BLOCKCHAIN AS THE BASIS OF THE DIGITAL ECONOMY. WORLD EXPERIENCE OF CRYPTOCURRENCY FINANCIAL REGULATION

Alexander SHMATKO[a*], *Alla GAVRILOVA* [a]

[a]*Simon Kuznets Kharkiv National University of Economics, Economic Informatics Faculty, Cybersecurity and Information Systems Department, UKRAINE*

[*] *Correponding Author: asu.spios@gmail.com*

ABSTRACT

The article discusses the international experience of cryptocurrency regulation on the example of such countries as the United Kingdom, the United States of America, Canada, Australia, Estonia, Ukraine, Japan, China, Latin American countries. If we consider the world map, which shows the status of cryptocurrency, then we can mark the countries that have been waiting. These countries include Venezuela, the USA, Canada, Australia, a part of the European Union, and such giants of technological innovations as China and Japan. A number of countries of the European Union, led by Germany, Latin American countries are in a neutral position, due to the lack of developed legislation aimed at regulating cryptocurrency relations. Cryptocurrencies in Ecuador, India, Nepal, Thailand, Vietnam and Bangladesh banned. The conclusion about the expediency of legal regulation of new phenomena, including internationally.

Keywords: Bitcoin, cryptocurrency, blockchain, fintech, IT, debt market, Ethereum.

1. INTRODUCTION

1.1 Fundamental Principles

The development of blockchain technology begins with the advent of bitcoins (Bitcoin) in 2008. The author's Bitcoin: A Peer-to-Peer Electronic Cash System under the pseudonym Satoshi Nakamoto [1] described how to build a peer-to-peer payment system with the ability to make electronic transactions without intermediaries - financial institutions. The work described a method for solving this problem using a digital signature. But, at the same time there was the problem of a trustee who controls the double spending. It is proposed to use a decentralized solution based on a peering system, cryptography, mathematical rules, such as, proof of work (Proof-of-Work) and general rules for conducting transactions between system participants. This decision called the bitcoin blockchain.

The paper proposes a system of electronic transactions, not based on trust. The construction of the scheme began with the traditional presentation of coins based on digital signatures, providing control of possession, but allowing double waste.

This problem solved by using a peer-to-peer network and a "proof of work" scheme to record the public transaction history.

When using this solution, an attacker who does not have most of the network resources will not be able to change the records of transactions that have occurred.

The advantage of such a network is the simplicity of its structure [1]. All network nodes constantly exchange information. There is no need for identification, since messages do not follow a particular route, information is transmitted on the basis of the principle of "least cost".

In the future, the blockchain identified as a separate technology that can be used in addition to cryptocurrency. This technology called "Distributed Registry Technologies" (Distributed ledger technology - DLT).

2. METHOD

Blockchain is a multifunctional and multi-level information technology designed to reliably account for various assets. Technology securely distributed storage of records of all ever committed transactions. Blockchain is a chain of data blocks, the volume of which is constantly growing as new blocks with records of the most recent transactions are added. This is a chronological database. Data is represented by a sequence of records that can be supplemented. Records along with supporting information are stored in blocks. Blocks are stored as a single-linked list. Each participant is represented by a node, which stores the entire current data array and contacts with other nodes. Nodes can add new entries to the end of the list, and also inform each other about changes to the list.

Consider the mechanisms and characteristics that support this activity.

The basic model of data distribution in a system built on the blockchain can be represented by a set of actions:

1. A new transaction is sent to all network nodes, the network is built on the principle of a peer-to-peer network, the transaction enters the raw data pool on these nodes.
2. Specialized machines by miners, add transactions located in the raw data pool to the block.
3. Each miner tries to pick up a hash of the block that meets the network rules (in the Bitcoin blockchain there is a certain number of zeros at the beginning of the block hash). This operation is called proof-of-work. There is another way to confirm the right to perform a block-making operation - a method of confirming a stake (proof-of-stake).
4. As soon as the miner receives a satisfying hash of the block, the data block is sent to all network participants, and the miner himself receives a reward for adding the block.
5. The nodes that have received this block check for the correctness of transactions and the absence of so-called double spending. If the block fails validation, it is discarded.
6. If agreement is reached on the correctness of the block, the miners start working on a new data block based on the hash of the newly added block [1].

All transactions are carried out with a cryptographic confirmation.

When registering on the network, each network participant receives two cryptographic keys: a private one - for encrypting a transaction, and a public one - for verifying a transaction.

When sending a transaction to the recipient, the sender signs the hash of the previous transaction and the recipient's public key and adds this information to the end of the transaction. The recipient can verify the entire transaction chain by checking all the signatures of the previous participants in the transactions [1].

The hash in this scheme is a data array transformed by a hash function. The transformation results in a unique alphanumeric string that cannot be converted in the opposite direction. The combination of using public and private keys with hashing gives the blockchain technology a high level of data security.

Each subsequent data block is based on the hash of the previous block. If one of the miners tries to add a block that does not comply with this rule, then such a block is automatically rejected by other members of the blockchain network. In order for the miner to add a non-valid block, it is necessary to change the hash of all previous blocks, up to the so-called "genesis block" - the first block in the system. This block is usually specified by system developers. From this, one of the essential properties of the distributed registry technology arises - the information that has entered the block chain cannot be changed after the fact.

It must be said that the addition of new blocks by miners occurs according to certain principles.

These principles were introduced into the system to increase the security of the blockchain and at the same time ensure the decentralization of the system.

At the moment there are two basic principles of adding a new block to the block chain - this is proof of the work done (Proof-of-work, or PoW) and confirmation of a share (Proof-of-stake or PoS).

Due to the fact that the security of the blockchain does not rely on a single certification authority, such as a bank, with its security infrastructure, each of the nodes of this system does not know a priori which version of the database is valid.

In the Bitcoin blockchain, network security relies on the Proof of Operation (PoW) algorithm in the mining process of blocks. Each node that wants to participate in the mining process must solve a computationally complex task in order to guarantee the validity of the block. The award for the decision is automatically credited to the miner with new bitcoins.

If an attack occurs on the blockchain database, the attacker must accomplish the same task as the rest of the network, i.e. The attack will succeed only if the attacker can attract significant computational resources.

Network security is supported by the following resources:

- specialized equipment for carrying out calculations;
- electricity required for equipment operation.

The idea of the share confirmation algorithm (PoS) is as follows: instead of computing power, the likelihood of creating a new unit and receiving an appropriate reward is proportional to the user's share of ownership in the system.

The users with the largest shares in the system have the greatest interest in maintaining the security of the network, as they will suffer most if the reputation and cost of cryptocurrency falls as a result of attacks. To conduct a successful attack, the attacker must acquire most of the currency, and it will be prohibitively expensive if the system is quite popular [1].

The main characteristics of the distributed registry technology:

- decentralization;
- openness of the entered data;
- Mathematical-cryptographic protection of information;
- the inability to change once entered into the system data.

3. EXPERIMENTAL RESULTS

The growing demand for global socio-political and economic reforms has led to serious changes not only in the so-called social contract, but also in the international legal system as a whole.

Virtual currencies (cryptocurrency) have become one of the key tools on the way to these evolutionary changes.

Attempts of effective legal regulation of cryptocurrency vividly illustrate the problems faced by state structures around the world not only in creating the optimal legal platform for cryptocurrency business, but also in trying to identify and understand the phenomenon of decentralized systems in general.

In the case of individual states that are at the forefront of the global financial economy, the historical context vividly illustrates the complete inability of some of them to adequately and competently respond to innovations and increasing technological progress.

For example, Australia, striving to provide favorable conditions for the development of the cryptocurrency industry and create its own financial and technological centers, demonstrates its intention to become one of the most progressive jurisdictions and does not rule out the use of decentralized network of blockchains in various areas of government regulation). The possibility of using the blockchain is also considered by Australia Post Non-state projects related to digital money are also actively developing [2].

In 2013, the Reserve Bank of Australia identified the Bitcoin cryptocurrency as an alternative to currencies of different countries and the payment system [3].

The Australian Securities and Investment Commission does not consider digital currency (cryptocurrency) as a financial product. Cryptocurrency activity (mining), or the use of cryptocurrency as a means of payment or exchange are not subject to licensing [4].

Standards for conducting a cryptocurrency business are established and are binding for members of the Australian Digital Currency & Commerce Associaton [4]. This organization may impose penalties on them.

The UK is the leader of cryptocurrency integration and the most favorable jurisdiction for conducting a cryptocurrency business. The UK at the state level provides support to the cryptocurrency community and cryptocurrency-related startups. The Bank of England conducted research on the hypothetical risks for the monetary system from digital currencies from 2014. The conclusion is that the risks are so minimal that possible regulation of cryptocurrencies will prevent their criminal use and support innovation in this area has been made [5].

The position of the UK government in the legal regulation of cryptocurrency activities is not developed. Digital money activities are in a gray area.

The European Union has taken a different path in the legal regulation of cryptocurrency business. Member States of the European Union are traditionally considered favorable for conducting a cryptocurrency business.

None of the regulators of the European Union has adopted any special rules for the regulation of cryptocurrency activities.

In 2012, the European Central Bank (European Central Bank) published a report in which it stated that the traditional regulation of the financial sector is not applicable to bitcoins. Bitcoin itself in the document was defined as a convertible decentralized virtual currency [6].

In 2016, the European Commission announced plans to tighten reporting standards for cryptocurrency exchanges and companies that provide cryptocurrency wallets to users. In particular, the European Commission planned to require European cryptocurrency exchanges and cryptocurrency purse providers to carry out mandatory user identification [7].

In November 2015, the European Court of Justice issued a decision according to which bitcoin should be considered as a currency (means of payment), and not a commodity. At least in terms of taxation.

Thus, bitcoin buying and selling operations for traditional fiat currencies should not be subject to value added tax [8]. Prior to this, national regulators treated the taxation of a cryptocurrency in different ways.

The procedure for taxing a cryptocurrency and other taxes on it is regulated by the national legislation of member states, depending on the nature of the cryptocurrency operation. In this case, as a rule, for the purposes of taxation, digital currency is considered as an intangible asset or commodity, and not as currency or money.

In Norway, Finland and Germany, the cryptocurrency is subject to capital gains tax (Capital Gains Tax) and wealth tax (Wealth Tax). In Bulgaria, digital currency is considered as a financial instrument and is subject to appropriate taxes [9]. In Austria, the cryptocurrency is considered by the tax authorities as an intangible asset, and its mining as an operating activity. Therefore, the income received as a result of its alienation is subject to income tax (Income Tax).

In general, legal regulation of cryptocurrency and operations with it in the European Union is carried out within the framework of the policy of countering the legalization (laundering) of proceeds from crime and the financing of terrorism.

With regard to cryptocurrencies, the United States of America took the path of tax regulation in the field of cryptocurrency trading, forcing all American cryptocurrency exchanges to verify their clients. At the same time, the USA is one of the most convenient countries in the world for running a cryptocurrency business.

But the legal regulation of digital currency in the United States is no less complicated than in Europe. This is mainly due to the peculiarities of the legal system of the state (the presence of both federal law and state law) and the lack of a common position among regulators regarding the legal status of cryptocurrency.

In 2012, the US Federal Bureau of Investigation released a report entitled “Virtual Bitcoin, the unique features of which present certain difficulties in deterring illegal activities.” In it, the FBI expressed its concern about the possibility of carrying out illegal activities in the anonymous Bitcoin payment system [10]. In 2013, representatives of the Federal Reserve System identified cryptocurrency as "a threat to the banking system, economic activity, and financial stability."

However, later, the ItBit Trust cryptocurrency exchange, having received the Charter of the New York State Trust Company Charter from the Department of Financial Services, became the first officially regulated bitcoin exchange.

Canada ranks second in the world after the USA in the number of Bitcoin-ATMs, which indicates the high popularity of cryptocurrency in this country. In order to better understand the blockchain technology, the state is developing a digital version of the Canadian dollar based on it [11].

In 2015, a report of the Senate Standing Committee Banking, Trade and Commerce was published, according to which the best strategy for dealing with cryptocurrency is to monitor the situation as technology develops. At the same time, the regulatory policy of the government in the field of digital currencies and decentralized technologies should be reduced only to a “light touch” [12].

The state continues to monitor the development of digital currency and distributed technologies, regulating cryptocurrency activities only when necessary.

China is one of the fastest growing financial and technological markets in the world. This is where most of the mining pools are located, that is, special web services that are used to distribute computing power.

In 2013, the People's Bank of China indicated that there was no ban on the implementation of cryptocurrency transactions. At the same time, Bitcoin was defined as a kind of asset, not a currency [13].

In 2016, 70% of transactions in the Bitcoin network passed through the Chinese mining pools, while 40% of all transactions were in cryptocurrency exchanges located in China.

Then it became known that virtual property (including digital currencies) could soon be recognized as a "fundamental human right" in China. The relevant definitions are contained in the new draft of the main provisions of the Civil Code of the country.

The current legislation of China does not contain any special tax rules and transactions with it. At the same time, a cryptocurrency is defined as a virtual commodity, not a currency. Thus, the sale of digital money may be subject to value added tax, and income and profits in cryptocurrency are subject to income tax, income tax and capital gains tax.

Every year the number of cryptocurrency business incorporated in China is growing. However, the approach to the legal regulation of cryptocurrency relations in China is still not developed.

In Brazil, the Central Bank also initially warned of the risks associated with the use of digital money. At the same time, in order to tax cryptocurrency transactions, the Federal Tax Service considers digital money as a financial asset.

In Colombia, the Central Bank noted that digital currencies are not currency and legal tender.

And in Ecuador and in Bolivia, cryptocurrency is officially banned. In addition, in Thailand, Vietnam, Iceland and Bangladesh, transactions with bitcoins are prohibited and illegal.

In turn, attention should be paid to the experience of Ukraine, which is among the top 10 countries in the world in terms of the number of Bitcoin users. Initially, the National Bank of Ukraine equated cryptocurrencies to money substitutes that have no real value and are not allowed to be used by individuals and legal entities. However, after lengthy consultations with the Bitcoin communities in 2016 in Ukraine, a memorandum was signed on launching a system of decentralized online auctions in state institutions at municipal and regional levels, created for the privatization and leasing of state property, creating licenses. Also, the concept of the e-government portal E-Ukraine was presented with the aim of interaction between citizens, business and the state.

In 2016, the Ukrainian Stock Exchange became the first platform in the world where futures (derivative securities) for cryptocurrency were traded.

The National Bank of Ukraine announced the possibility of issuing electronic hryvnia, which will be based on the blockchain technology in December 2017.

The legislation of the Russian Federation currently does not define either the term "cryptocurrency" or its legal status, which entails a heterogeneous approach to these issues by state bodies. From the letter of the Federal Tax Service of October 3, 2016, it follows that Russian legislation does not explicitly prohibit Russian citizens from performing operations using cryptocurrency, which the Federal Tax Service qualifies as foreign exchange transactions. Chairman of the Central Bank of the Russian Federation Elvira Nabiullina October 5, 2017 stated that cryptocurrency is a private digital money, should not be legalized as a legal means of payment.

This breakthrough regarding the official definition of the cryptocurrency status was made by the Republic of Belarus, whose president signed Decree No. 8 on December 21, 2017. According to paragraph 4 of Annex 1 to this decree, the cryptocurrency is defined as bitcoins or another digital sign (token) that is used internationally means of exchange.

Estonia is most keen to attract the attention of cryptocurrency specialists. Estonia does not regulate the circulation of cryptocurrency. Estonia has intentions to regulate the circulation of bitcoins, however, the question remains open. The issue of allocation of special zones with a special status for cryptocurrency is being considered.

European countries are competing ahead of the curve. A country in which the conditions for the existence of cryptocurrency will be more acceptable, will receive an additional resource for development. If we talk about the leadership of individual countries, then Italy comes first. According to the independent agency SoinTelegraf in 2016–2017 In Italy, 269 Bitcoin operators and 4 Bitcoin ATMs were registered (1 operator per 225,800 residents). The United Kingdom is in second place in Europe - 11 ATMs and 362 operators are used here (the ratio is 1/177 000 inhabitants). In third place is Finland: 7 ATMs, 34 operators, 1 operator per 160,000 inhabitants. Then the Netherlands: 53

ATMs, 968 operators, 1 operator per 36,500 residents, Slovenia: 4 ATMs, 58 operators, 1 operator per 35,500 inhabitants.

The use of the capabilities of electronic voting, among other things, seemed interesting and in demand, including on the basis of unmanaged e-proxy voiting technology. This kind of technology could be a successful continuation of crypto-secure voting systems that were tested in the United States at one time and rejected due to a crisis of confidence.

4. CONCLUSION

The development of technology has repeatedly led to a change in the political and economic picture of the world. The development of technology that makes it possible to abandon the centralized guarantor of authenticity and depository of information may raise the question of the leading role of the state in managing politics, economics and other aspects of life. Analysis of the main applications of blockchain technologies should be carried out with an emphasis on identifying possible effects from their use in the banking sector and the development of the digital economy.

It should be noted that the banking sector, which is threatened by the spread of the decentralized blockchain / bitcoin system, is actively working on various projects and consortia related to the solution of various issues of using this technology. This is evidence of the serious transformational potential of blockchain technologies, and there is every reason to assume that the blockchain will become one of the most important components of the emerging digital economy and those innovations that will lead the post-industrial development to a fundamentally new level.

REFERENCES

1. Nakamoto S. A Peer-to-Peer Electronic Cash Systemю - http://coinspot.io/technology/bitcoin/perevod-stati-satoshinakamoto/

2. Information Paper for the Payments System Board // Reserve Bank of Australia. May 2013.

3. Australian Regulator: Bitcoin is Not a Financial Product // CoinDesk.

4. Australian Digital Currency Industry Code of Conduct // Australian Digital Currency business association

5. Digital currencies: response to the call for information // The UK Government. March 2015.

6. Questions and Answers: Action Plan to strengthen the fight against terrorist financing // European Commission, 2016

7. EU Banking Regulator Issues Warning on Virtual Currencies // CoinDesk, 2013

8. Virtual Currencies: Court Rules that Selling Bitcoin Is Not Money Transmitting and Selling Bitcoin to Criminals Is Not a Crime. Latham & Watkins While Collar Defense & Investigations Practice and Financial Institutions Group. August 31, 2016.

9. Bit Coins: Decrypting the Currency (Updated) // Lexology. 2016.

10. Bitcoin Virtual Currency: Intelligence Unique Features Present Distinct Challenges for Deterring Illicit Activity // Federal Bureau of Investigation, .2012

11. Canada Has Been Experimenting With A Digital Fiat Currency Called CAD-COIN // Forbes, 2016.

12. Digital Currency: You Can't Flip This Coin! // Senate of Canada. June 2015.

13. China's Central Bank Governor: PBOC Won't Ban Bitcoin // Coin Desk. 2014.