UDC 336.743

A.S. Akhmetova[1], Z.A. Yeskerova[1], B.K. Spanova[2]

[1]*Ye.A. Buketova Karaganda State University, Kazakhstan;*
[2]*Karaganda Economic University of Kazpotrebsoyuz, Kazakhstan*
(E-mail: ahmetova.2017.86@mail.ru)

Blockchain as the basis of the economy

In this review article the author explains the basics of blockchain technology and some of its key concepts. The purpose of this article is to give a brief description of the currently existing options for using the blockchain in the economy and the information technology industry. The article will be of interest to people who are always in search of a new one; here are four specific applications that highlight technology. The authors want to prove the fact that the «blockchain» is ready to be a good replacement for an already outdated banking system. The paper also describes the main technological aspects and principles of the blockchain, which allows us to evaluate the use cases presented. After all, throughout history you can see evidence of the ability to change the value of a business. Today's Internet serves as a digital marketplace, a platform for economic activity and a repository of virtually all human knowledge. The authors describe the main stages of evaluating a potential idea regarding the main aspects of the blockchain. This helps to understand the need to develop a detailed model of the feasibility of a blockchain. The overarching theme is that an increasing number of daily transactions involving money, stocks, and valuable documents can begin to be transmitted through distributed network registers based on a chain of blocks with cryptographic protection and with a better level of detail. The central argument is based on the fact that the blockchain will raise the market for the provision of services by speeding up calculations and cleaning, including «smart contracts», data delivery and gradual disintermediation. We also cover possible threats to this development, especially issues of regulation and discussion of potential risks arising from this new technology.

Keywords: blockchain, economy, banks, money, digital asset, cyber security, payments, technology.

We live in a wonderful century, where flights into space are no surprise, where one inventor-enthusiast can build an entire Corporation and start producing electric machines. Technologies are improving every day in all aspects of our life. But one thing remains unchanged — banks. Banking institutions that were created several hundred years ago have not undergone major changes yet. It has already been proven that today's system in its present form does not perform its full functionality. Too often, companies run into problems, crises are becoming more common, inflation is becoming more and more unstable, public debt reaches historic highs. Now about blockchain, why does this technology, which at best now plays a minor role for today's economy and society, cause so much unrest? The magical appeal of technology is concentrated in its promise.

Numerous non-governmental, governmental and commercial organizations are actively investing in blockchain research and development to ensure the future. The institutions covering the United Nations, the International Monetary Fund, the EU Commission, the US Department of National Security and the National Science Foundation are investing in blockchain research initiatives. It is likely that almost every large multinational corporation has begun to study or invest in blockchain technology, from Walmart (the American company operating the world's largest wholesale and retail chain) to Western Union (a company specializing in providing financial intermediation services). In one word, using the blockchain allows companies to eliminate the need for central parties or brokers to participate in various processes, eliminating the costs, human error, time and security risks involved.

Meanwhile, remarkable (though very volatile) returns in crypto currencies such as bit coin and ether are attracting public attention to assets as speculative investments. Since June 27, 2017, the price of one bit coin has increased by 169 % and amounted to 3800 dollars, while the price of one ether has increased by 1500 % and 140 dollars respectively. The total market capitalization of crypto currencies is about 98 billion dollars. These figures vary greatly depending on price movements.

Blockchain promises to solve two fundamental problems of the Internet. First, the fact that the information can be copied effortlessly that devalues it and trusts at a time when economic relations are migrating to cyberspace. We describe the problem; previously it was considered impossible to distinguish the original from the copy in cyber economics. The cost of producing digital assets was zero, allowing for the free creation of copies of an existing asset. This was both an advantage and a disadvantage. Digital assets could be very easily created in large quantities, they were also easy to carry and protected from deterioration. But

Blockchain solves the problem by introducing the principle of the deficit in the digital sphere. Payments of the same amount can never be copied as they are verified on a global computer network. Each payment is clearly marked and different from other payments using this chain block mechanism. Blockchain also allows for safe transactions regardless of the individuals involved. The reliability of the payment system and the monetary unit both encourage the use of the system and stabilize it. Thanks to these two aspects, Blockchain actually represents something like a quantum leap in the development of the digital economy.

Another key indicator for any project is to estimate the cost of trust — the costs incurred by the parties to the transaction because they have to either rely on their counterparty or on a trusted intermediary to make the transaction safely. Blockchain can reduce these costs, thereby overcoming the barrier of mistrust, by ensuring transparency and automation of the proposed transaction. The technology can reduce the accounting and reconciliation of procedures or prepare access to services.

What is the basic concept? As described at the beginning, this is a type of universal journal, or ledger, for transactions of all kinds. According to its internal mechanics, this kind of technology is aimed at formalizing all economic relations — this is the first. Secondly, it is looking for ways to reduce the entire economic document flow and subject it to the rules of the logbook. Briefly summarizing, the blockchain idea is the creation of an omnipresent technology, which guarantees transaction transparency, but on another hand, it requires strictly regulated processes in business operations.

The financial sector rejects innovations that flourish in all other areas of our lives. There are many definitions of the blockchain by different authors, and there is no single, internationally agreed definition; therefore, it is important to understand its main parts. Now about technology, blockchain is a distributed database, in which storage devices are not connected to a common server [1]. Some believe that the blockchain technology has not been clearly defined with its position in the market yet; therefore, they use bitcoin as a guide and divide it into three main parts — transactions, consensus, and the network. This database stores an ever-growing list of ordered records called blocks. Each block contains a timestamp and a link to the previous block. Since transactions are checked, executed and recorded in chronological order in a secure database, where they remain available for search and on demand, which makes it an excellent alternative, or supplementing the current banking system.

The system of digital money (Bitcoin, lightcoin, dash, ethereum) is the first and, perhaps, the most obvious use of the blockchain technology. Money can be immediately transferred in real time from one continent to another, at very low costs and in seconds. Instead of waiting for several days or weeks, paying high commissions, as is the case with existing international money transfer solutions. Simple Mail Transfer Protocol (SMTP) is the basic protocol by which users can send each other emails in a problem-free way, regardless of their email provider.

The secure register of digital assets is the first in the list of reasons for the transition of the banking system to the blockchain. The same technology of a distributed ledger provides the means for recording and transferring digital assets over the Internet, and assets cannot be copied or multiplied (thus solving the problem of double costs, which was previously a problem of digital currencies). The digital asset registry is a list of smart property. A smart asset is a value that is registered on the blockchain. Digital asset registries can use blockchains extensively as a system for recording, transferring, and checking asset ownership.

The second reason is a process optimization. By optimization, it means not only simplification and acceleration, but also cost reduction. The main pattern of development is in developing complex systems from centralization to decentralization. Systems begin with centralization, because it is the most effective structure for creating, establishing and enforcing rules, that is, for creating a structure of knowledge. This minimizes duplication and establishes a clear hierarchy that can resolve disputes. But it is precisely these features that mean that centralization has costs that are beginning to accumulate, especially during the period of expiration of operation. In the country's economy, it manifests itself as inflation, corruption and rent seeking. In the end, adaptation and differential selection lead such systems to decentralization, as centralization costs increase in the way of operation and, at the same time, decentralization costs fall, often due to technical progress (for example, cryptography and computers, in the case of blockchain). Centralization brings order, but this order can be fragile.

You no longer need to build branches, office buildings, and offices for employees, huge archives to save a customer database. Instead, blockchain-based banking applications can solve many problems [2]. You will not need to send a request to the credit bureau, since all information about all customers will be distributed and stored in the general register of all banks in the world.

Cybersecurity is the third. According to statistic brain, in 2016 alone, more than 5 billion dollars were stolen from bank cards around the world. Centralized databases are an attractive target for hackers, since it is easier to conduct Distributed Denial of Service attacks on one specific database than to deploy forces on all computers used in the world [3].

Using cryptography, transaction information is recorded so that it is permanent and unauthorized. As a result, we can call the blockchain «no change». System attacks are extremely complex. The blockchain entry is downloaded to thousands of computers around the world that participate in the network. These computers constantly synchronize or update records for new transactions. As a result of such widespread data dissemination, the data warehouse is reliable, and attackers do not have a single point of failure. To remove the blockchain, you need to destroy thousands of computers in the system throughout the world.

Given the recent advent of technology, one of the possible risks is still relevant. This is long-term digital storage, which in the case of blockchains is not as simple as in conventional centralized databases. Another reason for possible security risks is the lack of research and the subsequent standardization of security measures in the industry. As indicated by Halpin & Piekarska, the current development of the blockchain is mainly carried out by practitioners without the involvement of cryptography experts. Thus, sustainability and safety solutions are constantly changing and vary from case to case due to the individual choice of developers, which is based on their practical experience. It may also include a selection of defective protocols and implementation errors, such as unsafe language design. The lack of a common vocabulary also creates additional problems in developing secure solutions, although at the moment there are attempts to create it.

Last but not least, there are risks associated with the use of cryptography. Although the algorithms used, such as error-correcting code and Rivest, Shamir and Adleman, are usually considered safe, it is still possible to detect unknown vulnerabilities or backdoors, as was the case with the Secure Hash Algorithm-1 hashing algorithm. The biggest cost of hashing is electricity and high-performance equipment. Thus, the blockchain is highly dependent on large numbers of devices containing semiconductors, such as memory chips, graphics cards and computer processors. Graphics processing unit (GPU) chips manufactured by companies such as AMD and NVIDA, turned out to be much better in computing than standard processors. Such efficiency in computing power, combined with a reduction in the cost of hardware, is likely to continue to support the emergence and growth of blockchain technologies. The assumption of quantum computers and their perceived capabilities that easily decipher existing algorithms cannot be considered an appropriate risk. However, it may materialize sometimes in the future. The use of private / public keys also implies a risk from the user's point of view — denial of access to data due to the loss of a private key that cannot be recovered or recalculated.

For bitcoins and other «Byzantine fault-tolerant» networks, the most visible way to manipulate data in the blockchain is a coordinated attack by most network participants, called «attack by 51 %» (there are different types of attacks) that require different levels of participation for success. In addition, experts agree that quantum computers of the future will not be able to hack modern cryptography schemes.

At the same time, decentralized storage records protected by cryptographic signatures on blockchains can significantly improve cybersecurity. Greater user control and accounting of personal data is an expected feature of decentralized solutions. AI (artificial intelligence) is built directly into the network through a sophisticated protocol that automatically identifies, verifies, confirms, and routes network transactions. The result is a reliable and durable system.

One of the most intriguing ideas developed in the blockchain industry is the payment channels. The payment channel is auto renewable or not a financial contract executed over time in three steps:

– one party opens a payment channel with one or more parties and publishes an advance payment escrow file in the file;

– the second party, in turn, creates a separate «money pot» for the amount requested by the second party;

– and over time the transaction is completed, after it is updated or closed.

The idea originated for micropayments, where phased transactions do not make sense, and an automated contractual agreement can support aggregate consumption.

Ethereum is a promising and comprehensive blockchain technology with a wider range of capabilities than the first-generation bitcoin system [4]. Although bitcoin has a narrow programming freedom (some compare the programming capabilities with the capabilities of a graphing calculator) and, in fact, is a log of payments between the parties, ethereum can be used to quickly create new applications.

Reliability programming language (solid), ease of use and versatility. It is «Turing-complete», which means that it is able to approximately simulate the computational aspects of any other real universal computer language, which leads to more complex applications.

As part of the Turing completeness of the Solidity programming language, anyone can create conditional contracts (using «if / then» and other logical operators) that run autonomously. Coded contracts are called smart contracts and can fulfill previously agreed terms.

Intellectual contracts are of great importance: they can be considered legally feasible and can benefit countless industries, eliminating time and human errors from contractual processes.

Please note that since the contracts are in the blockchain, their code is open source; Public visibility encourages developers to be extremely attentive to their code so that hackers do not use it to attack the program.

In combination with high-quality developer tools and main components (Truffle, Metamask, uPort). And significant industry support (Ethereum Enterprise Alliance together with ConsenSys, a venture capital firm based in Brooklyn), ethereum shows great promise and popularity in the community [5].

On-air cryptocurrency is necessary for executing the code and smart contracts in the Ethereum blockchain. Users must spend a small amount of ether, called «gas», to stimulate the network to conduct and verify transactions and execute smart contracts. These «gas» payments for the execution of transactions are an integral use of the ether in the network.

To date, attempts are being made to eliminate bandwidth limitations associated with the blockchain. An application typically involves removing most transactions from a chain and periodically recording «net» in the chain. Other efforts focus on an alternative consensus-building mechanism, such as «proof of interest», which is still largely untested and runs the risk of being controlled in the hands of one party, which accumulates great potential. They are also trying to divide the block into several smaller chains that may be interconnected, but, as a result, there is a higher risk that any of these mini-chains may be vulnerable. In the meantime, there is promising evidence with zero knowledge and other suggestions for protecting privacy in decentralized networks.

Thus, proposals for solving problems of scalability and privacy can also entail some form of compromise. Using a blockchain or a distributed register for specific use tasks will include an assessment of the appropriate tradeoffs and size optimization, which is most important for this application. Allowed blockchains are developed for most businesses. Applications can exhibit significantly different properties from the decentralized block chains discussed above [6]. Most likely, they will work as stationary systems. However, moving to a general book, digitizing and optimizing processes that are currently largely boring or burdensome, the entire cost curve can be shifted down, reducing overall transaction costs.

Currently there are only a few ways to invest in blockchain technology:

– investing in cryptocurrency, such as bitcoin, translation and/or ripple;

– investments in «pure games» of blockchain-based technologies for mining;

– investments in support services of blockchain providers: companies that produce hardware and software that makes cryptographic mining and blockchain systems possible.

Each method of investing in the blockchain technology has its own trade-off between risk and reward. Considering the possibility of investing in leading cryptocurrencies, it is important for an investor to understand that the values fluctuated greatly. For example, in April 2016, the price of one bitcoin was about $1000. The cost of bitcoins in November 2017 exceeded $16000, and in February 2018 dropped below $7000.

As for investments in earlier, pure blockchain companies, these organizations include companies that can profit from the broader implementation of blockchain technology. These include cryptocurrency production farms that can optimize and improve business processes that depend on hardware and software, as well as databases. «HIVE Blockchain Technologies» Ltd is an example of such a company and has set itself the goal of becoming a world leader in the field of crypto mining in building a bridge between the crypto and traditional markets. The level of risk of investing in these companies varies. It will depend on how likely the company is to succeed in creating and developing technologies.

Finally, investors can invest in companies or service providers in the blockchain ecosystem, which can provide a more diversified approach to clean games and buying cryptocurrencies. These companies include server suppliers and semiconductor manufacturers that provide the vital infrastructure necessary to support blockchain technology. Memory manufacturers also provide critical services in commercial currency mining.

Examples of public companies providing these services. Intel is an American multinational company well known to computer components manufacturers. Western Digital Corporation is an American computer storage company and one of the largest computer hard drives. By investing in various aspects of the blockchain ecosystem, people can gain access to diversification benefits that reduce risk, thanks to a potential risk-based yield increase.

And in conclusion, we would like to summarize that all four proposals frustrated in this article may have a positive economic effect on the financial situation in the world. From this analysis it follows that many daily operations with money, assets and documents can begin to be carried out in digital networks with cryptographic security. The emergence of cryptocurrency and blockchain has made many changes in the world of finance. Previously, the traditional system of financial transactions included the active participation of third-party financial institutions, that is, banks. However, at present blockchain helps to make transactions between private individuals, companies located abroad, without the participation of intermediaries. Previously, the world economy was controlled using fiat currencies, supported by the state, that is, the dollar, euro, pound, etc.

The applications described above are mainly developed and used in the financial sector. The main reasons are the introduction of the blockchain in the form of cryptocurrency, the extensive resources of large financial organizations and the rapid innovative culture of these organizations contribute to this. Other sectors, such as government agencies, are less flexible, so blockchain adaptation is much slower. The article outlines the basics of assessing the feasibility of using blockchain. This can be done by examining the main components of the functionality of the blockchain and finding out the relationship with this problem. It is worth noting that the research in the blockchain evaluation model is still at a very early stage, and further research is needed in this area. Proper assessment of the need for a blockchain can save a lot of resources on software development and maintenance costs.

In addition to performing peer-to-peer transactions, the blockchain has helped companies seal and execute contracts using smart contracts functions in publicly available blockchains, such as Ethereum. Smart contracts allowed the creation of a fundraising mechanism — initial coin offering, known as the «killer application» for Ethereum — which resolved the pain point faced by entrepreneurs attracting traditional venture capital. This mechanism led to the fact that in 2018 more than 14 billion dollars were attracted to companies with blockchain support.

Only nine years have passed since the first white paper on Bitcoins appeared, and now companies, governments are studying technology to find possible uses for the sake of efficiency. And, perhaps, in the near future to begin the third industrial revolution.

References

1 Генкин А. Блокчейн. Как это работает и что ждет нас завтра / А. Генкин. — М.: Альпина Паблишер, 2018. — 145 с.

2 Дрешер Д. Основы блокчейна / Д. Дрешер. — М.: ДМК Пресс, 2018. — 78 с.

3 Свон Мелани. Блокчейн. Схема новой экономики / Мелани Свон. — М.: Олимп-Бизнес, 2015. — 98 с.

4 Скиннер Крис. ValueWeb. Как финтех-компании используют блокчейн и мобильные технологии для создания интернета ценностей / Крис Скиннер. — М.: Машиностроение, 2016. — 145 с.

5 Тапскотт Дон. Технология блокчейн. То, что движет финансовой революцией сегодня / Дон Тапскотт. — М.: Эксмо, 2016. — 346 с.

6 Никитин А.Н. Криптовалюта, полная надежд. — / А.Н.Никитин. М, 2017. — 25 с.

А.С. Ахметова, З.А. Ескерова, Б.К. Спанова

Блокчейн экономиканың негізі ретінде

Мақалада «блокчейн» технологиясының негіздері және кейбір негізгі тұжырымдамалары түсіндірілді. Мақаланың мақсаты — экономикадағы және ақпараттық технологиялардың индустриясында блокчейнді пайдаланудың қолданыстағы нұсқаларын сипаттау. Мақала әрқашан жаңадан ізденуге ынта адамдарға қызықты болады, мұнда технологияны ерекшелейтін төрт арнайы бағдарлама бар. Авторлар ескірген банктік жүйені жақсы ауыстыруға дайын екенін дәлелдегісі келеді. Сондай-ақ мақалада келтірілген қолдану жағдайларын бағалауға мүмкіндік беретін блокчейннің негізгі технологиялық аспектілері мен қағидалары сипатталған. Себебі тарихқа үнілсек, бизнестің мәнін

өзгерту қабілеті дәлелденген. Бүгінгі Интернет цифрлы нарық, экономикалық қызмет ету платформасы және адамның барлық білімін сақтауға арналған. Авторлар блоктың негізгі аспектілері туралы ықтимал идеяны бағалаудың негізгі кезеңдерін сипаттаған. Бұл техникалық-экономикалық негіздемесін әзірлеудің қажеттілігін түсінуге көмектеседі. Негізгі тақырып — ақшаны, акцияларды және құнды құжаттарды қамтитын күнделікті операциялардың көбеюі криптографиялық қорғанысы бар және бөлшекті жақсы деңгейде болатын блоктық тізбеге негізделген таратылған желілік регистрлер арқылы берілуі мүмкін. Орталық аргумент «блокчейн» есептеулерді және тазалауды жеделдету арқылы қызметтерді ұсыну нарығын көтереді, соның ішінде «ақылды шарттар», деректерді жеткізу және бірте-бірте жою. Сондай-ақ осы дамудың ықтимал қатерлерін, әсіресе осы жаңа технологиядан туындайтын әлеуетті тәуекелдерді реттеу мен талқылау мәселелері қарастырылған.

Кілт сөздер: блокчейн, экономика, банктер, ақша, сандық активтер, киберқауіпсіздік, төлем, технология.

А.С. Ахметова, З.А. Ескерова, Б.К. Спанова

Блокчейн как основа экономики

В статье даны основы технологии «блокчейн» и ее некоторые ключевые концепты. Цель этой статьи — дать краткое резюме существующих в настоящее время вариантов использования блокчейна в экономике и индустрии информационных технологий. Статья будет интересна людям, что всегда находятся в поисках нового, здесь описаны четыре конкретных приложения, которые выделяют технологию. Авторы доказывают тот факт, что «блокчейн» готов быть хорошей заменой уже устаревшей банковской системе. В работе также приведено описание основных технологических аспектов и принципов работы блокчейна, что позволяет провести оценку представленных вариантов использования. Ведь на протяжении всей истории можно увидеть свидетельства способности изменить смысл ведения бизнеса. Сегодняшний интернет служит цифровым рынком, платформой для экономической деятельности и хранилищем практически всех человеческих знаний. Автор описывает основные этапы оценки потенциальной идеи в отношении основных аспектов блокчейна. Это помогает понять необходимость разработки подробной модели осуществимости блокчейна. Всеобъемлющая тема заключается в том, что все большее число ежедневных операций с участием денег, акции и ценных документов могут начать передаваться через распределенные сетевые регистры на основе цепочки блоков с криптографической защитой и с более улучшенным уровнем детализации. Центральный аргумент строится на том, что блокчейн поднимет рынок оказания услуг за счет ускорения расчетов и очистки, включения «умных контрактов», доставки данных и постепенной дезинтермедиации. Также раскрыты возможные угрозы этому развитию, особенно вопросы регулирования и обсуждения потенциальных рисков, вытекающих из этой новой технологии.

Ключевые слова: блокчейн, экономика, банки, деньги, цифровой актив, кибербезопасность, платежи, технология.

References

1 Genkin, A. (2018). *Blokchein. Kak eto rabotaet i chto zhdet nas zavtra [Blockchain. How it works and what awaits us tomorrow]*. Moscow: Alpina Pablisher [in Russian].

2 Dresher, D. (2018). *Osnovy blokcheina [Fundamentals of the blockchain]*. Moscow: DMK Press [in Russian].

3 Svon, Melani. (2015) Blokchein. *Skhema novoi ekonomiki [Blockchain. The scheme of the new economy]*. Moscow: Olimp-Biznes [in Russian].

4 Skinner, Kris (2016). *ValueWeb. Kak fintekh-kompanii ispolzuiut blokchein i mobilnye tekhnolohii dlia sozdaniia interneta tsennostei [How FINTECH companies use blockchain and mobile technologies to create Internet values]*. Moscow: Mashinostroenie [in Russian].

5 Tapskott, Don (2016). *Tekhnolohiia blokchein. To, chto dvizhet finansovoi revoliutsiei sehodnia [Tech Blockchain. What drives the financial revolution today]*. Moscow: Eksmo [in Russian].

6 Nikitin, A.N. *Kriptovaliuta, polnaia nadezhd [Cryptocurrency full of hope]*. Moscow [in Russian].