefore, for the disposal of bitcoins, the presence of this file is not mandatory.

The addresses are anonymous and do not contain information about their owner. The bitcoin address is 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. The user of Bitcoin can create several addresses on his own initiative.

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:

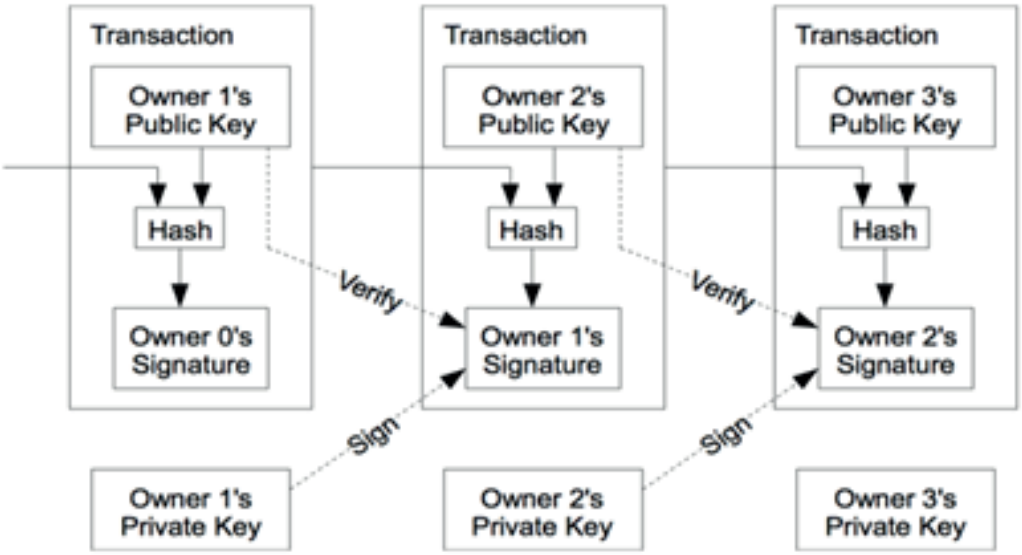

Figure 1: The principle of transactions.

4. 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.

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.

Encryption is widely used to protect data and users in the blockchain system. Thanks to this, 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.

5. Conclusion

So, the transfer of bitcoins reduces itself to specifying the conditions that are formed using public keys to further disposal of them. To perform the next operation with the received bitcoins, a corresponding electronic signature using secret keys will be required, this will be the fulfillment of the conditions. The network checks the signatures with a pair of public keys. As a result, only the owner of the secret key can manage the bitcoins. The most classic condition is to specify a bitcoin address.

The creation process of a decentralized free currency is referred to as mining, it is based on a cryptographic algorithm that converts data into a bit string.

Thus, bitcoin is an intangible virtual currency, which is used as a kind of payment system. This money is not fiatic, but they can be used as an actual payment for purchases in online stores. The transfer of bitcoins from the owner to the owner is the transfer of encrypted data.

Also it is important that bitcoin is based on blockchain, this technology provides a large field for the implementation of new ideas in new areas. For example, cybersecurity, despite the fact that the main register of blockchain is public, data transmission is checked and carried out using advanced cryptographic methods. This ensures that the data came from the right sources and was not intercepted in the interim period. And the more common the blockchain becomes, the lower the probability of hacking. One of the ways in which the system becomes more secure is that there are no intermediaries in its operations. This 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 quite 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] M.M. Pryanikov, A.V. Chugunov. Blokchain as a communication basis for the formation of the digital economy: advantages and problems / M.M. Pryanikov, A.V. Chugunov // International Journal of Open Information Technologies ISSN: 2307-8162. - 2017, vol. 5, No. 6. - pp. 49-54. (Date of publication June 2017, circulation date October 9, 2017)

[2] Blockchain and bitcoin in Russia. Not only bitcoins: 20 spheres in which you can also use blockchain: [Electronic resource]. Access mode: https://cryptorussia.ru/zametki/ne-tolko-bitkoiny-20-sfer-v-kotoryh-tozhe-mozhno-ispolzovat-blockchain (Publication Date August 19, 2017, circulation date 02.11.2017)

[3] Wikipedia. Bitcoin. Cryptocurrency. Blockchain. Virtual currency. Digital currency: [Electronic resource]. Access mode: https://ru.wikipedia.org/wiki/ (Date of circulation 04/23/2017)

[4] Studopedia. Electronic payment systems "[Electronic resource]. Access mode: https://studopedia.ru/9_76344_elektronnie-platezhnie-sistemi.html (Publication Date May 13, 2015, circulation date 03.11.2017)

[5] WordPress Tutorial. Electronic payment systems: [Electronic resource]. Access mode: https://wordpress-book.ru/zarabotok/elektronnye-platezhnye-sistemy/ (Publication date 11.08.2014, circulation date 28.10.2017).

[6] Electronic payment systems: [Electronic resource]. Access mode: http://web-klik.ru/elektronnye-platyozhnye-sistemy/ (Date of publication 07/07/2016, circulation date 02.11.2017)

[7] Rusbase. How will blockchain change our life?: [Electronic resource]. Access mode: https://rb.ru/opinion/blockchain/ (Date of publication 06/04/2016, circulation date 10.05.2017)