MASTER DISSERTATION

ON THE TOPIC

" The Blockchain System and Application in Finance "

Musayev Kamal Arif

BAKU - 2019

THE MİNİSTRY OF EDUCATİON OF THE REPUBLİC OF AZERBAİJAN

AZERBAIJAN STATE UNIVERCITY of ECONOMICS

INTERNATIONAL GRADUATE AND DOCTORATE CENTER

Head of the Center Dos. F.S.Ahmadov

sign_____

"20" May 2019

MASTER DISSERTATION

ON THE TOPIC

"The Blockchain System and Application in Finance "

Code and name of Programme: 060403, Master

Specialisation: Financial Management

Group: 650

Master:
(Musayev Kamal Arif)
_____

_____since

Program manager (dos. Seyfullayev I.Z.)
_____

_____ since

Scientific Supervisor
PhD. in. Econ., Quliyev.E.N.
_____

_____since

Head of the Department (Dr. Kalbiyev Y.A.)
_____

_____ since

BAKU - 2019

XÜLASƏ

Tədqiqatın aktuallığı. Son zamanların trend mövzusu olan kripto valyutaların iş p
bağlı danışarkən burada xüsusilə "Blokçeyn" texnologiyasını vurğulamaq çox önəm
müddət "bitcoin" kimi önəmli kripto valyutaların qiymətlərində müşahidə edilə
volatillik, ümumilikdə kripto valyutalara olan marağın artmasına səbəb olur. Bu da özü ilə
bərabər sahənin əsasında dayanan fundamental biliklərə olan tələbi artırır. Təkcə, "Bitcoin"
son bir ay ərzində 45% ucuzlaşmışdır. Sahə ilə bağlı fundamental biliklərin artırılması,
marağın daha da artması və sahəyə yatırımlar üzrə risklərin düzgün idarə olunmasına imkan
yaradır.

Tədqiqatın məqsəd və vəzifələri: Tədqiqatın əsas məqsədi Blockchain (bloklar zəncirinin) və
həmçinin də kriptovalyutaların fəaliyyət mexanizmini müəyyən etməkdir.

İstifadə olunmuş tədqiqat metodları: Tədqiqatda induksiya, deduksiya, sintez və analiz,
həmçinin də müqayisəli təhlil metodlarından istifadə edilmişdir.

Tədqiqatın informasiya bazası: Tədqiqatın informasiya bazasının əsasında Blockchain
(bloklar zənciri) və bitkoin və digər bu kimi kriptovalyutalar haqqında nəzəriyyəçilərin əsas
fikirləri və praktik məsələlər dayanır.

Tədqiqatın məhdudiyyətləri: Respublikamızda bitkoin və yaxud da bloklar zənciri kimi
kriptovalyutaların alınması və yaxud da istifadəsi demək olar ki, əhali qrupları arasında çox
az rast gəlinməkdədir. Belə bir şəraitdə isə əsas məqsəd belə kriptovalyutalara olan inam
hissinin yaradılmasıdır.

Tədqiqatın nəticələri: Tədqiqat nəticəsində məlum oldu ki, blockchain (bloklər zənciri) bir
şəbəkədir. Lakin "Alibaba", "Uber" kimi şəbəkələrdən fərqli olaraq "Blockchain" mərkəzsiz
fəaliyyət göstərir və cəmiyyət üzvləri arasında işlək vəziyyətdə olur.

Nəticələrin elmi- praktiki əhəmiyyəti: Texnologiyanın inkişafı nəticəsində bitkoin kimi
kriptovalyutaların fəaliyyəti sürətlənməkdədir. Hər bir blok özündən əvvəlki blokun
kriptoqrafik heşinə (ing.: "hash"), vaxt arayışına və köçürmə əməliyyatlarına sahib olur. Heş
funksiyası paylanılmış dəyərlər funksiyasıdır. Kriptoqrafik heş funksiya isə heş funksiyasının
xüsusi formasıdır və "bir istiqamətli funksiya" da adlanır.

Açar sözlər: blockchain, bitkoin, kriptovalyuta, heş funksiya

LIST OF ACRONYMYS

BTC: Bitcoin

US: United State

USD: United State Dollar

ICO: Initial coin offering

CONTENTS

INTRODUCTION

The blockchain technology began to actively penetrate into many areas of life. By its significance, it is comparable to the creation of the Internet and the widespread smartphoneization, literally penetrating the modern world and changing everything around: and how people work, and how people relax, and how people communicate with each other. In this regard, it would not be superfluous to learn in more detail what a blockchain is and why this technology is so good.

Life is inextricably linked with money, data and documents. Because of this, people have to contact various intermediaries who give them this money, documents and data, check it, certify their authenticity, give copies, check the authenticity of the copy, and so on.

Objective. The objective of the thesis is a comprehensive study and analysis of theoretical aspects and directions of effective use of blockchain system and ways of application in finance.

Methodology. The study is based on the analysis of scientific works of domestic and foreign scientists and economists concerning the blockchain technology activities as an financial category and its application, approaches and directions of such application.

The results of the study show that the blockchain technology covers various areas of activity of people. Many financial companies have already invested or plan to invest in the use of blockchain technology. On the one hand, the blockchain offers many opportunities that can permanently change our usual way of exchanging values. On the other hand, it is perceived as a threat to the existing trade model. Changes are always difficult, especially when it comes to global scale. However, the potential of the blockchain makes it clear that transformation is inevitable.

Practical significance. The use of blockchain technology allows to effectively organize the sharing of a variety of things - solar panels, wastewater treatment

systems, etc. It can create reputation protocols that will regulate the possibility of admitting one or another person to common services. By fixing on the network how different people use shared assets or services, it is possible to more equitably allocate resources and invoice them for payment. This model increases energy efficiency, as people will pay only for what they consume. Blockchain technology offers great opportunities and has many applications. When used properly, it will contribute to the rapid growth of many sectors of the economy.

Value / originality. The study of areas of blockchain technology of enterprises allowed to formulate the actual definition of this category. The author's interpretation of this definition is characterized by a systemic and comprehensive and logically describes the main actions, their focus and period of application, that is, the novelty and relevance of the study.

I Chapter. REVIEW OF BLOCKCHAIN TECHNOLOGY

1.1. Review Of Blockchain technology

The word "blockchain" is neologism even among advanced IT users: it is not more than 8-10 years old. The surge in popularity of this ingenious technology with great prospects falls at the peak of growth of electronic currencies based on the blockchain - in particular, Bitcoin. This is logical: expensive and suddenly grown in price goods (smartphones, gold, oil) always attracts increased attention - even those who are far from the world of information technology. Understanding the essence of this technology is as useful as owning computer skills or being able to drive a car. This knowledge is not for everyone; but those who own them are in a privileged position. Mathematical or computer education is not required - the explanations are really simple.

Blockchain is a shared, distributed ledger that records transactions within a network. The blockchain technology is built on ledgers distributed over several nodes (participants) within the network, which are peer-to-peer replicated. The peer-to-peer replication can be explained as every node is acting as both publisher and subscriber to the transactions made within the network. They receive and send transactions to others, where the information is synchronized with all nodes in the specific network. This method eliminates the need for a trusted third party for transactions, e.g. a financial institution. Instead, the massive distributed network where the validity of a transaction is agreed upon by all nodes are providing immutable records. Blockchain is using a consensus based model to ensure validity, meaning that all nodes must agree upon the transaction. Since the data within the network is distributed to all nodes and that peer-to-peer replication prevents tampering of data, the distributed network requires no central governing organ to be the trusted party since the independent nodes creates a consensus (O'Keeffe, M.; Terzi, A., 2015: p.25)

The blockchain is made up of blocks that contain a number of transactions made, which are then linked (chained) together through cryptographic, forming the blockchain. Blockchains consist of three main parts: blocks, chain and network. The block is where all the transactions are recorded to a ledger during a given period. Depending on the objective of the blockchain, the size, period and triggering events for every block is determined, i.e. it is not the same for all blockchains. The blocks are replicated over the entire network to create the validity and consensus as intended. The chains are blocks that are linked together, creating the blockchain. The glue that links the blocks together are cryptographic hash functions, which can be explained as the fingerprint of the data from the previous block that it "chains" itself to, which is referred to as parent block. This process is referred to as game theory since the full nodes compete against each other to find the correct hash function and collect the reward, which usually is a token of a cryptocurrency.

Picture 1. The Process of a Transaction in the Blockchain
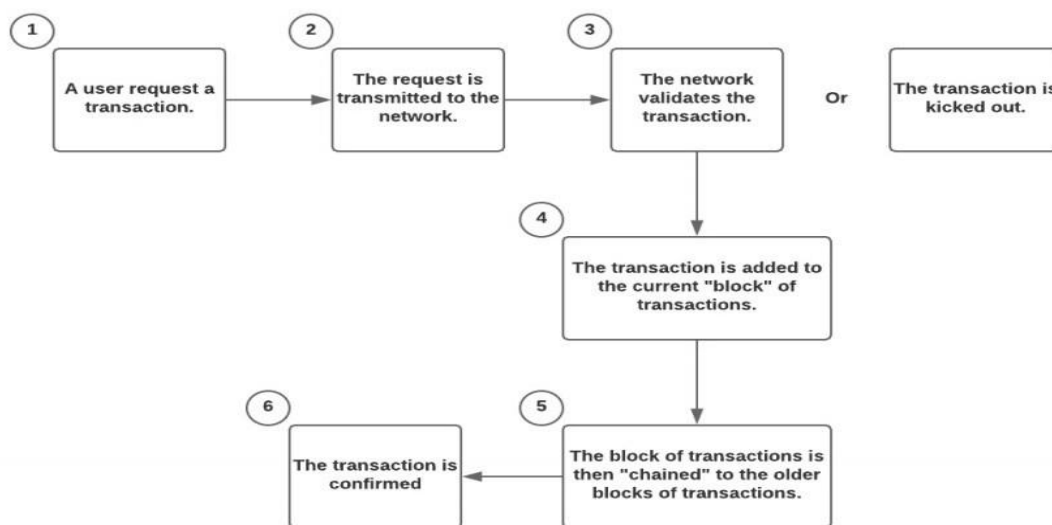

Source: Soo, Aeze 2016. The Blockchains Application Directory. Retrieved 6

The nodes illustrated are full nodes that holds the ledger i.e. the blockchain. This ledger is distributed over all full nodes in the network is replicated against the other full nodes that create the consensus. A block within the blockchain consists of

9

all transactions made within the network during the given period, before the block is chained and a new block is created. Each transaction holds the information regarding the sender, the receiver, and what the transaction consists of. This transaction data is encrypted, preventing the network from decipher the information even though it is visible. This provides an anonymity for the nodes as it at the same time makes the transaction verifiable .

Picture 2. The Main Components of Blockchain
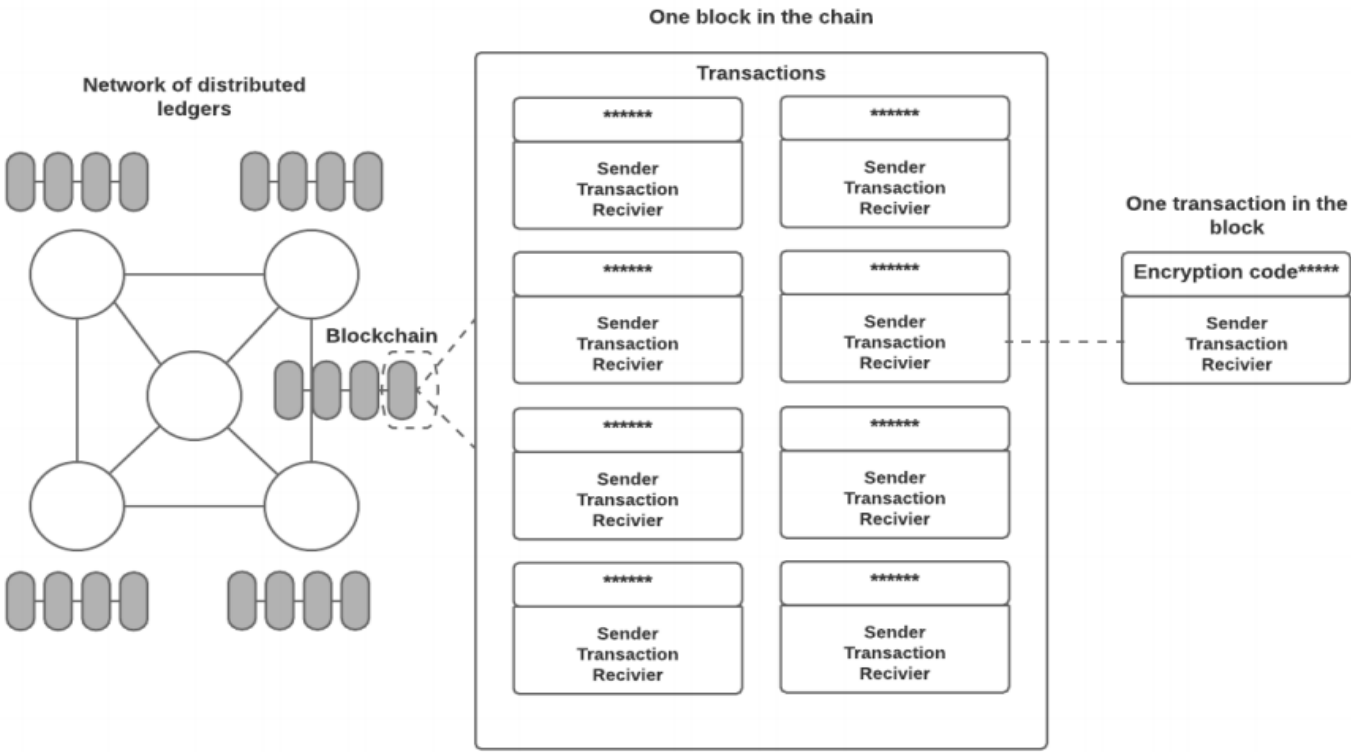
Source: Raval, Siraj (2016). "What Is a Decentralized Application?". Decentralized Applications: Harnessing Bitcoin's Blockchain Technology. O'Reilly Media, Inc.

By allowing digital information to spread, but not be copied, the blockchain technology has created the foundation of a new kind of Internet. The technology was originally developed for digital currency, Bitcoin, but the technical community is currently looking for other potential uses for this technology (Soo, A, 2016).

Bitcoin is called "digital gold" not without reason. Today, the total value of the currency is about $ 18.8 billion. The blockchain can create other types of digital value. It is not necessary to know how the blockchain works in order to use it, as well as, for example, the Internet or the car. However, having basic knowledge about this new technology will help to understand why it is considered revolutionary.

Blockchain is, as it is not difficult to guess from the name, 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. "Blockchain is an eternal digital distributed economic transaction log, which can be programmed to record not only financial transactions, but practically everything that has value," Don and Alex Tapscott (Don & Alex Tapscott), authors of the Blockchain Revolution (2016).

The information stored in the blockchain exists as a common and constantly verifiable database. This way of using the network has obvious advantages. The blockchain database is not stored in any one place, which means that it keeps records really publicly and they are easily checked. There is no centralized version of this information that could be damaged by a hacker. Copies are stored on millions of computers at the same time, and its data is available to everyone on the Internet .

In order to go to the analogy with Google spreadsheets, it is suggested to read the following opinion of a blockchain expert.

In the traditional way of working with document sharing, a Microsoft Word document is needed to be sent to another recipient and ask for changes to be made. The problem with this scenario is that it is necessary to wait for the copy to return before to see the changes made or make other changes, so it is impossible to edit it while someone else is working with it. This is an example of how databases work today. Two owners cannot do something with the same record at the same time. In the same way, banks maintain cash balances and transfers: they block access (or reduce balance) for a while while conducting a transaction, then update the other side, and

then re-open access (or update again). With Google Docs (or Google Sheets), both parties have access to the same document at the same time, and the only version of this document is always visible to both. This is somewhat similar to the general transaction log, but it is a general document. The distributed part comes into play when sharing is associated with a number of people.

Picture 3. The mechanism of blockchain technology
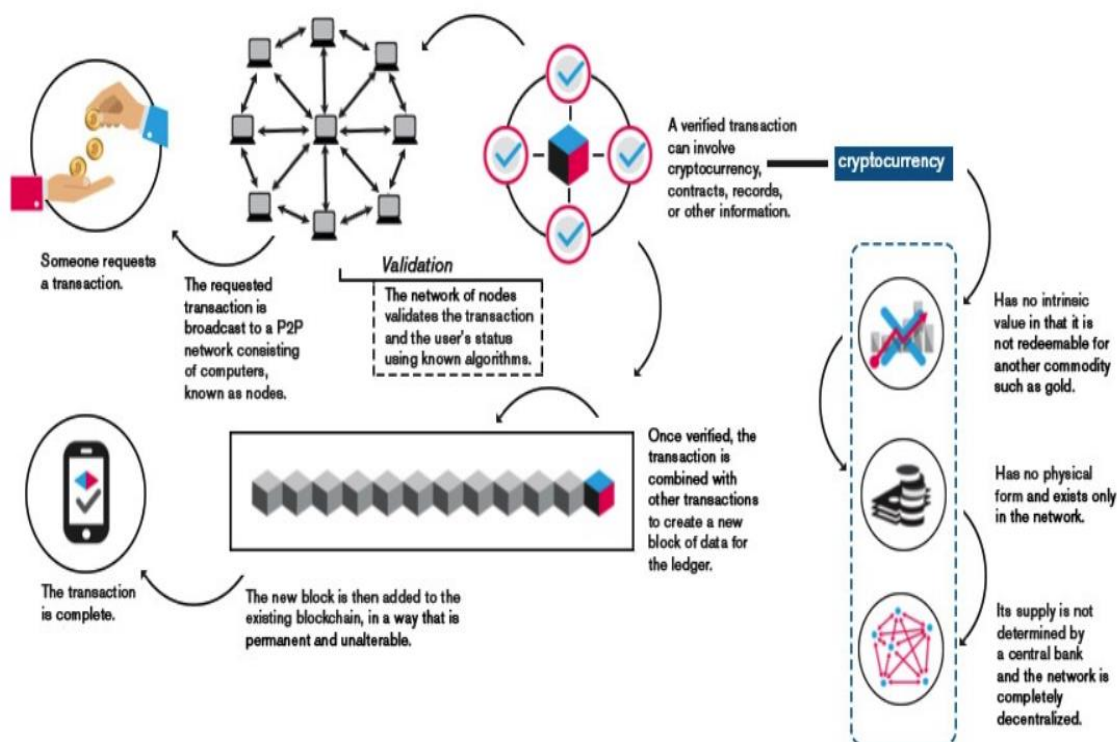
Source: Swan, M., 2015. Blockchain: Blueprint for a new economy. "O'Reilly Media, Inc."

Blockchain technology, like the Internet, has built-in error tolerance. Keeping blocks of information identical in the entire network, the blockchain cannot:

- Controlled by one;

- Does not have a single point of failure.

Bitcoin was invented in 2008. Since then, the Bitcoin blockchain has been operating without significant disruptions. (Today, the problems associated with Bitcoin were due to hacking of services built on top of it, or lack of control. In other

words, these problems arise because of bad intentions and human errors, and not because of flaws in the protocol architecture).

For almost 30 years, the Internet has proven its reliability. This achievement bodes well for blockchain technology that continues to evolve .

"No matter how revolutionary this may sound, the blockchain is indeed a mechanism that provides the highest degree of accounting and identification. No more missed transactions, human or machine errors, or even changes made without the consent of the parties involved. Most importantly, the blockchain helps to ensure the legitimacy of a transaction by recording it not only in the main registry, but in a distributed registry system connected via a secure verification mechanism. " - Ian Khan, TEDx speaker | Author | Techno-futurist (Swan, M.,2015: 47 p.).

The blockchain network exists in a state of consensus - automatically checks itself every ten minutes. A kind of self-auditing digital ecosystem. The network negotiates every transaction that takes place at intervals of ten minutes. Each group of these validation operations is referred to as a "block". This results in two important properties:

- Transparency - data is embedded in the network as a whole, and they are, by definition, public.
- Privacy - changing any unit of information in the blockchain requires the use of gigantic computing power to replace information in the entire network.

Only a limited number of nodes or everyone can be granted access to reading the history of transactions. There are two types of blockchains that relate to this: Public blockchains and private blockchains. All users have access to reading all transaction history and to create new transactions within public blockchains, compared to private blockchains where access is limited to a predefined group of nodes. The actual writing of transactions can be related to the conflict between security and speed, where the decision related to who will have the right to write

transactions is made. If everyone is granted to write transactions, the effort required will be advanced, i.e. very expensive, since the network need to be secure. But if the access is restricted to trustworthy nodes, a less advanced effort is required. There are two types of blockchains that are related to this: Permissioned blockchains and permissionless blockchains. Permissionless blockchains allow everyone to write transactions, giving every node the opportunity to verify transactions, as well as create and add new blocks. Permissioned blockchains have a predefined trusted group of nodes that are granted writing access within the network. Meaning that only this group of nodes be a part of the distributed consensus structure and verify transactions.

The system under consideration appeared in 2009 along with the Bitcoin cryptocurrency. Its creator was the mysterious Satoshi Nakamoto, about which very little is still known (it is not even clear whether it is one person or a whole group of people). It was Nakamoto who laid the foundation on which the key principles of the blockchain function were laid. Initially, this technology was calculated only for Bitcoin, but then new payment systems appeared with cryptocurrency of the same name (Litecoin, Dash, ZCash). Each system introduced something new, but they all relied on the principles created in 2009.

As mentioned above, this network is a chain consisting of blocks (they can also be called links). All links are interconnected and contain some array of cryptographic information. A new dataset can be formed only after closing the old element. The block is closed after the selection of a unique key (in the case of Bitcoin, this is a 64-digit number).

Key selection is carried out by mining, during which the computing power of certain equipment (processor, video card or ASIC) is used. The main goal of this operation is to find a cryptographic signature to the block in the form of a hash. After selecting the key, the block is closed, and the miner receives payment in the form of cryptomonet. Different systems have their own unit reward (12.5 BTC, 25 LTC, 12.5

ZEC, 3.35 DASH). Since a large number of people take part in deciphering, the reward is distributed between them, and the amount of payment depends on the contribution of a particular participant to the search for the key (Haber, S.; W. Scott., 1991: 36 p.)

"Thick" wallets download all transaction blocks to a PC (or to another storage). Owners of full-fledged storage should allocate a solid amount of memory on the drive (in the case of the same Bitcoin, for the blockchain, 210.09 GB should be released as of August 15, 2018). Moreover, the number of blocks is constantly increasing, which means that it is necessary not only to allocate the specified amount of memory, but also to leave an impressive margin. Being a full node is not so easy, but these users are of great importance for the network - the more, the faster the information about remittances is processed .

An equally important principle of the blockchain is anonymity. We mentioned above that this network is transparent. Anyone can view the transaction history, the direction of specific transfers and even the amount of transactions. However, the identity of the sender and the recipient is not disclosed, which gives people complete freedom to make deals.

Access to the blockchain is carried out using special keys containing unique cryptographic entries. Each individual user has such a key. Since any cryptographic identifier is unique, hacking the network is almost impossible (for this, hackers must have access to all computers of the system). Due to this principle, the blockchain has an extremely high degree of reliability.

Separately, it is necessary to say about the mechanisms that guarantee the viability of the network. These are 2 types of algorithm:

- Proof of work done (Proof of Work or PoW).
- Proof of share (Proof of Stake or PoS).

The Proof of Work algorithm is used in the Bitcoin network. It is somewhat reminiscent of office reporting, when each employee in writing reports to the

authorities about the work done in order to receive a salary. In the case of the blockchain, PoW checks the calculations that are generated when the block is formed. The principle here is quite interesting. A data array is considered closed if its hash value is less than the signature required by miners. In other words, a specific cryptographic cipher authenticates the block. Network node authentication is done by node nodes.

As of August 15, 2018, the average time to create a new "link" in the Bitcoin blockchain is 9 minutes 4 seconds. For the specified time interval miners are looking for a signature, and verification is carried out instantly. The Proof of Work algorithm has one significant flaw: it requires solid computing power. Therefore, a transaction fee is charged for the transaction of BTC coins, which is a fee for using these capacities.

Against this background, the Proof of Stake algorithm looks more attractive. He is actively promoted by Vitalik Buterin - the creator of cryptomonet Ethereum. The essence of PoS is that the leading role here is played not by computing power, but by the balance of a cryptocurrency wallet. That is, the transfers will be carried out not with the help of technology, but thanks to active crypto coins in the repositories. With perfect hands, all cryptocurrency holders on the platform with the Proof of Stake algorithm will play the role of investors. This means that mining will become secondary. At the same time, PoS is not without flaws, one of which is the possibility of duplicate transactions (Raval, S: 2016: 45 p.)

The golden mean for normal operation of the blockchain is a combination of PoS and PoW. At the present stage, such an algorithm is used only in several systems:

- Blackcoin;
- Espers;
- KATZcoin.

If we talk about why blockchain is needed, here we can single out a lot of potential applications. First of all, using this technology it is real to create an almost

16

ideal payment system that allows to do without third-party participants (banks and other centralized institutions). Already, the blockchain is capable of performing tasks specific to the financial services market:

- registration of transactions;

- installation of authenticity of the person;

- conclusion of contracts.

The latter task is of particular interest, because it can be automated. The fact is that blocks can store not only information about transactions, but also other digital information, including computer code. This code can be programmed to automatically enter into a contract when the specified conditions are met. For example, the parties to the transaction can enter their keys, thus giving consent to the conclusion of the contract, after which the system will immediately register it. Such a mechanism of interaction between the parties is called a smart contract and the most interesting thing is that its possibilities are almost limitless. In a similar way, you can program:

- the purchase of shares of a certain company when prices reach the target;

- payment of electricity when the volume of electricity consumed reaches a predetermined value;

- control over the use of intellectual property (it is possible to limit the time of viewing information, its copying, the ability to share on social networks).

In the near future, blockchain use is possible at the highest level. Every year this technology attracts more and more attention from both large companies and entire countries. The use of this network means payment systems VISA, Mastercard, SWIFT.

Ukraine, the United Arab Emirates and Sweden are discussing the possibility of maintaining the land registry on the basis of the blockchain. India plans to fight land fraud with this technology.

Moreover, the blockchain network is already being used to identify refugees in Finland. A blockchain e-citizenship system has been launched in Estonia. Also, the identity verification system based on the technology in question is being tested in Brazil, and since June 2017 a similar innovation has been actively used in the Irish consulting company Accenture and in the US corporation Microsoft.

As can be seen, the blockchain can be used in different ways. The main thing is to clearly understand the purpose of the application and correctly implement the plan .

So, we have dealt with almost all issues related to the blockchain technology; understand what it is and what for. It remains only to highlight the strengths and weaknesses of this system:

Table 1. Strengths and weaknesses of blockchain technology

Strengths	Weaknesses
Decentralization - the network is missing one main server. All its members are equal. They can exchange information and money directly without involving centralized systems.	The technology can be used for money laundering and shadow business.
High degree of reliability, protecting the network from hacker attacks.	The operation cannot be rolled back with a random money transfer.
Transparency - information about all transactions is publicly available.	Low chances that the system will work normally outside the cryptocurrency ecosystem. For example, if the network starts storing at least some of the data on VISA system transfers, the weight of the blockchain will reach hundreds of terabytes.
On the basis of the blockchain, it is possible to create new peer to peer payment systems, eliminating the flaws of the old versions.	
Universality - the technology in question can be applied in almost all spheres of life: the	

financial sector, legal services, and medicine.

Even despite the presence of some minuses, the blockchain can be called one of the most breakthrough creations of the 21st century. This technology can permanently change not only the financial market, but also the scope of other services. However, much will depend on the interest of ordinary people, and on the initiative of political figures.

1.2. Option of Cripto currencies

As mentioned in the previous chapter, the blockchain technology has mostly been used for cryptocurrencies at the time of writing. The word "cryptocurrency" denotes a new type of payment instrument intended for use on the Internet. Cryptocurrencies represent a novel and avant-garde digital currency with the intent of harnessing a financial system that is aimed at a worldwide adoption scheme and supplanting or substituting national sovereign fiat currencies and dominating the modern financial systems with one single digital fungible asset that is traded globally and is based on a global exchange-backed valuation.

The cryptocurrencies that exist today largely follow several characteristics. These characteristics include:

• A Peer-to-Peer connection and data transfer scheme and is therefore decentralized by nature (Although there are some exceptions such as nationally developed cryptocurrencies).

• Contain a finite and fixed total amount or supply of coins that can be generated or given (Also influences price, availability).

• Incorporates a public ledger (Mostly known as a Blockchain) or database that stores records of transactions and transfers of coins which prevents double spending.

• Feature a computational algorithm or "Proof of work" which verifies the integrity of the blockchain and consecutive blocks that contain the transaction data. In

most cases, the Bos 12 computational power is provided by "Miners" to the network. Due to the finite amount of coins in circulation in most cryptocurrencies, the algorithm scales in difficulty and computational power required in accordance to the amount of coins mined.

• Utilize some form of cryptography (Usually public and private key cryptography) for safe storage.

Unlike ordinary money, represented by banknotes and coins or having electronic equivalents in the WebMoney or Yandex.Money system, cryptocurrency has no physical media and exists only in the form of program code. Therefore, it is often referred to as virtual or digital currency. The program code of digital money contains information about the quantity and for which wallet addresses these coins are attached. The owner of the virtual currency is the user of the computer network who has access to this address. Moving coins from one address to another means making a purchase-sale transaction with it (Kopfstein, J., 2013: p.45) .

Cryptocurrency is a digital currency protected by cryptographic technology. There is no physical analogue of these monetary units, they exist only in the virtual space. The term "cryptocurrency" came into use after the publication of an article telling about Bitcoin - a digital currency and payment system. Bitcoin is the brainchild of Satoshi Nakamoto, but what kind of person or group of people is behind this pseudonym is still not known for certain. The concept of a decentralized payment system Nakamoto introduced October 31, 2008. Its main principles are: anonymity for all participants, protection from fraud and independence from regulatory organizations.

A Bitcoin network consists of interconnected blocks of transactions. Each subsequent block contains information about the previous one, so that it can be built them into a single chain and get information about all transactions made earlier (but not about Bitcoin owners). The process of creating new blocks is called mining. For the next block to appear on the network, it is necessary to generate a cryptographic

signature for it. By the way, their emission is not an endless process. It is known in advance that no more than 21 million bitcoins can be created.

At first, it was relatively easy to create blocks; single miners also coped with this. Over time, the complexity grew, for mining required substantial computational power, so miners began to unite into pools and extract new Bitcoins together.

Bitcoin is the most popular digital currency in the world. This coin appeared in 2009 thanks to the efforts of the now legendary Satoshi Nakomoto and is the very first in time. The primacy of Bitcoin among other cryptomonet today is confirmed in the following areas: programming - the principles of decentralization and limited emission implemented during the creation of Bitcoin have become reference characteristics for the development of other virtual currencies. Finance - Bitcoin has the most expensive exchange rate against the US dollar and the largest total value. Media - the word "Bitcoin" became the leader of queries in Google search at the end of 2017 and is often used as a synonym for the term "cryptocurrency".

Cryptocurrency works only in a computer network. In its blockchain, which is essentially a database, information on the amount of digital money stored in wallet addresses is publicly available. Moving a virtual currency between wallets, that is, making a transaction, is recorded each time by a new entry in the blockchain (Haber, S.; W. Scott: 1991).

The need for digital currency has arisen due to the fact that ordinary money has ceased to satisfy the requests of a significant number of consumers. The development of the Internet has necessitated the need of its users for a payment instrument that will have the following advantages: accepted in all countries of the world ensure instant payment transactions; keep secret the identity of the owners of virtual assets; guarantee inflation protection and central bank regulation. Currently, virtual currencies, in addition to the listed initial tasks, are actively used for investing. Given the rising cost of cryptomonet, many users view their acquisition as a way to increase material wealth.

The easiest way to become the owner of the necessary amount in virtual currency is to buy. On the Internet, crypto exchangers and cryptobirds provide assistance in this. The first carry out transactions quickly, but usually work illegally. The latter are more reliable services, but require registration and often personal identification. It is possible also purchase virtual currency by participating in startup financing for the initial placement of coins (ICO). It should be remembered that some of the ICO teams after collecting money disappear without a trace.

Small amounts can be obtained with the help of so-called bitcoin-cranes, handing out users small bitscoins for viewing ads. Mining, i.e. mining cryptocurrency provides a steady income, but requires a significant investment in equipment.

Mining is the process of mining cryptocurrency associated with the calculation of complex mathematical problems using computer power. The organization of mining depends on the size of the allocated budget. The presence of a large amount allows to purchase ASIC - equipment specifically designed for the extraction of digital currency, and, accordingly, provides the greatest profit. With limited funds, it is advisable to examine the available video card for its ability to extract a certain type of coins. In any case, mining requires taking into account fixed energy costs and commissions when connecting to the pool (server for mining).

Universal criteria for their differences are the conditions of their emission and attitude towards decentralization. However, each coin is positioned as a means of implementing a certain idea. Among the largest virtual currencies, the most popular concepts are the following groups:

- Bitcoin, Bitcoin Cash, Litecoin - coins, combined blockchain technologies and the idea of developing virtual payments;

- Ethereum, EOS, Cardano, NEO - these names represent platforms that are designed for the development of smart contracts;

- Ripple, Stellar - implement the idea of instant money transfer;

- Monero, Dash - coins, aimed at ensuring the anonymity of payments.

Prices for Bitcoin and other coins are very volatile. The main factor in the fall or growth of the exchange rate is the news that determines the prospects for the development of the cryptosphere. First of all, this is information about the successes, plans or problems of cryptocurrency companies. Cryptomarket is very sensitive to events that indicate the attitude of the authorities to Bitcoin and other coins. The economic policy of such significant countries for the cryptoindustry as the USA, China, Russia, South Korea has a significant impact on the value of digital currencies.

Also, the prices of coins are determined by the behavior of their owners. Cryptomarket is subject to the collective fear of missing a profit or losing it. Therefore, the chart of rates of digital currencies sharply grows or falls, if investors cover a single impulse.

The use of virtual currencies is based on user trust. Unlike national currencies, the value of digital money is not supported by assurances of state banks and other official financial institutions. Digital coins are freely convertible and their significance is determined primarily by the supply-demand ratio. Guided by this principle of the market economy, Satoshi Nakomoto programmed a Bitcoin deficit, limiting its maximum amount to only 21 million coins (Kopfstein, J., 20132: 45 p.).

Now on the market there are coins that are not restricted in emissions. The demand for these coins is determined by the possibilities of their practical application. For example, the demand for Ethereum is largely based on the idea of creating and maintaining smart contracts.

In order to make money on cryptocurrency, it is necessary be a developer, miner or trader, exchange trader. Participation in the launch of cryptocurrency projects as a developer guarantees significant earnings, but requires a high level of professional training. The miner's earnings are influenced by the costs of purchasing mining equipment and paying for electricity. The role of the merchant of digital coins requires constant attention to the trends of the crypto market and involves buying at a

low price and selling at a high. Merchants are faced with high fees on cryptobourse and a complex mechanism for withdrawing profits. Given the high risks in the cryptocurrency trade, it is recommended to invest in the purchase no more than the amount of money that it can be afforded to lose.

Cryptocurrency has several significant advantages. First, it is not afraid of inflation. If the printing press goes mad and puts on a frantic amount of money, it is logical that this money will be worthless. With Bitcoins, this situation is excluded: their number is known in advance and limited.

Another plus is decentralization. There is no single center from which the system is managed, which means that it is extremely difficult to impair the operation of this system by forcibly limiting the spread of the currency. The network simply does not have a single owner, it is controlled by users around the world.

The next advantage is anonymity. Transactions can be tracked and seen how many bitcoins moved from one wallet to another, but it's not so easy to determine who exactly owns the wallet. Anyone can open an account in bitcoins, for this appropriate software and access to the network is needed.

Cryptocurrency rapidly broke into the global financial markets, claiming its rights to its high demand along with the traditional currency. After the success of bitcoins, the global cryptocurrency market is replenished daily with new altcoins. In the past six months alone, more than 500 new types of cryptocurrency have been created, and the process of generating digital coins continues to gain momentum.

The global capitalization of the cryptocurrency market exceeded $ 700 billion, which gives grounds for bold forecasts for its further growth. For comparison, in the USA alone, the total volume of bank deposits is estimated at $ 3 trillion, and the capitalization of the world securities market reaches $ 86 trillion. Against this background, the capitalization of the cryptocurrency market looks like a novice player among experienced and venerable professionals.
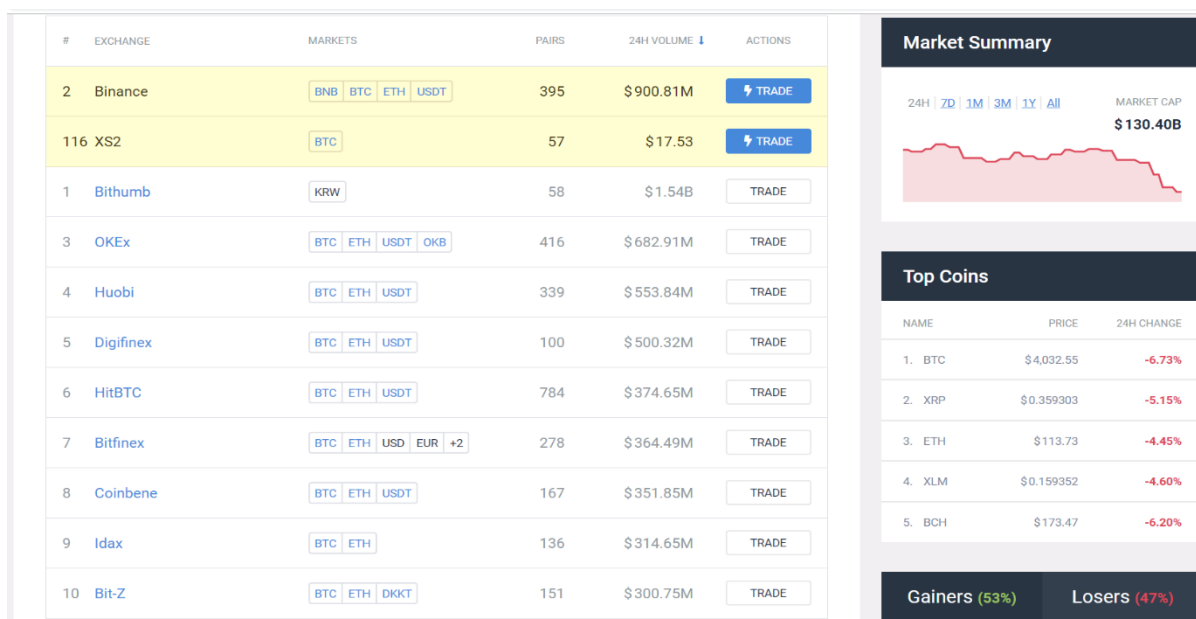
However, the price of cryptocurrency is characterized mainly by steady growth. For example, the quotation of the most popular Bitcoin has soared many times over a short time, which led to an increase in demand for this type of cryptocurrency, and also stimulated the emergence of new altcoins - alternative digital coins .

In order to have a bitcoin wallet, it is necessary to go to the official website of the payment system and select from the list of applications for Android, iOS, Windows, macOS and Linux an option that fits. The only problem is that such applications may take up too much space, but in this case there is another way.

Multicurrency wallets - wallets supporting several types of cryptocurrency have become a very convenient tool for storing and exchanging digital coins. Depending on the method of storage, the following types of wallets are distinguished: online, mobile, local and hardware. The table below shows the most popular multicurrency wallets for various platforms and the types of cryptocurrencies that they support.

In order not to waste time searching for the exchanger with the most favorable rate, it is needed to use CoinCodex - this is a service that collected information on current rates of more than 100 exchangers. Independently looking for the most advantageous in such a pile of offers is a task for the infinitely patient. With CoinCodex, it is possible literally in a couple of clicks to determine which exchanger services to use.

Picture 4. CoinCodex Cryptocurrency Exchanges Service interface

#	EXCHANGE	MARKETS	PAIRS	24H VOLUME ↓	ACTIONS
2	Binance	BNB BTC ETH USDT	395	$900.81M	⚡TRADE
116	XS2	BTC	57	$17.53	⚡TRADE
1	Bithumb	KRW	58	$1.54B	TRADE
3	OKEx	BTC ETH USDT OKB	416	$682.91M	TRADE
4	Huobi	BTC ETH USDT	339	$553.84M	TRADE
5	Digifinex	BTC ETH USDT	100	$500.32M	TRADE
6	HitBTC	BTC ETH USDT	784	$374.65M	TRADE
7	Bitfinex	BTC ETH USD EUR +2	278	$364.49M	TRADE
8	Coinbene	BTC ETH USDT	167	$351.85M	TRADE
9	Idax	BTC ETH	136	$314.65M	TRADE
10	Bit-Z	BTC ETH DKKT	151	$300.75M	TRADE

Market Summary

24H 7D 1M 3M 1Y All — MARKET CAP $130.40B

Top Coins

NAME	PRICE	24H CHANGE
1. BTC	$4,032.55	-6.73%
2. XRP	$0.359303	-5.15%
3. ETH	$113.73	-4.45%
4. XLM	$0.159352	-4.60%
5. BCH	$173.47	-6.20%

Gainers (53%)   Losers (47%)

Source: Bernstein, 2017. Blockchain based intellectual property management.

In order to understand the dynamics of the cryptocurrency market online, to be aware of the changes in quotations by types of cryptocurrency, to have reliable and relevant material for analyzing and forecasting in the short and long term, the website has interactive charts for quotes, tables with courses cryptocurrency and other useful information .

To find the best rate, select the currency you have and the one for which you want to exchange it. The service provides a list of exchangers that carry out operations with these types of currencies, you sort them by exchange rate, compare and select. When there is no possibility to exchange currency directly, double exchange will help - a transit currency comes to the rescue.

If the current state of affairs does not suit, it is possible to set up alerts. As soon as the course gets to the appropriate mark, CoinCodex will notify by email or in Telegram. It is possible to study in advance the fluctuations in the course of the period from an hour to a year.

The course of cryptocurrency online is displayed on this section in the table with the ability to sort the columns with the corresponding indicators. The cryptocurrency market is changing not only daily, but even every minute.

Capitalization is defined as the value of a cryptocurrency multiplied by the number of coins in a cryptocurrency turnover. Price - the average value between the rate of buying and selling cryptocurrency on various cryptocurrency exchanges. At the moment, the price is formed according to 22 exchanges. Also, the columns to the right indicate the change in the price of cryptocurrency as a percentage relative to its value in the last 24 hours.

Volume is the total number of transactions on a particular cryptocurrency for the last 24 hours on all exchanges for which the price is formed in this table.

By default, the rate of digital coins is set in US dollars USD. But it is possible to choose the rate of cryptocurrency in relation to other popular currencies: ruble, euro, pound, franc, zloty, etc. Also, you can set and analyze the course of all altcoins in relation to bitcoin (BTC) or broadcast (ETH). Such cryptocurrency pairs will be of interest to those users who are actively engaged in trading on cryptocurrency exchanges

Real-time cryptocurrency rates, capitalization, trading volume and dynamics of changes will help the user to determine the best and future cryptocurrencies both for a certain period of time and as of the current date. In addition, in order to properly make investments in cryptocurrency, you need to assess the state of the market and choose the optimal time to enter it.

Of course, supply and demand are the main factors that influence the rate of crypto money. It is difficult to say how well technical analysis works in the cryptocurrency market. Highly volatile fluctuations in the course of digital coins, as a rule, are due to the information background. The demand for a particular currency depends on what source and how much information is positive or negative.

In addition, a certain directly proportional dependence of the rate of altcoins on the course of Bitcoin is traced. In most cases, when Bitcoin depreciates, the rates of almost all altcoins fall with an even higher percentage. Rates only some cryptocurrency can grow relative to BTC, which may be due to the good news at this time and specifically on these digital coins.

For example, the message of the People's Bank of China about the suspension of all ICO (Initial Coin Offering) held on Chinese platforms led to a sharp decline in the Bitcoin rate, followed by an altcoin rate in an even larger percentage ratio. In other words, the Central Bank of China officially recognized the primary placement of cryptocurrency tokens as an illegal operation. After that, some major Chinese stock exchanges announced the termination of trading.

Determining the legal status of cryptocurrency in any country is a very positive factor for the upward movement of the course. Japan became the first country in the world to recognize Bitcoin and some Altcoins as an official means of payment. In many countries, the status of cryptocurrency is in the process of being determined, including in Ukraine and Russia.

Also, the positive news for Bitcoin and certain Altcoins are the emergence of crypto-ATMs, the addition of new coins to major exchanges, the aggregation with payment systems, the use of cryptocurrency capabilities and Blockchain technology by large global corporations in various fields, the implementation of cryptocurrency developers of various technical options and much more. That is, the more cryptocurrencies become part of the daily life of citizens of different countries, the more their value and value grows.

To determine prospective cryptocurrencies, you need to study in detail the information on each coin you choose, namely: the history of creation, technology, development plans, their implementation and the public's reaction to it, course charts and trading volumes for different periods.

Also, you should pay attention to the main criteria for prospective cryptocurrency (Keirns G. 2017: p.52):

Evaluation of market capitalization as evidence of financial stability of the currency.

Liquidity - indicates the demand for cryptocurrency. In other words, how easy it is to sell / exchange.

The nominal value of a cryptocurrency expressed in another currency. Higher rate as evidence of sustainability.

Volatility or how changeable the main indicators of cryptocurrency.

The list of the best cryptocurrencies is quite extensive, and choosing the most promising of them is to guarantee a successful investment in the future.

Today there are several thousand of the most diverse cryptocurrencies, but most of them are soap bubbles. The most popular and reliable for 2018 are (Oliver, J., 2017):

- Bitcoin is the most popular cryptocurrency and, figuratively speaking, the founder of the genre. With its advent, Bitcoin marked the beginning of the development of all other similar currencies. The developer is a hidden group of programmers who call themselves Satoshi Nakamoto.

It is worth noting that the creators of BTC have left the free code of their development, which has enabled other specialists to create on this basis new types of cryptocurrencies. BTC emission is limited to 21 million (at the moment this limit has not yet been reached).

- Ethereum is a platform for creating decentralized online services based on the blockchain (Dapps, Decentralized applications, decentralized applications), working on the basis of smart contracts. Implemented as a single decentralized virtual machine. It was proposed by the founder of Bitcoin Magazine Vitalik Buterin at the end of 2013, the network was launched on July 30, 2015. Being an open source platform, Ethereum greatly simplifies the introduction of blockchain technology, which explains the interest not only of

new startups, but also of the largest software developers, such as Microsoft, IBM and Acronis. Financial companies, including Sberbank, are showing significant interest in the platform.

Unlike other cryptocurrencies, the authors do not limit the role of Ethereum to payments, but offer it, for example, as a means for sharing resources or registering transactions with assets using smart contracts, in particular, the authors called Ethereum a "crypto fuel" for executing smart contracts with a peer-to-peer network. Ethereum is sold on exchange services, and the capitalization of the total amount of air has exceeded thirty billion dollars.

- Litecoin was founded by programmer Charlie Lee, who in the past worked for Google. Release Lightcoin was launched in 2011. The main idea of this work is to become a peculiar analogue of silver in the digital finance market, given that Bitcoin already known to you is often associated in value with gold. LTC emissions are limited to 84 million.

- Zcash is an open source cryptocurrency developed by Zerocoin Electric Coin Company, providing confidentiality and selective transaction transparency. Zcash payments are published in a public block chain, but the sender, receiver, and transaction amount remain private. The Zcash trading symbol, ZEC, is not an official ISO 4217. Like Bitcoin, Zcash has a fixed total stock of 21 million units. For the first time, the currency was announced on January 20, 2016 .

Although to some extent these altcoins are struggling to become the most popular payment system of all, the nuances keep them in different markets. For example, Monero is an anti-tracking cryptocurrency with anonymous transactions, which allows users to maintain the confidentiality of their transactions and maintain a balance without fear that third parties will know about it.

The first and most obvious use of cryptocurrency is payments, and the list of companies accepting Bitcoin to pay for goods and services is growing, and ATMs with a withdrawal function are located throughout the world. The race began to create a standard form of payment using cryptocurrency debit cards, such as Bitpay, which will allow their owners to pay for purchases through ordinary terminals in stores. Although all this is great, the blockchain technology is not limited to the financial sector. It can be used to solve many problems existing in the modern digital world. So now we can see hundreds of new projects with really incredible ideas .

Following the ethereum, dozens of smart contract platforms were created, offering innovative solutions to problems related to agriculture, medicine, IT, logistics and almost any other sector. For example, Sia allows you to rent unused hard disk space. In exchange for connecting this empty space to the blockchain, you will receive a certain amount of Siacoin, the project's own cryptocurrency. Here it should be noted the difference between coins and tokens. Coins exist solely as a form of digital money on their own blockchains. Bitcoin and lightcoin are vivid examples of coins. Tokens occupy a different niche and serve alternative purposes - for example, they represent a digital asset, a share, a fee for using the system, etc.

Dragonchain, Waltonchain and Civic - ERC20 tokens. This means that they exist in the ethereum blockchain, and they all serve the corresponding utilities provided by the project. It is important to note that the usefulness of cryptocurrency is its main characteristic: if the token has practical application and solves an existing problem, it will most likely increase in price. However, many useless coins ended up with more than they should have. For example, Dogecoin was originally a comic cryptocurrency without any value or real market use. With a market capitalization of about $ 600 million (at the time of writing), this is probably the most profitable joke in the world. Despite some low quality projects (or comic projects), it is fair to say that cryptocurrencies do not exist in a vacuum, but depend on the value of the decentralized application, platform, or blockchain they are based on.

Despite all its revolutionary properties, the cryptocurrency industry faces a number of problems that make mass recognition a slow and even somewhat painful process. Let's look at the biggest obstacles that cryptocurrency must overcome in order to get massive approval. In all methods of payment stability is important. At times, the volatility of most cryptocurrencies is frightening: they can drop significantly or increase in price in minutes. This is a good chance for investors, but the average seller or consumer will not resort to cryptocurrency because of such risks. Speed and transaction costs are another drawback. Few coins can compete with payment systems like Visa. For example, a bitcoin transaction now takes about an hour on average, and the commission exceeds $ 15. This makes Bitcoin useless for everyday operations. It is hopelessly slow and too expensive for small purchases. Not to mention the problem of scalability, which does not allow networks to process a large number of transactions over a certain period of time. Then there is the question of security. Crimes in the millions of dollars have already occurred in cryptospace, such as breaking into the Mt. Gox. Plus, users do not always correctly use cryptocurrency. While the cryptocurrencies are incredibly reliable, the "safety technique" is still evolving. Think about e-mail: it took users decades to learn how to recognize spam, infected and phishing emails.

The way in which new cryptocurrency projects attract funds has led to increased control and led to discussions about regulation. China and South Korea have banned participation in the ICO - the primary offers of coins - of their citizens, and a number of other countries may well follow suit. Unfortunately, several scammers managed to rob enough people by offering "new coins". Legitimacy is the key to recognizing cryptocurrency, and cowboy-style antics create a bad reputation for them and cause skepticism about the long-term viability of the technology. Even after the ICO issue is settled, the legitimacy of using cryptocurrency will continue to be questioned. The authorities will not approve the use of cryptocurrency by citizens for tax evasion or the financing of criminal activities (Castillo M. D., 2018) .

The list of problems is impressive, but each one of them has more than one solution on the horizon. The smartest people in the world entered the business, full of enthusiasm. Technological problems seem the easiest to overcome. Recent additions, such as IOTA, can provide unlimited scalability and almost instantaneous transactions at no cost. The so-called stable coins solve the problem of volatility, using various inventive methods so that the cost of cryptocurrency does not fluctuate. Security measures are intensifying, and exchanges, such as NEX, are becoming real fort Nocks of the cryptosphere. Despite all this rapid progress, the fate of cryptocurrency depends too much on the authorities. Fortunately, it is clear to many governments that cryptocurrencies have great value, which is difficult to realize until the end. To the extent that trillions of dollars will flow into a crypto economy, many countries are likely to try to become leaders of the cryptocurrency space. Where there is money, there will be taxes. As the economy develops, investors, corporations, and users will begin to obey the new rules that will dictate the government. We will inevitably get away from the insane anarchy of unregulated ICOs. A number of countries are already laying the groundwork for this to happen. While China and South Korea have preferred bans, Switzerland has released guidelines that build the legal framework for the ICO, striving to become the most cryptocurrency-friendly nation. Everything becomes more interesting. As soon as the bureaucrats give the green light to cryptocurrencies, companies of all shapes and sizes will not fail to take advantage of this. Naturally, the infrastructure will not lag behind: banks, commercial enterprises and service providers will catch up, and soon your grandmother will start buying Christmas crackers for bitcoins. The lights are muffled, and you better take a seat in the front row. Perhaps mass recognition will take months and even years, but the cryptocurrency is the star actor in the show, which definitely deserves attention.

II Chapter. BLOCKCHAIN IS A MODERN COMPETITOR OF CONVENTIONAL BANKING SYSTEM

2.1. Transactions of conventional banking system

Banking system is a set of banks operating in the country, credit institutions and individual economic organizations performing banking operations. In addition, the banking system includes specialized organizations that ensure the activities of banks and credit institutions: cash settlement and clearing centers, audit firms of banks, dealer firms dealing with securities of banks, organizations providing banks with equipment, information and personnel.

The established banking system has a two-tier organization. The upper level is the Central Bank (CB); lower level commercial banks and credit organizations. The Central Bank is decisive for the banking system, its activity allows regulating and controlling monetary relations in general, while maintaining the freedom of private entrepreneurship, which is ensured by the activities of commercial banks. Central Bank in all countries is the main link of the banking system, an institution that performs the functions of regulating the entire banking system (Dyer. W., 2006).

The bank, protecting and realizing the interests of the state, in general, performs the following functions: it carries out a monopoly issue of banknotes, thereby being a bank of banks; is a government banker; conducts monetary regulation and banking supervision. It also regulates the reserves of foreign currency and collateral, is the traditional custodian of foreign exchange reserves and performs numerous financial transactions at the international level: regulates international payments, balance of payments, participates in the operations of the world market of loan capital and gold, represents its country in international credit operations.

The main functions of commercial banks are:

1) mobilization of temporarily free funds of enterprises, organizations, the population and their transformation into capital;

2) crediting of enterprises, the state, the population;

3) cash management services to customers.

The conventional banks make millions of transactions per day. More than half of them directly concern their customers.

Virtually any operation - from the accrual of interest on deposits to complex intrabank actions with a currency - falls under the definition of "transaction".

Transaction (eng. Bank transaction, from lat. Transactio - agreement, contract) in general is any transfer using a bank account. A transaction process is reading information from a card that is processed at the operations center. The result of this processing should be the identification of the bank of the cardholder and the acquiring bank .

In the practice of credit institutions, there are several types of transactions:

- Banking transaction means making any operations related to the transfer of money between customer accounts.

- ATM transaction is a transaction involving the withdrawal of cash on a bank card using an ATM. This task is carried out for the purpose of receiving money or making payment for any services.

According to the method of implementation, the following types of transactions are distinguished (Gray J. and Reuter A.., 2006):

- Online transaction. Feature - carrying out the operation immediately (crediting of money, their cancellation or transfer). Such transactions include cash withdrawals through an ATM or transfer of funds within one credit institution.

- Offline transactions. Unlike the past type, here all calculations are made with a certain time delay. One example is banking transactions for the transfer of salary to the account of employees of the enterprise.

The most accessible option is transfer between accounts. In this situation, the size of the commission is 0.4-1.0 percent. Feature - in the possibility of participation of various banks in the process. These types of transactions are carried out in a short time and without delay on time.

Money transfer in any way is a transaction, regardless of the techniques. Transaction system includes:

- cash transactions with a plastic card and payment terminals;
- money transfer between bank accounts - is carried out by a bank employee;
- instant cash transfer, without opening an account - sent to the bearer of the passport and transaction code cipher, which the sender informs the recipient - WesternUnion, Contact, Golden Crown, etc;
- electronic banking - transactions within the electronic payment systems Qiwi, PayPal, Webmoney, etc.

As a final part of a banking operation, a transaction can be initiated by submitting a written order to the bank, by electronic order through Internet banking systems or other communication systems, as well as with the help of some payment instrument.

The most common case is a bank transaction for payment by a bank card in a trade and service enterprise. Such a transaction begins when the cardholder decides to pay for a product or service, and transfers the card (or pays for it himself) to the cash worker .

By means of a POS terminal, in order to authenticate the holder, the card information from the terminal is transmitted to the acquiring bank serving the terminal and having an agreement with the owner of the outlet. Depending on the agreement, the outlet pays the bank a fee for its participation in processing the transaction. Further the information us received by the acquiring bank.

Acquiring bank accepts payment cards as a means of payment for goods, works, services. It is performed by an authorized acquiring bank (English acquiring bank) by installing payment terminals (POS-terminals in the case of traditional merchant acquiring, mPOS-terminals in the case of mobile acquiring) or imprinter at commercial or service enterprises (TSP).

Picture 5. Transaction Process Cycle
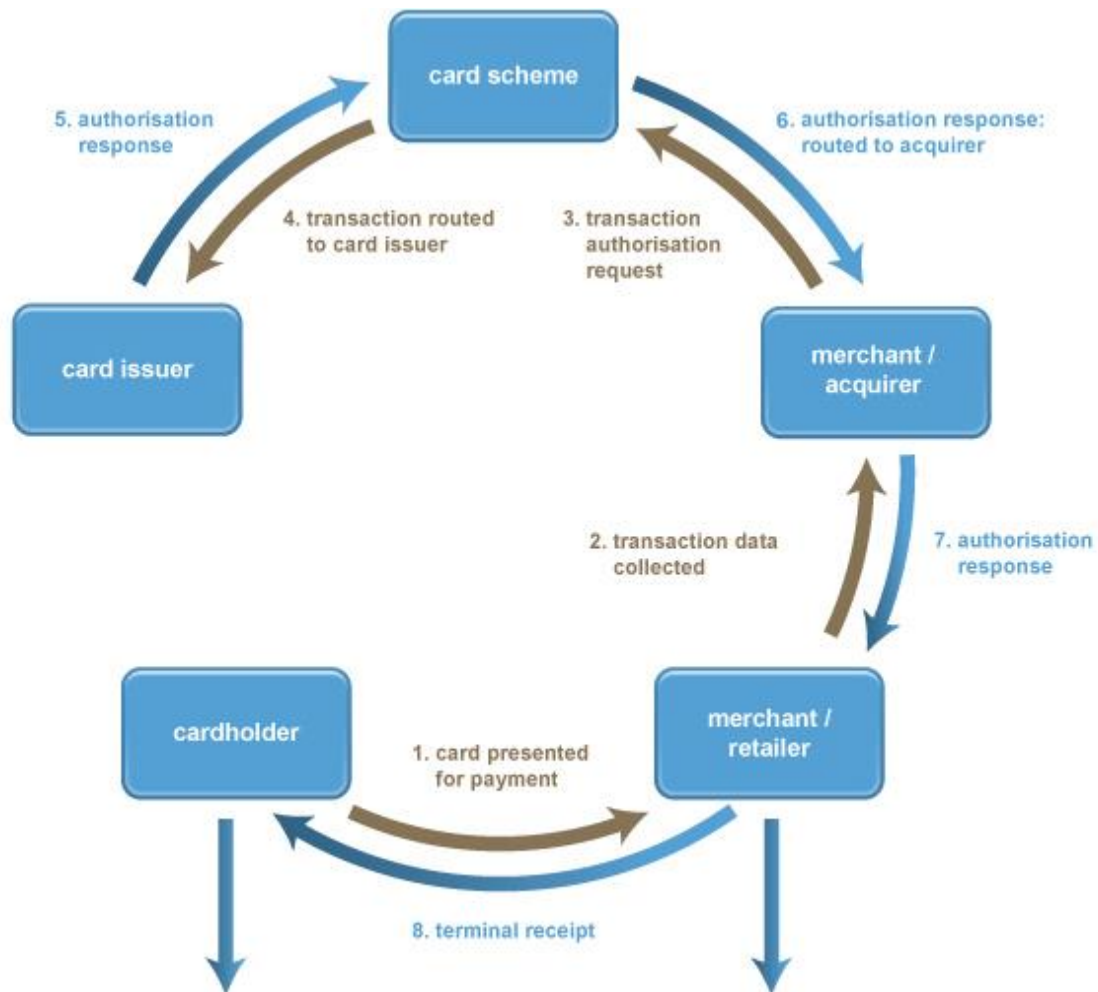
Source: Levin V.K. Information security in information systems and networks // Programming. - 1994.

Mobile POS-terminal or mPOS (from the English. Mobile Point Of Sale - mobile point of sale) is a compact device, which is a trading terminal connected to a smartphone or tablet computer, which allows to carry out cashless payments using a bank card. The main advantages are compactness, low cost and the ability to make

payments at any point where there is Internet access (including cellular communication). A device for reading information from a bank card (reader) is connected to a smartphone via a connector, most often a popular 3.5 mm mini-jack. Also, the reader can be connected via USB-connector or Bluetooth-connection. A program is being installed on the smartphone - the bank's mobile payment application. Services that provide acquiring services using mPOS terminals charge a fee. As a rule, the commission is charged in the range from 1.8% to 2.75% of each transaction (it may vary depending on the tariff policy of banks) (Dyer. W., 2006).

It is possible to accept payments from a bank card without a reader, by manually entering the bank card data directly into the bank's mobile payment application (virtual POS terminal).

Currently, there are more than 18 million trade and service enterprises in the world, where it is possible to pay for purchases using payment cards.

Most of the market for acquiring services is occupied by banks - members of Visa and MasterCard. American Express cards are also widely used in the USA. In Russia, the MIR payment system is being actively implemented.

There is also Internet acquiring - accepting payment for bank cards and electronic money via the Internet using a specially developed web interface that allows you to make payments in online stores and pay for various services (telephone, utilities, Internet access, etc.).

It is also customary to refer to the issuing of cash to bank card holders. Such issuance, as a rule, is carried out through an ATM or with the help of a specially configured POS-terminal (POS-cash point). This area also includes various self-service devices that accept cards.

Then the acquiring bank transfers information to the payment system that serves this card. There, the data gets to the operational center to which the banks participating in the payment system are connected. This center is checked for the presence or absence of payment card data in the stop list and, depending on the result,

it refuses the transaction or it is approved with a further referral to the issuing bank that issued this card and servicing the bank account / accounts attached to it customer.

Here it goes to the processing and authorization center, where advanced checks are carried out on the legality of the processed transaction.

A processing center is a legal entity or its structural subdivision providing informational and technological interaction between the participants of the calculations. The concept of a processing center, as a rule, is used to apply to organizations engaged in processing operations using plastic cards (Titorenko G.A., 1997: p.52).

Most of banks issuing bank cards create their own banking processing centers, which are structural divisions of banks that carry out information and technological interaction between the participants of settlements and ensure that the intrabank processing of operations with plastic cards is carried out. Each of the plastic card settlement systems imposes its own requirements on processing centers that process plastic card operations. For example:

- Visa International and MasterCard International - require certification by payment systems as a third-party processor.
- Diners Club International and American Express require payment systems licensing for technological support of operations.

Processing centers must also be licensed to provide information encryption services in international payment systems using bank cards and maintenance of encryption tools intended for use in international payment systems.

If fraud or violation of the terms of service has been suspected is given a refusal. Depending on the card type (debit or credit) and the authorization priority set by the bank, this may check the available balance of funds in the account or the payment limit, as well as verify the holder's PIN. If all checks are satisfied, the issuer approves the operation and within the framework of the transaction, also through the payment system, the answer is given in the outlet.

By mutual settlements with the payment system, the issuer transfers to the acquirer the amount of funds requested in the transaction, as well as the payment system commission for processing the transaction.

In turn, the bank deducts from the client's account the amount of money paid and confirmed by the client for payment (for debit cards) or reduces the available payment limit, thereby reserving part of the funds for subsequent debit (for credit cards). The transaction is completed at the time of receipt back to the sales point of response with approval or refusal.

Examples of similar transactions can be a set of actions when instructing a bank to transfer funds from one account to another or cash withdrawal at an ATM (both with and without a bank card).

In an offline transaction, an operation can be carried out without contacting the acquirer bank and the follow-up verification measures. This is valid for card accounts where the bank's available balance is pre-booked by the bank and information on the payment amount and card details remain in the memory of the POS terminal. Within the balance available on the card, funds are approved for write-off, but it happens much later after the terminal is connected to the communication channel and the accumulated information is transferred to the serving bank .

Secure Electronic Transaction (SET, Secure Electronic Transaction) is a standardized protocol for conducting credit / bank card transactions through unsafe networks (for example, the Internet). SET is not a payment system itself, but a set of security rules and protocols (digital certificates, cryptographic technologies) for authenticating transactions. This allows users to safely use credit / bank cards in an open network. However, SET has not gained popularity. VISA is now promoting the XML protocol 3-D Secure.

During the transaction, sometimes there are both systemic and technical failures. This means that there may be a faulty payment terminal, or problems on the

server. In this case, the funds from the credit card may have time to write off, or vice versa, the operation failed even before the cancellation.

So what if the transaction fails? It is necessary to immediately call the customer support service of the bank servicing the card and explain the essence of the situation. Depending on the complexity and nature of the failure, the problem will be solved in 2-3 days, and maybe everything will be delayed for some time, during which it is necessary to maintain a composure and wait for the resolution (Levin V.K., 1994: p.63).

If when sending money or making purchases with the help of modern payment systems there was a transaction error, you need to quickly take action.

If the details given are incorrect, the recipient's full name or the secret transfer code is lost, the problem is solved by the customer support service of this system. If you mistakenly entered the wrong card number of the recipient and the money "went the wrong way", here it is more difficult. It will be necessary to write an application at the bank and if, after his intervention, the "beneficiary" remains deaf, it will be necessary to settle the issue of the return of funds on his own, since there is a human factor.

2.2. SWIFT as a main interbank connector

The transfer of funds in foreign currency from current balance foreign currency accounts abroad in favor of foreign individuals and legal entities is carried out in the form of an import bank transfer.

A bank transfer is a bank order addressed to its correspondent about the payment of a certain amount of money on behalf and at the expense of the transferor to a foreign recipient (beneficiary) indicating the method of reimbursement to the paying bank of the amount paid by him.

To speed up transactions, reduce the cost of banking operations as a result of using messages that are unified in content and format, the SWIFT system is used.

Through SWIFT, banking operations such as money transfers, transfer of information on the status of bank accounts, confirmation of foreign exchange transactions, settlements under collections, letters of credit, securities trading, reconciliation of disputed issues, maintenance of electronic accounts of clients and their funds are carried out.

On May 3, 1973, in Brussels, representatives of the 239 largest banks in Europe and North America founded and registered a consortium of SWIFT (Society for Worldwide Interbank Financial Telecommunication) - a community of global interbank financial telecommunications designed to design, implement and regulate the international telegraph network financial transfers between members of this organization. Currently, over 4,000 banks from 70 countries participate in the SWIFT system (Lauts, E. B., 2008).

For these purposes, work was carried out to create and harmonize a standard language of communication between member banks of the community, which allowed for the automatic processing of incoming messages. Translations of some of these standards that have the status of an international standard are published in this edition.

The SWIFT system is based on three distribution centers in Brussels, Amsterdam and the state of Virginia (USA), which are equipped with dual processors.

Each of the processors separately can regulate the flow of incoming information. Each country - a member of SWIFT - has its own national hub (message hub), which is connected by telephone lines to one of the distribution centers and together with the lines is owned by SWIFT. Banks - members of the community, connect to the hubs on the local lines of communication of their country.

SWIFT rules require that its member organization "should be engaged in the same type of business as the others, and take part in international telegraph financial transmissions".

SWIFT is formally a Belgian cooperative society registered in Brussels. It is wholly owned by SWIFT member banks, and its shares are distributed in proportion

to the number of telegraph messages sent by the bank via the SWIFT telegraph network. Each member bank pays a one-time fee of 1.5 million Belgian francs upon entry into the organization of SWIFT. For connection to the regional processor (Brussels, Amsterdam, New York, Vienna, Copenhagen, London, Luxembourg, Milan, Montreal, Oslo, Paris, Stockholm, Frankfurt, Helsinki, Zurich) a one-time fee of 190 thousand Belgian francs was set. For the equipment of communications and training in their use (depending on the specific forms of connection of each bank) are charged about 700 thousand Belgian francs (Bratko A. G., 2006).

The SWIFT service tariff is charged quarterly to its members. A typical telegraphic message (delivery -20 minutes) containing less than 325 characters costs 18 Belgian francs. For urgent messages (delivery - 1 minute) the cost is 2 times higher. SWIFT member banks pay the cost of sending telegraph messages to the regional processor. (Tariffs are indicated for October 1978. At present, the size of the down payment depends on a number of reasons and ranges from 50 to 300 thousand US dollars, the cost of telegraph messages has also increased).

For the transmission of telegraph messages there are two sequences: regular and urgent. For urgent messages, you can specify the delivery time. All messages receive sequence numbers, numbering is monitored. The transmission of each message is confirmed by the password.

The SWIFT system makes it possible to carry out the following types of telegraph transfers (Kapaeva TI., 2006: p.24):

- client translations;
- bank transfers;
- debit and credit notices;
- foreign exchange transactions;
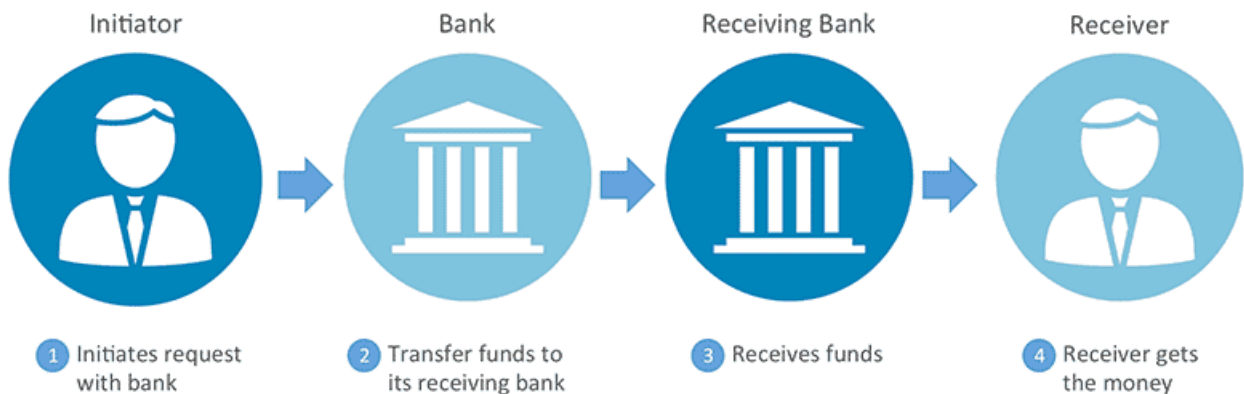- credit and deposit operations;
- interest payments;

- account statements.

For each type of message, a special format has been developed, which indicates the number of mandatory or arbitrary details in the message.

SWIFT does not make payments on transmitted wire transfers. The calculation is made by debiting or crediting correspondent accounts, i.e. the receiving bank debits the account of the sending bank and credits the account of the receiver of the telegraph transfer. If the receiving bank assumes the risk of a loss from a credit operation, it can pay the money to the recipient of the transfer, and later settle with the sending bank.

As an example of the use of SWIFT, below is a diagram of the main blocks of the mechanism of functioning of the telegraph transfer system.

Picture 6. The mechanism of functioning of SWIFT transfer system

| Initiator | Bank | Receiving Bank | Receiver |

1 Initiates request with bank
2 Transfer funds to its receiving bank
3 Receives funds
4 Receiver gets the money

Source: Frederick Mishkin. Economic Theory of Money, Banking and Financial Markets = The Economics of Money, Banking and Financial Market. - 7th ed. - M .: "Williams", 2006. - 880 p. - ISBN 0-321-12235-6 ..

1. Parties performing payment transactions.

They make decisions about transferring money in the name of the recipient party. Parties that make payment transactions may be corporations, institutions, banks, individuals.

2. Mechanisms of payment transactions.

The parties listed above give their banks appropriate telegraphic transfer orders either by telephone or in writing (telex, teletype, mail, fax, telegraph). At this stage, the most important thing is to verify the identity of the sender of the money transfer. Verification methods are directly dependent on the types of mechanisms used to compose instructions. Telex and teletype have return response systems and keys for comparing customers' signatures. Telegraph communication systems use keys to compare customer signatures, passwords and special forms of identification. Verification of orders issued by telephone, involves callbacks to the parties that issued the relevant instructions. On orders sent by mail, the bank must verify the signature of the parties that issued them.

3. Processing and delivery of payment.

The bank carries out a payment transaction through one of four telegraph lines: Fedwire, Bankwire, CHIPS and SWIFT. Usually, the banking connection with the telegraph network is carried out automatically, and each telegraph network has its own codes for making various payment orders. Thus, most banks at this stage of processing payment orders use two operators: one to enter data into the telegraph transfer system, and another - to verify the input data. Similarly, telegraph transfers that come to the bank are also processed by two operators: one - notifies the parties about their receipt, the second - makes entries on the accounts.

4. Notice of receipt of payment.

Immediately upon receipt of funds, the bank notifies the recipient (corporation, institution, bank or private person). Telegraphic transfer cash can be of two kinds, in the record of which telegraphic communication system was used to transmit it. Cash with payment on the same day or immediately upon receipt of the transfer can be received on the day specified in the payment order. Cash with payment on the next day or funds received from clearing houses can be received on the next business day.

Money transfers involve two different information flows.

- cash flow from the sender of the transfer to the recipient in the form of one or several payment orders.
- the flow of payment orders and information on payment transactions, starting from the party making payments, and continuing through notifications.

These flows can be very difficult due to the fact that financial institutions that are not part of this system will use the services of correspondent banks that are members of any of the telegraph money transfer networks to make wire transfers.

The SWIFT network is a data transmission system organized so that banks from different countries equipped with terminals of different models with different speeds can easily understand each other.

SWIFT messages contain fields identifying all participants in the transfer of information and payments.

Currently, there are 7 categories of messages that include more than 70 types. Each type of message is focused on the most complete and accurate reflection of the requirements for the presentation and sale of data that may arise in the practice of banks using these messages, that is, performing operations of this kind.

The message text consists of fields, some of which are mandatory, some fields are pre-numbered.

Required fields contain the information necessary to properly process this message. Additional information (for full instructions), if necessary, is located in the "optional" (optional) fields. Messages are usually transmitted from one SWIFT user to another (other), but there are also "system messages" that allow users to interact with the communication system (requests) and the system with the user (reports, etc.). Thus, system messages are used to request certain actions and receive special accounts, to search for messages in the database, for educational and training purposes. The SWIFT communication system can send inquiries and wait for user

responses or inform it about the state of the systems, its updates, new services, and so on (Kapaeva TI., 2006: p. 47).

All the specifics of the SWIFT system, as a system of financial interbank communications, is reflected in categories, groups and types of messages.

Each message consists of 4 components: header, text, certificate, end.

Thus, the header contains the eight or eleven-digit address of the beneficiary's bank, the sender's terminal code, the current five-digit number that performs the control and protection function, as well as the three-digit message code with a two-digit priority code.

The type of message is determined by a three-digit numerical code, with the first digit corresponding to the category of operation underlying the message. For example, a transfer on behalf of a client is indicated as 100, transfer, transfer at the expense of the bank's funds as 200, transfer of the bank at the expense of the third bank 202, confirmation of a currency transaction as 300. For encoding messages from the field of documentary collection, category 4 is used, for operations with securities - category 5, for letter of credit operations - category 7 and for special messages such as debit - credit - an advice and account statements - category 9.

Actually, the message text consists of a sequence of fields indicated by a two-digit numeric code. The meaning of some of these fields is given below:

32: Amount

50: Translator

57: The bank in which the account is maintained

69: Beneficiary

70: Assignment

71: For whose account and the amount of commission

72: Information transmitted by the bank

Depending on the type of message, certain fields must be filled in, others may be optional. However, some of them should not be filled in certain messages, for example, the interest rate in the transfer at the expense of the client.

The three-letter alphabetic code developed by ISO (International Organization for Standardization) is used to designate currencies. The first two letters indicate the country, and the last - the currency of the country concerned, for example, the DEM code is used to denote a German mark.

All messages are automatically encrypted as soon as they are entered into the communication network, which ensures the secrecy of information.

The message also contains a "certificate", which ensures that the text of the message has not been changed during the transfer.

The customer's bank informs the sending bank of the need to send a message and transfers the appropriate amount to it. When receiving a message, the recipient bank transfers this amount to the account of the settlement bank, the payments being made.

Settlements between the sending bank and the receiving bank are made using an account that opens in one of them for the other. Who for whom opens an account depends on the type of currency in which the calculations are made. If the payments are made in the currency of the state in which the beneficiary bank is located, then it will deposit the corresponding amount in the debit account of the sending bank in its bank.

On the contrary, if payments are made in the currency of the country in which the sending bank is located, then it opens the account of the receiving bank and provides it with a loan for the appropriate amount.

In some cases, payments go a long way than messages through intermediary banks, depending on the specific payment terms. Notification of correspondent banks about payments made special messages. If four intermediary banks are involved in the organization of communications, the messages identify the client bank, settlement

bank and the correspondents of the sender and recipient. At the same time, the identifiers of the sender and recipient are not indicated in the text of the messages, as they are in its header (Frederick M., 2006).

The technical infrastructure of the SWIFT system is represented by computer centers located throughout the world, connected by high-speed data transmission lines, which are allocated from state, national or commercial communication networks. The heart of the network - the systems are two processing centers: in Holland and the USA, which are connected to autonomous regional processors installed, as a rule, in each of the countries that have joined the system.

The regional processor performs the function of entering the SWIFT network. The messages accumulated in it are encrypted and sent via international communication lines to the operations center. SWIFT uses a variety of lines of communication (both national and commercial) on loan.

Here the corresponding verification is carried out: the correctness of the format of the documents, the dates and the addresses of the sender and the recipient, the status of the device that transmitted the message are verified. After this message is quoted in encrypted form. The copying procedure favorably distinguishes SWIFT from other electronic systems. For example, in the American settlement system, the transaction is considered completed after the funds arrive at the beneficiary's reserve bank. The SWIFT member (both the sender and the recipient) has the right for an additional fee to receive a copy of the doubts, messages for the implementation of the issues raised. After checking and copying a message via international communication lines, it goes to the regional processor of the country where the receiving bank is located, and from there to the bank (Macesich, G., 2000: p.47).

One of the main achievements of SWIFT is the creation and use of special standards of banking documentation, called upon by the international standardization organization. The unification of bank documents made it possible to avoid difficulties and mistakes that were caused by discrepancies in the traditions of their design in

different countries, difficulties of a linguistic nature. A considerable advantage of these standards is that their creators are at the same time their users, and, therefore, have the opportunity to improve them promptly. All kinds of incoming and outgoing documentation were reduced to approximately 70 types of formats, divided into groups by main types of operations. Thus, the group "operations with securities" includes 16, the group "settlements under collection" - 7, "settlements under letters of credit" - 18 kinds of documents. The advantages of SWIFT standards turned out to be so obvious for banking institutions that others similar (London CHAPS, French SAGITTAIRE, New York CHIPS) also adopted them, or created an automatic translation system of SWIFT standards into their own.

- bank terminal that is installed in a bank and is intended for access of bank personnel to the network. The terminals of the SWIFT system are usually a personal computer. Mounted equipment can be delivered on a turnkey basis or integrated into an existing banking system;

- regional processor (RP), the main purpose of which is to organize the interaction of users of a certain limited area (countries, groups of countries);

- slice processor (SP), necessary for the exchange of messages between the RPs connected to it, the short-term and long-term archiving of messages and the generation of system reports. The SWIFT system allows you to save information about transfers made within 4 months;

- System Management Processor (CCP), which performs the functions of a system monitor, system and network management. There are 2 PUS: one in Holland, the second in the USA. The CCP is the only level of the system, which is not busy processing messages, but is intended solely to control the SWIFT system as a whole;

Access to the system is as follows (Krahmalev SV., 2007):

Each message is assigned a consecutive input number when it is entered into the system and an output number - when it leaves it. Checks are performed on these numbers. If the input number is out of order, the system rejects it, disconnects the terminal from the system and requires a new identification by means of a code. Messages entered into the system with a departure from the standard protocol or format will be rejected.

The SWIFT system has advantages and disadvantages. First of all - the benefits:

Competitiveness. The international payment and credit turnover is increasingly concentrating on the participants and users of SWIFT. Banks that do not want to be forced out of international payment transactions must, for reasons of competitiveness, join SWIFT.

Security. The security of the transfer, that is, protection against fraud, loss and unanswered payment orders and financial messages, is significantly enhanced by the presented system. In addition to the security programs used in computer centers and SWIFT hubs (access control, machine room control), some special security measures are built into the system that guarantee its greater degree compared to the traditional balance of payments. In particular, these include (Rudakova O.S., 2009):

- verification of permitted use of system terms at the beginning and at the end of the system itself;
- automatic numbering of all incoming and outgoing messages in the prescribed order, the numbering order is controlled by the system itself;
- automatic transmission of messages between two banks through the establishment of the relationship on an individual key;
- automatic verification of information in the receiving bank.

Protection of communication lines by SWIFT operational centers and national regional processors, through the use of special coding devices based on random number generators, which make messages inaccessible to unauthorized persons.

Thus, a complete SWIFT security environment consists of a multi-level combination of physical security, transmission line security, operational security and procedural security.

For the sake of greater security when sending messages, the line connecting the SWIFT member bank and its regional processor can be protected by the bank.

Rapidity. The speed of transferring messages using SWIFT improves the ability to accelerate the relocation of funds for banks and their customers (on a daily basis, 600 thousand payments are checked accordingly.

Sending a payment order from Frankfurt to New York, for example, in the normal message mode, takes less than 20 minutes, in the urgent message mode, it takes about 5 minutes.

Messages sent via SWIFT, as a rule, reach their destination faster than via a normal telex, since the number of intermediate stations by telex is larger.

Other advantages of SWIFT are the possibility of sending messages in priority, searching messages sent 10 days ago and receiving telegraph banks.

The advantage of the SWIFT system is responsibility within the system. SWIFT creators installed rules that allow individual members to make claims for damages to SWIFT or to another participating institution in certain circumstances.

In particular, the circumstances are determined under which the sending bank, the receiving bank or one of the parties. This is especially true for SWIFT if the message was acknowledged to the sender, but not transmitted to the recipient. An error of the system or its personnel is considered such a situation when the member banks are not immediately informed about errors in other banks, operating centers or regional processors (Suren L., 2007: p. 45).

Opportunities for rationalization within the bank - another advantage of the system. After transfer via SWIFT, received payments and financial messages can be immediately processed by a computer without prior manual processing. On the other hand, any transaction offered as a SWIFT message (for example, confirmation of a currency transaction, payment order, etc.) can be immediately and automatically turned into an outgoing message.

Another significant economic effect can be obtained by improving the control over the balances of nostro accounts and speeding up the relocation of funds on the accounts, which is achieved by quickly transferring account statements through SWIFT.

In order for these rationalization opportunities to be fully realized, it is necessary to reorganize the labor process in the relevant divisions of the bank. Such changes require a significant investment of time and labor, and can be carried out gradually, for example, first in the currency operations department (confirmations and payments), then international settlements, and reconciliation of nostro accounts.

Unfortunately, this system is not without flaws. One of them is, to a certain extent, the dependence of the internal organization on a very complex technical system and the associated technical problems and failures can be just a disadvantage.

However, the high costs that burden small banks most of all are of much greater significance. Although using SWIFT can reduce costs as a result of system-related rationalization, these benefits are usually difficult to measure and compare to large costs.

Another drawback is the reduction in the ability to use a payment credit (for the duration of the document run). The resulting SWIFT reduction in processing time and mileage of documents reduces the gap between the debit and credit of the accounts on which this transfer is reflected.

Summing up all of the above, I would like to note that the need to enter foreign banking systems (in particular, SWIFT) is associated with modern conditions for the development of the banking sector.

The solution to this problem should begin and today it takes place in all banks - the Client-Bank complex, which is based on an agreement.

The most advanced step in the automation of a commercial bank is the SADKO system, which includes the MARS interbank automated settlement system. According to experts, this system can be called the domestic equivalent of the SWIFT system.

2.3. Advantages of blockchain as non-intermediate system

The use of the latest information technologies in all spheres of human activity opens up new opportunities for optimizing business processes. What seemed incredible 15 years ago, such as online payments, e-banking and virtual currencies, became part of our daily lives. One of these technologies has become the blockchain.

Initially, this technology served as a distributed database for storing and executing transactions in the Bitcoin system, but its scope is much wider.

A distinctive feature of the blockchain is the lack of a single centralized database for data storage. All data is distributed between interconnected blocks, chained together through complex algorithms. In addition, each block stores its own piece of information. New blocks are added to the end of the chain and cannot be changed after validation. This circumstance provides a high level of security and resistance to hacker attacks. At the same time, it is worth highlighting other advantages of the technology under consideration (Timothy W., 1997: p.36):

- transparency of transactions that can be tracked by all network participants in real time;
- the ability to control availability levels;
- speed of transactions;

- automatic validation of blocks after confirmation of the transaction by the user.

The address of the wallet looks like a random set of letters and numbers. In fact, this is an encrypted identifier that is unique to each participant in the system and is used to send money to the wallet owner

Transactions as mentioned above are records of completed actions that are stored in users' wallets.

Each block in the chain stores data about the previous and current blocks, which, in turn, forms a whole chain.

Through the use of solutions based on blockchain technology, financial structures can receive a number of advantages:

- cheaper and faster international money transfers. The cost of a traditional international transfer is about 5-20% of the amount transferred. Blockchain allows you to reduce this figure to 2-3%, making the process itself much faster.
- smart contracts are programs that automatically verify and facilitate the implementation of agreements.
- user identification. Network members enter personal information about themselves. This information is used to enhance transaction security.
- stock trading. In the long run, technology can replace brokers and decentralize the stock exchange.

Other sectors in which Blockchain can be used:

- shipping The technology eliminates the need for numerous intermediate structures.
- the property. Automating the verification and execution of contracts will greatly simplify the execution of agreements.
- blockchain can be used to obtain certificates and confirm diplomas.

- new technology will ensure the safe and fast exchange of confidential medical information between institutions.

Many financial companies have already invested or plan to invest in the use of blockchain technology. On the one hand, the blockchain offers many opportunities that can permanently change our usual way of exchanging values. On the other hand, it is perceived as a threat to the existing trade model. Changes are always difficult, especially when it comes to global scale. However, the potential of the blockchain makes it clear that transformation is inevitable.

The leading organizations - Deutsche Bank, the US Federal Reserve, Barclays Bank, Citigroup - are already using blockchains. One of the reasons, of course, is the so-called FOMO (Fear Of Missing Out) blockchain - the fear of losing leadership positions. According to PwC, 90% of banks in North America and Europe spent more than $ 1.4 billion on blockchain in 2016. However, the scale of the introduction of this technology has not reached mass. In fact, a significant number of banks and insurance companies were dissatisfied with the results, so they postponed this decision for later. Will the organization return to the blockchain implementation? Recent events in the financial sector give reason to say that they will return.

Bank BBVA became the first financial institution in the world to provide a loan of 75 million euros using blockchain technology. In addition, they presented the blockchain strategy, which is based on three main elements: implementation, ecosystem and experience. The bank is working on building blockchain solutions that will provide a full digital cycle of interaction with customers. In addition, they plan to promote the development of expertise, regulatory framework and explore the impact of decentralization on the system as a whole. The company also plans to launch a blockchain academy to teach employees the basics of working with new technology and prepare for changes in the future (Krahmalev S.V.,2007: p.45).

By structure, the blockchain is a network of peer computers that can communicate with each other. The system consists of a chain of blocks that store

cryptographic data about transactions, agreements, contracts. Such networks can be both public (each participant can write and read data) and private (the rights to verify transactions belong to certain participants). The blockchain provides all business members of the network with equal access rights to the overall transaction history, which can in no way be changed after confirmation. This technology can significantly simplify traditional banking operations - reduce the time for processing and at the same time the cost and the number of cases-exceptions to the rules. Transactions that are carried out using blockchain technologies have four main advantages: reliability, transparency, speed, and economic efficiency.

It is important to understand that blockchain technology is not a universal approach that can solve all problems. However, there are four main areas in which a blockchain can be an indispensable solution.

The financial sector is increasingly suffering from fraud and cyber attacks. The point of vulnerability is located primarily in centralized databases, when all information is stored in one place. Unauthorized intervention can cause a lot of harm to such bases. Blockchain significantly reduces the risk of interference due to database decentralization. Since there is not one, but many nodes with information, it becomes much more difficult to penetrate, since it is necessary to attack them separately.

In the banking sector, there is the concept of Know Your Customer. It means that companies working with private finances must identify and identify the counterparty before conducting the transaction.

According to the Thomson Reuters Survey, financial institutions spend an average of over $ 60 million annually on customer identification and verification. The purpose of this procedure is to track who banks work with and prevent potential financial terrorism and money laundering. Another important reason for identifying a client is to verify compliance with the requirements in order to avoid administrative fines. Blockchain can help significantly reduce transaction costs in this direction. This

can be achieved by storing information about trusted customers in the blockchain node, to which other banks, insurance companies and accredited organizations will have access. Thanks to this approach, companies will not have to spend time identifying a client from scratch.

Trading blockchain platforms avoid the need for centralized identification or the presence of intermediaries. In the case of securities transactions, you can also reduce the risk of double costs. Such trading platforms work with digital tokens that can be placed and tracked transparently on the exchange. Since the digital token acts as a certificate of authenticity, the chance to earn extra money is significantly reduced compared to physical versions.

Using blockchain technologies to make payments between various financial institutions and customers can significantly reduce the costs of banks. In addition, it can increase the level of security and speed of domestic and international payments.

A few months ago, the Batavia blockchain trading platform, founded by the UBS giant together with IBM, has already conducted the first real cross-border transactions. During the pilot launch, two operations were carried out: the sale of cars from Germany to Spain and textile raw materials from Austria to Spain. In the process, a link was established between all parties (suppliers, buyers and financial institutions) necessary to conduct transactions.

Despite the potential, the use of blockchain technologies does not guarantee a 100% solution to the above-mentioned business problems. When creating blockchain solutions, a financial company may encounter many factors - changes in the market situation, the number of financial transactions, or regulatory changes. All this can also unpredictably affect the system, so we must be ready for possible challenges.

In addition, since blockchain solutions are used on a massive scale, it is very important that the system can be scaled while maintaining efficiency. Today, according to TechInAsia, this issue has not yet been fully resolved. For example, the popular Ethereum blockchain platform can, on average, conduct about 10 transactions

per second, while the financial giant Visa performs 5-8 thousand transactions over an identical period of time. It is obvious that such a difference in the number of operations carried out imposes certain restrictions. But the situation will change very soon. Companies developing blockchain technologies are already working on solving this problem. Over time, they will offer an infrastructure that can scale. This will allow massive use of blockchain platforms (Oliver, J. 2008: p.45).

Probably, there is every reason to talk about a revolution that will completely change the industry we are used to. Old processes and mountains of paper documents will be replaced by digital innovations that are based on the principles of cooperation and trust. Frauds and scams can become a thing of the past thanks to highly secure systems.

At first glance, the introduction of the blockchain can look risky and dangerous for the financial industry, where even a minor problem can cause losses of billions of dollars. However, after analyzing the scheme of work and the potential of the blockchain, it is safe to say that the changes are already inevitable, as are the opportunities that the blockchain brings with it. It is only a matter of time, as well as effective cooperation of financial organizations to build a global infrastructure.

Digital transformation affects all industries, but some of them adapt to new conditions faster. The financial services industry has always slowly adapted to change, but in the near future an unprecedented transformation awaits it. Recognition of the concept of Open Banking in the legislation of the UK and the European Union will radically change the way we interact with customers, with the result that financial advice will become more accurate and personalized.

According to the Open Banking concept, all large banks must provide all their customers' data in a standardized format so that they can be used by accredited third parties with the permission of customers. This radical change in the way the banking system functions will make it possible for customers to manage all their bank accounts through one smartphone application. In addition, comparison services will

be able to use the financial data of users to offer them personalized advice from banks and services. Probably, banks of other countries will also have to introduce the Open Banking standard in the future (Timothy W., 2003: p.547).

For enterprises, the emergence of 5G, AI, machine learning, integrated registries and other new technologies will significantly accelerate the introduction of innovations. All these technologies will unrecognizably change the future of finance in the next few months. This is especially true of distributed registry technology, which can drastically change the banking sector.

A distributed registry is a database that tracks ownership and thus provides a permanent record of transactions that cannot be faked. In addition, validation of a distributed registry is performed directly by the network, so there is no need for a centralized control authority. The most well-known distributed registry is the blockchain, since it lies at the heart of the bitcoin cryptocurrency *. And although it remains to be seen whether virtual currencies like Bitcoin will become an integral part of our life, the blockchain technology has already practically entered our life.

The fake-proof audit trail, which provides blockchain technology, can radically transform various areas (for example, fraud detection and tax collection), and in the future can even be used for online voting. However, the full potential of this technology will manifest itself in the field of finance. Although the banking sector has always slowly adapted to the digital era (mainly due to outdated systems and the need to work with a large number of documents), the introduction of the blockchain is intended to radically change the traditional banking system and save a lot of time and money. Indeed, this technology will save investment banks $ 12 billion a year, according to an Accenture * report (Zhukov E.F., 2007: p.45).

The blockchain provides banks with two main advantages: reducing costs by optimizing and speeding up the execution of operations. This is especially true for international trade settlements, which are usually carried out rather slowly, as well as for servicing individuals. The British bank Santander UK * is already using

blockchain technology to speed up international payments through the bank's application. And the American bank American Express * recently merged with Santander Bank to provide the possibility of international payments based on the blockchain through the Ripple * financial startup platform. In addition to saving time and money, the blockchain will help reduce the number of cases of financial fraud, since the methods used by cybercriminals cannot bypass this new technology.

It should be noted that the blockchain's capabilities are not limited to monetary transactions - distributed registries can store any digital information, such as smart contracts. This advantage can benefit companies from various industries that conduct financial transactions. So, you can add program code to perform certain actions as soon as a predefined set of criteria is completed. For example, to pay the invoice after the job or delivery of goods. Blockchain technology can also be used to streamline the identity verification process.

Now almost all international banks are implementing the blockchain in an experimental mode, but companies from other industries can take advantage of this technology. For example, Oracle * has launched the Oracle Blockchain Cloud Service based on Intel technology for enterprise customers using the Oracle Blockchain Cloud Service. The service runs on a platform of scalable Intel Xeon processors, which are equipped with features to improve the security and performance of the blockchain. "Semiconductor and software technologies, as well as security technologies developed by Intel, can improve blockchain security and scalability," explains Doug Fisher, senior vice president and general manager, Software and Services Group, Intel.

In addition, Intel and Microsoft * are working on creating a new Cocco Framework for corporate clients. The platform will integrate Intel® Software Guard Extensions (Intel® SGX), which provide additional levels of protection for personal and sensitive data by encrypting transaction data, which also improves scalability. In addition, the new platform also promises to increase the speed of operations and will

allow developers to create flexible distributed registries with which it will be convenient for companies to work.

Since the blockchain is designed to transform the financial sector, it will be necessary to create a new regulatory framework to regulate the widespread introduction of this technology. Successful implementation also depends on the adoption by companies of a single set of rules, which, first of all, should describe the principles of personal and confidential data protection. This will take some time, but the blockchain already has the potential to completely change the scope of financial services, as well as other industries, including health care, manufacturing and retail

III Chapter: APPLICATIONS OF BLOCKCHAIN IN FINANCE

3.1. Experience of developed countries in implementation of blockchain in Finance

Today, far-sighted specialists all over the world are thinking about what the new protocol is leading us to, which allows mere mortals to trust each other through thoughtful code. History does not know anything of the kind: reliable transactions directly between two or more parties, verified and confirmed by joint efforts of the masses of participants and controlled by the personal interests of the entire team, and not controlled by large corporations that are chasing profits.

Perhaps such a protocol is not called Almighty, but a reliable global platform for our transactions is something daunting. It is called the Trust Protocol.

This protocol underlies an ever-increasing number of worldwide distributed registers, the so-called blockchains (or chains of blocks), the largest of which is Bitcoin. Behind the complex technology and inappropriate word stands, however, a simple idea. Blockchains allow us to send money safely and directly from me to you, bypassing the bank, credit card issuer or PayPal.

This is no longer the Internet of information, but the Internet of values or the Internet of money. It is also a platform that allows everyone and everyone to know the truth - at least in terms of structured fixed information. Speaking quite simplistic, this is open source: anyone can freely download and use it, as well as develop new tools for managing network transactions based on it. Thus, it has the potential to create countless new applications and opportunities that are not yet open, which can change very, very much .

In the minds of the average user, the word "blockchain" ("chain of blocks") is quite closely related to the term "bitcoin", which is reflected in the correct perception of the first term.

On the one hand, the popularity of Bitcoin is of interest to the blockchain, on the other hand, in the mass consciousness, Bitcoin is often associated only with something negative, forbidden and subject to prosecution by lawmakers.

A blockchain is a tool with which you can store transaction data (database). An instrument cannot be obviously good or bad: the instrument is the same, the application and the consequences are different.

Blockchain is a technology that constantly records transactions so that information cannot be erased later, but can only be consistently updated, in fact, an "endless historical trace" is preserved.

Blockchain technologies are catalysts for tremendous changes that will affect management, lifestyle, traditional corporate models, society and its global institutions. The introduction of the blockchain will be coupled with resistance, because this is a fundamental, global change.

Blockchain technology can change not only everything related to money markets, payments, financial services and economies, but also all other industries and, moreover, almost all areas of human activity. Blockchain is a fundamentally new paradigm that allows you to organize activities with less effort, more efficiently and much more widely than other existing paradigms. Decentralization as a general model can work effectively if there is a flexible universal network that allows you to perform transactions without intermediaries (https://coinspot.io/world/glava-mvf-predlagaet-borotsya-s-kriptovalyutnymi-riskami-s-pomoshhyu-blokchejna / (appeal date 03/14/2018).

Some scientists argue that the invention of double-entry bookkeeping led to the emergence of capitalism and nation-states. A new digital register of economic transactions can be programmed to preserve almost any valuable and important information for humanity: birth certificates, marriage and death certificates, property rights, higher education diplomas, financial reports, medical records, insurance claims, voting votes, origin Products - any information that can be presented in the form of a code.

Examples of operations performed using blockchain technology:

• In the spring of 2016, work began on a blockchain-based land cadastre project for Georgia. The use of the blockchain will increase the level of security and speed up the process of remote processing of documents, and the cost of registering rights to land is also expected to decrease from an average of $ 50–200 to 5–10 cents;

• In the fall of 2016, an Israeli startup (Wave), a British bank (Barclays) and an Irish manufacturer of milk (Ornua) conducted a letter of credit of $ 100,000 (previously the process would have taken a week or more due to bureaucracy and verification of all documents, but thanks to cryptography and automated verification of everything about everything took about four hours);

• On December 21, 2016, Alfa-Bank conducted a transaction letter of credit through the blockchain and S7.

The Central Bank of the Russian Federation, together with the major banks of the country, created the Masterchain platform, the goal is to increase the transparency and efficiency of existing financial systems.

Masterchain is a tool for interaction between financial market participants using the technology of distributed registries. It allows you to make payments online, quickly confirm the relevance of data about the client or transaction, as well as quickly create financial services. In addition, the masterpiece accelerates the exchange of information between counterparties and provides the necessary level of confidence during financial transactions, noted in the Central Bank.

Masterchain will be developed in the framework of a consortium for the study of financial technologies created by the initiative of the Central Bank. In the future, it is planned to consider the use of the masterpiece prototype as an integral part of the financial infrastructure of the new generation.

Qiwi, Sberbank, Alfa-Bank, Otkritie Bank and Tinkoff Bank took part in the creation of a new technology, the press service of Sberbank specified.

"We plan to try to organize the transfer of value, for example, transactions in the field of corporate lending," - said in the bank "Discovery".

"The use of blockchain technology is intended to increase the speed, transparency and efficiency of the new generation financial systems. A significant reduction in infrastructure maintenance costs is also expected due to its distribution among the participants. At the first stages of implementation, technological changes will have little impact on user experience, the technological component will remain for customers" behind the scenes "" - say representatives of Sberbank.

In the bank "Opening" note that the masterpiece opens for banks a new frontier in technology.

"We have reached the turn of the technological possibility of realizing the re-use of the results of customer's identification of one bank by another bank without the need to visit the office. In fact, the system provides a technological opportunity to record the event that one bank performed the identification, and the other can reuse and accept customer data digital channel (for example, through a mobile application), "said the bank.

Pavel Chebotarev, head of the Binbank Group's innovative development center, adds that using the new Russian service masterchain will help the bank in working not only with individuals, but also legal entities; in creating products and technologies that use remote customer identification; as well as in the exchange of information between financial market participants .

One of the first applications of the blockchain technology that is not related to cash settlements is the fight against Internet censorship with Namecoin, an altcoin used for registering and checking addresses in the domain name system (DNS). Namecoin is an alternative transnational DNS that governments and corporations cannot control. The advantages of a decentralized DNS are that it allows you to freely publish information on the Internet to anyone who is threatened by the pressure of local authorities and censorship.

Can the blockchain solve the problems of international economic assistance? The earthquake in Haiti in 2010 was one of the most devastating natural disasters in history. According to various estimates, from 100,000 to 300,000 people died. As a result, the country's leadership did not cope with its responsibilities in this situation. The global community donated more than $ 500 million to the Red Cross, a well-known international organization. The investigation revealed that the funds were spent for other purposes or disappeared altogether (David C., 2009: p.45).

Blockchain is able to improve the provision of international assistance by eliminating intermediaries who have funds along the way. And also, being an immutable register that records the movement of funds, the blockchain will make institutions accountable to the ordinary user. Imagine that you can track every dollar that you donate to the Red Cross, from the starting point (on your smartphone) to the end point - the particular person who was helped by your money. You could conditionally deposit your funds so that the new amounts are automatically transferred when the Red Cross performs each of the agreed tasks for which the money is collected.

The blockchain technology will allow items to collaborate, exchange units of value - energy, time, money - and rebuild logistics chains and production processes in accordance with the information available to them about the needs and capabilities of all elements of the chain. Already, smart devices can be assigned metadata and program them so that they recognize other objects according to their metadata or react in a certain way to specified circumstances, and without the risk of error or outside interference.

Speaking at a meeting of the collegium of the Federal Service for State Registration, Cadastre and Cartography (Rosreestra), the head of the Ministry of Economic Development Maxim Oreshkin spoke about a pilot project that will allow thousands of real estate transactions to be recorded monthly using the blockchain.

According to M. Oreshkin, "nowhere in the world is there a full-fledged working system for recording rights on the blockchain," and Russia is leading in this area.

In July 2017, Nikolay Nikiforov, head of the Ministry of Communications, spoke about plans to use the blockchain when concluding real estate transactions, speaking at the St. Petersburg International Economic Forum.

In October 2017, the Ministry of Economic Development proposed to conduct an experiment with the introduction of the blockchain into the real estate registry. Among the stated objectives of the experiment is to guarantee the protection of property rights and increase the availability of data in the registry.

The blockchain technology is already radically transforming the mechanisms of government and makes it possible to make them more productive and more advanced and cheaper. It also creates new opportunities for change in democracy itself, allowing the government to become more open, free itself from lobbying control and act in accordance with the four dimensions of business ethics. We can already see how the blockchain technology can change the role of a citizen and his participation in the political process: from voting and access to social services to solving the chronic problems of society and ensuring the responsibility of elected politicians for their election promises.

The EU Parliament has been thinking about the implementation of elections to public authorities through the blockchain.

The European Parliament has not yet discussed this concept. This application of technology has already been discussed for public and private needs, based on the idea that the blockchain with additional software will allow users to vote for distributed decision-making.

"Many experts agree that the introduction of electronic voting would require a revolutionary change in security systems. The debatable question is whether the

blockchain will be transformed or simply grow with time, and how its introduction will affect the future of democracy"

The proof of work algorithm that underlay the original development of Bitcoin was even described as one type of "vote" for which transaction chain would be the longest, and therefore, correct.

Futarhia is a two-stage process that allows you to first vote for the overall result (for example, "increase GDP"), and then vote for proposals that allow you to achieve this result. At the first stage, ordinary voting is held, at the second stage, forecast markets are used. Voting in forecasting markets can be conducted using various cryptocurrencies (EconomicVotingCoin or EnvironmentalPolicyVotingCoin) or other economically significant tokens. In essence, this is investment and speculation, a bet on one or the other side, which is expected to win. For example, you can buy a "contract to invest in new biotechnologies" if you think that it is better to achieve the result.

"Higher GDP" than other contracts, such as an "agricultural automation investment contract".

Like the idea of voting using random sampling, the concept of futarchy can be implemented using blockchain technologies that ensure scalability, decentralization, reliability, pseudonymity, and registry maintenance. The idea of futarchy, which was proposed by economist Robin Hanson, and Vitalik Buterin, the founder of the Ethereum project, translated into context of the blockchain, can be briefly described with the phrase "vote for the result, put on conviction". This example clearly demonstrates the transformative potential of blockchain technologies. It is possible that such models of voting and indication of preferences, as a two-tier structure of futarchy, will become the norm and will be widely used as a mechanism for making all complex decisions involving a large number of people. This can lead to a completely new level of coordination of human activities, much more complex than it is now. Of course, any new government structure, including futarchy, is abusive.

The managing director of the International Monetary Fund, Christine Lagarde, said that governments and state banks should cooperate in creating a legislative base for the circulation of cryptoactive assets. The creation of such a base, according to K. Lagarde, will prevent the conversion of cryptocurrency into an instrument for money laundering and terrorist financing.

K. Lagarde noted that the blockchain technology behind cryptocurrencies offers promising innovations that can increase access to financial services. New, cheap payment methods can help millions of people in low-income countries, where the majority do not have access to traditional bank accounts.

Greek Finance Minister Janis Varoufakis may have become one of the first high-ranking political leaders studying the use of blockchain payments in the national economy. At the height of the financial crisis in Greece, he developed a plan to create a parallel payment p2p system based on the blockchain. He emphasizes:

"I have never been impressed by Bitcoin itself, but from the very beginning I said that blockchain is a wonderful solution to many problems that we could not even imagine."

He proposed to create an alternative p2p-payment system based on the blockchain. This was supposed to save Greece from financial intermediaries in receiving money from the troika or other money markets. However, in the event of a cessation of the receipt of money from the troika, J. Varoufakis should have created a parallel payment system in order to ensure the payment of taxes by citizens and companies of Greece. And this was supposed to be a new form of money - what he eventually called fiscal money (Ruzakova OA, Grin E.S., 2017).

One of the most revolutionary aspects of this unrealized plan was to allow the state to borrow directly from citizens or businesses and vice versa. In fact, J. Varufakis tried to use the blockchain in order to take away the role of intermediaries from European credit authorities and to build new credit relations between citizens, companies and the state.

Theoretically, such a system could be bogged down in corruption and reduce public confidence in the authorities, although, according to Varoufakis, in Greece this could happen "on a very limited scale". For example, the Greek authorities could abuse these tax credits, distributing new fiscal money among allies and friends. It was here that Barufakis saw the potential of the blockchain: "The payment system on the blockchain would allow combining anonymity and transparency on the total total size of cryptocurrency transactions. As we know, the blockchain successfully solves the trust problem.

Creating a registry of intellectual activity based on the blockchain platform will create the possibility of legal use of content. At the same time, before introducing such a registry, it is necessary to develop criteria for its creation, to ensure technical testing, and a balance of interests between right holders and users. The creation of such registers is especially important due to the rapid development of social networks (Instagram, Vkontakte, Facebook, Odnoklassniki), in which any files are constantly exchanged. Thus, it is necessary to carefully consider the creation of a registry based on blockchain technologies, in which users should be able to legally use the results of intellectual activity, and rightholders should receive a reward for such use.

Entrepreneurship is vital for economic development and the prosperity of society. The Internet was supposed to free up entrepreneurs by giving them the means and capabilities of large companies, but not their problems, such as inherited culture, the ossified work processes and the heavy ballast of the past. However, the loud successes of the dotcoms, who made their owners billionaires, disguise an unpleasant truth: in many developed economies, entrepreneurship and the emergence of new companies in the last thirty years have been in decline. In developing countries, the Internet has barely reduced the barriers for potential entrepreneurs who are forced to fight suicidal government bureaucracies. The Internet has not given billions of people access to the financial instruments necessary to start their own business. Of course, not everyone is destined to become an entrepreneur, but even the average person who

is trying to earn a decent income is hampered by the lack of financial instruments and the domination of government restrictions.

3.2. Future of blockchain system in world finance system

Even years after the beginning of the spread of the Internet, people did not take it seriously. Since then, the network has firmly entered our lives and has become an environment where we communicate and buy goods and services. Moreover, it now has a significant impact on the political life of many countries.

As in the case of the Internet, cryptocurrencies are developing after the key technologies for this area - now it is a new open architecture of the blockchain. It is also decentralized and also based on several open protocols, using which companies and individuals can create products and services.

In my opinion, the potential of the blockchain technology depends entirely on how common it is in the world of ordinary people. At the moment, the recent success of Bitcoin has helped it stand out. However, only this year Bitcoin and cryptocurrencies slowly faded into the background, and, finally, it was the blockchain that interested investors.

Already in the first half of the year, blockchain startups in the amount earned about $ 240 million in profits from venture investors, so we can see that the technology is rapidly gaining momentum.

This year is likely to be a continuation of the trend in the market, aimed at innovations and global changes in the financial world. Below we will present the forecast for the blockchain, denoting possible major events in the industry this year.

Despite the fact that while the blockchain is mainly used only in the world of finance, we will soon see a rapid expansion of the sphere of influence of this technology. Now, we can observe the blockchain penetration into the healthcare industry. IDC Health Insights predicts that this year more than 20% of pharmaceutical organizations will have to go to blockchain projects, so for 2018 the technology will

expand its influence so that by 2020 a huge number of corporations will have their operating blockchain (Lisitsyn N., 2018).

As in the early stage of Internet development, there are now many competing technologies at the same time, therefore, speaking of the blockchain, it is worthwhile to clarify which particular implementation is being discussed.

There is one more parallel: when everyone uses the same network, technology brings the most benefit, so in the future we will probably talk about a particular blockchain winning this race.

People can consider Bitcoin as a prototype of a new, decentralized financial system. Yes, its current possibilities are limited (for example, while there is a small amount of transactions in it compared to conventional payment systems), but its code describes both regulations and economic laws at the same time, and in this sense it offers an opportunity to look into the future. For example, in order for an operation to be accepted in a bitcoin blockchain, it must satisfy certain rules.

Bitcoin simply does not violate the rules, automatically checking transactions for compliance, and in the event of a violation (for example, the absence of a valid digital signature), the transaction is rejected by the network.

In the field of financial instruments, Bitcoin, being the first mass cryptocurrency, has definitely shown how to play by the new rules without intermediaries and control from above. Even the "monetary policy" of Bitcoin is written in its code: new money is issued every 10 minutes, and the offer is limited, more than 21 million bitcoins will never appear - this is similar to the gold standard (i.e., a system in which the money supply is tied to the goods, and not determined by the government).

Nevertheless, it is difficult to argue with the fact that Bitcoin is an completely implemented technology: the network works, people attribute real economic value to Bitcoins, and all the miners who support the blockchain, and the authors of programs for users, without exception, follow its rules.

Blockchain maintains a reliable, albeit fairly simple payment system, and successfully resists attacks. And the opportunities that blockchain use promises to our financial system can simultaneously be a cause for both optimism and pessimism. Unfortunately, the enthusiasm of investors is somewhat ahead of the actual development of technologies - it can often be seen that the word "blockchain" is used as a fashionable label pasted on quite traditional databases.

In the pre-Internet era, there were many players, including telecom operators and cable television providers, who tried to create interactive multimedia systems based on their networks, but none of them gained popularity, and their names have sunk into oblivion.

The financial system is very complex, and this complexity creates risks. A new decentralized cryptocurrency-based financial system can be much simpler by reducing the number of interlayers and intermediaries - many risks in this case would disappear, and besides, it would be possible to create completely new types of financial products.

Cryptocurrencies can open the financial services market to people who are now excluded from their turnover, and also reduce the cost of entering the market and thereby increase competition, while the regulators would have occasion to rethink the rules by which the financial system operates.

In addition, we could reduce systemic risk: regulators suffer as much from the opacity of modern finance as much as users - research shows that increasing transparency leads to a reduction in intermediary chains and end-user costs.

History shows that when a certain technology matures, not only the practices associated with it change, but even the values of its users - and the same thing will certainly happen with blockchain technology.

Bitcoin was created in response to the 2008 financial crisis; the community formed around the new technology had a strong libertarian bias, and many of its members opposed the power of the modern establishment - in many respects it

resembled the culture that had developed around free software with its anti-capitalist ideas.

Nevertheless, it is likely that the blockchain will eventually be mastered by large corporations, banks and governments - like Linux, which has now become the basis of a huge amount of commercial goods and services.

Such a fundamental restructuring of a significant part of the economy will become a big problem for today's financial business, and in order to prepare for these changes, it is necessary to invest in research and experimentation - to take place in the new financial system.

Over time, the blockchain can be expected to provide even more security, more practical applications and products that are more convenient for customers. When customers decide that products based on this technology are cost-effective and convenient to use, the market will follow customers. "In the blockchain world they say: five months in the cryptobranch is like five years in the ordinary world in terms of changes. How long the transition will take is unclear, but the movement is gaining momentum. Growing trust, security, and efficiency always helps companies compete. Blockchain can help with this.

However, in my vision, despite the enormous potential of the blockchain, which can rightly be called revolutionary, this technology may pose some danger. The main reason why many projects in the blockchain will fail will be a mindless desire to "snatch a piece", however, the blockchain is a technology that requires a special approach and a meaningful attitude to itself. Otherwise, any project that aims only at making a profit can be a waste of time.

As in the case of any technology around which there is a huge stir, along with the rapid development of the blockchain, we can see a negative reaction from regulators. Blockchain has all the necessary resources to fundamentally change our world, therefore, no doubt, regulators will not close their eyes to the development of this technology.

CONCLUSION

The blockchain technology began to actively penetrate into many areas of life. By its significance, it is comparable to the creation of the Internet and the widespread smartphoneization, literally penetrating the modern world and changing everything around: and how people work, and how people relax, and how people communicate with each other. In this regard, it would not be superfluous to learn in more detail what a blockchain is and why this technology is so good.

Life is inextricably linked with money, data and documents. Because of this, people have to contact various intermediaries who give them this money, documents and data, check it, certify their authenticity, give copies, check the authenticity of the copy, and so on.

Blockchain is able to make an economic system decentralized, transparent and free from control. With it, it is possible to build a new financial system, get rid of intermediaries in conducting transactions, as well as change public administration.

An important task is to summarize and systematize the available data, as well as the classification of the main stages of development of blockchain technologies with the identification of features that will allow to assign a specific technological solution to a particular class.

Based on their technological essence, the use of blockchains seems to be the most promising in the field of automating such administrative procedures with state participation, the essence of which is to make legally significant entries in certain registries or registers reflecting civil status, property rights, health status confirming legal capacity or the reputation of various subjects.

So far, the growth of the blockchain's popularity is in many ways comparable to the movement of anti-globalists, as opposed to the desire of states for total control and management. First of all, it is the desire of people and businesses to protect their freedom and reduce costs.

However, sooner or later decentralization will come to the government, gradually crowding out centralized models.

The cryptocurrencies that exist today largely follow several characteristics. These characteristics include:

• A Peer-to-Peer connection and data transfer scheme and is therefore decentralized by nature (Although there are some exceptions such as nationally developed cryptocurrencies).

• Contain a finite and fixed total amount or supply of coins that can be generated or given (Also influences price, availability).

• Incorporates a public ledger (Mostly known as a Blockchain) or database that stores records of transactions and transfers of coins which prevents double spending.

• Feature a computational algorithm or "Proof of work" which verifies the integrity of the blockchain and consecutive blocks that contain the transaction data. In most cases, the Bos 12 computational power is provided by "Miners" to the network. Due to the finite amount of coins in circulation in most cryptocurrencies, the algorithm scales in difficulty and computational power required in accordance to the amount of coins mined.

• Utilize some form of cryptography (Usually public and private key cryptography) for safe storage.

Unlike ordinary money, represented by banknotes and coins or having electronic equivalents in the WebMoney or Yandex.Money system, cryptocurrency has no physical media and exists only in the form of program code. Therefore, it is often referred to as virtual or digital currency. The program code of digital money contains information about the quantity and for which wallet addresses these coins are attached. The owner of the virtual currency is the user of the computer network who has access to this address. Moving coins from one address to another means making a purchase-sale transaction with it .

Banking system is a set of banks operating in the country, credit institutions and individual economic organizations performing banking operations. In addition, the banking system includes specialized organizations that ensure the activities of banks and credit institutions: cash settlement and clearing centers, audit firms of banks, dealer firms dealing with securities of banks, organizations providing banks with equipment, information and personnel.

The established banking system has a two-tier organization. The upper level is the Central Bank (CB); lower level commercial banks and credit organizations. The Central Bank is decisive for the banking system, its activity allows regulating and controlling monetary relations in general, while maintaining the freedom of private entrepreneurship, which is ensured by the activities of commercial banks. Central Bank in all countries is the main link of the banking system, an institution that performs the functions of regulating the entire banking system.

Even years after the beginning of the spread of the Internet, people did not take it seriously. Since then, the network has firmly entered our lives and has become an environment where we communicate and buy goods and services. Moreover, it now has a significant impact on the political life of many countries.

As in the case of the Internet, cryptocurrencies are developing after the key technologies for this area - now it is a new open architecture of the blockchain. It is also decentralized and also based on several open protocols, using which companies and individuals can create products and services.

In my opinion, the potential of the blockchain technology depends entirely on how common it is in the world of ordinary people. At the moment, the recent success of Bitcoin has helped it stand out. However, only this year Bitcoin and cryptocurrencies slowly faded into the background, and, finally, it was the blockchain that interested investors.

Already in the first half of the year, blockchain startups in the amount earned about $ 240 million in profits from venture investors, so we can see that the technology is rapidly gaining momentum.

This year is likely to be a continuation of the trend in the market, aimed at innovations and global changes in the financial world. Below we will present the forecast for the blockchain, denoting possible major events in the industry this year.

People can consider Bitcoin as a prototype of a new, decentralized financial system. Yes, its current possibilities are limited (for example, while there is a small amount of transactions in it compared to conventional payment systems), but its code describes both regulations and economic laws at the same time, and in this sense it offers an opportunity to look into the future. For example, in order for an operation to be accepted in a bitcoin blockchain, it must satisfy certain rules.

Bitcoin simply does not violate the rules, automatically checking transactions for compliance, and in the event of a violation (for example, the absence of a valid digital signature), the transaction is rejected by the network.

In the field of financial instruments, Bitcoin, being the first mass cryptocurrency, has definitely shown how to play by the new rules without intermediaries and control from above. Even the "monetary policy" of Bitcoin is written in its code: new money is issued every 10 minutes, and the offer is limited, more than 21 million bitcoins will never appear - this is similar to the gold standard (i.e., a system in which the money supply is tied to the goods, and not determined by the government).

Nevertheless, it is difficult to argue with the fact that Bitcoin is an completely implemented technology: the network works, people attribute real economic value to Bitcoins, and all the miners who support the blockchain, and the authors of programs for users, without exception, follow its rules.

Blockchain maintains a reliable, albeit fairly simple payment system, and successfully resists attacks. And the opportunities that blockchain use promises to our

financial system can simultaneously be a cause for both optimism and pessimism. Unfortunately, the enthusiasm of investors is somewhat ahead of the actual development of technologies - it can often be seen that the word "blockchain" is used as a fashionable label pasted on quite traditional databases.

Today, far-sighted specialists all over the world are thinking about what the new protocol is leading us to, which allows mere mortals to trust each other through thoughtful code. History does not know anything of the kind: reliable transactions directly between two or more parties, verified and confirmed by joint efforts of the masses of participants and controlled by the personal interests of the entire team, and not controlled by large corporations that are chasing profits.

Perhaps such a protocol is not called Almighty, but a reliable global platform for our transactions is something daunting. It is called the Trust Protocol.

This protocol underlies an ever-increasing number of worldwide distributed registers, the so-called blockchains (or chains of blocks), the largest of which is Bitcoin. Behind the complex technology and inappropriate word stands, however, a simple idea. Blockchains allow us to send money safely and directly from me to you, bypassing the bank, credit card issuer or PayPal.

REFERENCES

1. O'Keeffe, M.; Terzi, A. (7 July 2015). "The political economy of financial crisis policy" 452 p.

2. Soo, Aeze 2016. The Blockchains Application Directory. Retrieved 6. December 2016, 458 p.

3. Raval, Siraj (2016). "What Is a Decentralized Application?". Decentralized Applications: Harnessing Bitcoin's Blockchain Technology. O'Reilly Media, Inc. 254 p.

4. Swan, M., 2015. Blockchain: Blueprint for a new economy. "O'Reilly Media, Inc." 475 p.

5. Haber, Stuart; Stornetta, W. Scott (January 1991). "How to time-stamp a digital document". Journal of Cryptology., 125 p.

6. IOTA, (2017). IOTA - Next Generation Blockchain

7. Kopfstein, Janus (12 December 2013). "The Mission to Decentralize the Internet" 547 p.

8. The Theory of Economic Development. 7th edn (transl. Opie R) Harvard University Press: Cambridge, MA, 254 p.

9. Bernstein H., (2017). Blockchain based intellectual property management. 239 p.

10. Keirns G., (2017). Will the Internet of Things Need Its Own Blockchain?. [Online] CoinDesk.com

11. 2016. Gartner: Blockchain Tech Hits Hype Cycle Peak

12. Oliver, J. (2017), Are Blockchains Key to the Future of Web Enctryption?, 452 p.

13. Bitcoin (2008): A peer-to-peer electronic cash system, 452 p.

14. Castillo M. D.., (2017). Blockstack Releases Blockchain-Powered, Tokenized Internet Browser., 452 p.

15. W. Dyer (2006). Third Generation Transaction Monitors, 325 p.

16. Gray J. and Reuter A. (2006). Transactions: Lectures and practice. - San Francisco: Morgan Kaufman, 206 p.

17. Demin V.S. and others (1997). Automated banking systems. - M: Menatep-Inform, 365 p.

18. Titorenko G.A. and others (1997). Computerization of banking. - M: Finstatinform, 452 p.

19. Levin V.K (1994). Information security in information systems and networks // Programming. - 452 p.

20. Lauts, E. B (2008). Banking services: legal support for stability. - M., 452 p.

21. Bratko A. G (2006). Banking law (theory and practice). - M., 228 p.

22. Kapaeva TI (2006). Accounting in banks. - M .: INFRA-M, - ISBN 5-16-002583-9 .. - 576 p.

23. Frederick M.,. (2006) Economic Theory of Money, Banking and Financial Markets = The Economics of Money, Banking and Financial Market. - 7th ed. - M .: "Williams", - ISBN 0-321-12235-6 .. - 880 p.

24. Macesich, G (June 30, 2000). "Central Banking: The Early Years: Other Early Banks". Issues in Money and Banking. 254 p.

25. Krahmalev SV (2007) Modern banking practice of international payments. - "GrossMedia", 540 p.

26. Rudakova O.S (2009). Banking electronic services: Textbook. Allowance - M .: University textbook, - 400 p.

27. Suren L (2008). Foreign Exchange Operations: Fundamentals of Theory and Practice - 2nd ed. - M.: Delo, 176 p.

28. Timothy W (2003). Koch. Bank management. -Ufa: spectrum. Part V, 452 p.

29. Zhukov. E.F.: (2007). Banks and banking operations: Textbook for universities / Ed. prof. Vina Paul. Era cryptocurrency. How bitcoin and blockchain change

the world economic order. Moscow: Mann, Ivanov and Ferber Publishing House, 2017 (2018). 429 s.

30. The head of the IMF offers to deal with cryptocurrency risks with the help of Blockchain https://coinspot.io/world/glava-mvf-predlagaet-borotsya-s-kriptovalyutnymi-riskami-s-pomoshhyu-blokchejna / (appeal date 03/14/2018)

31. The concept of voting on a random sample (random-sampling elections) proposed by David Chaum, a cryptologist, PhD in computer science and management.

32. Mogayar W., (2018). Blockchain for business. M., 215 p.

33. RIA Novosti [Electronic resource]. Access mode:

34. Ruzakova OA, Grin E.S (2017). The use of Blockchain technology to systematization results of intellectual activity // Bulletin of Perm University. Jurisprudence. Vol. 38. 520 p.

35. Lisitsyn N., (2018). Blockchain development forecast: 5 steps to the future, 2018. 12 p.

LIST OF TABLE

LIST OF PICTURE