DOI: 10.37943/12ZATX3943

Ruslan Shaidulov
Master's degree in Scientific and Pedagogical Direction
ruslanshaidulov11@gmail.com, orcid.org/0000-0003-4060-6763
Atyrau University, Kazakhstan

Zita Kenzhegalieva
PhD, Acting Associate Professor of the Department
z.kenzhegalieva@asu.edu.kz, orcid.org/0000-0002-3172-2597
Atyrau University, Kazakhstan

BLOCKCHAIN AS DATA PROTECTION IN FINANCE

Abstract. Five years ago, it would have been difficult to describe Kazakhstan's economy as highly digitized. However, the country is currently implementing state programs aimed at improving the socio-economic conditions of its citizens, with a focus on digitalization and the streamlining of financial monitoring systems for budget expenditure. The process of introducing digital technologies, in various forms, serves to increase transparency in state reporting, which in turn helps to control budget expenditures and investments. The goal of these efforts is to improve economic indicators within the state budget system and to allocate public funds more efficiently in order to achieve the best results across all sectors of Kazakhstan's economy. In addition, the adoption of blockchain technology can address various security threats and problems, such as phishing attacks, server hacking, and compromised accounts, by allowing users to reclaim control of their data. The use of blockchain, which offers a high level of security and privacy, has the potential to revolutionize industries that rely on trust. In the long term, it is expected that blockchain will become a widely accepted and integral part of society, similar to the internet. The digitalization of finance in Kazakhstan is necessary to simplify and automate accounting, financial monitoring, and various banking and tax operations. It also makes it possible to improve the transparency of financial reports and increase the efficiency of budget management. The digitalization of finance can also reduce the risks of errors in working with accounting documentation, simplify accounting, and improve cost control. With the use of digital technologies, the process of data collection, processing, and storage becomes more efficient, saving time and resources.

Keywords: finance, digitalization, blockchain, stages, transparency, smart contracts.

Introduction

In the modern world, it is necessary to use all the latest technologies to maintain the country's competitiveness in the world. The financial sector has always been friendly to innovations, especially if they help reduce risks and significantly decrease the probability of various shocks in the economy. One of these technologies could be "blockchain," a technology capable of bringing the greatest transparency to transactions and deliveries. Blockchain is a technology for the reliable, distributed storage of records of all transactions ever made [1]. In a blockchain-like system, transactions can be made with any currency, financial contract, tangible or intangible [1]. The smart contract helps to strengthen the terms of the transaction in the blockchain world. The main problem of classical and generally accepted contracts in the world is the "Bureaucratic guarantor" or "state." The state judicial system is the main repulsive

Scientific Journal of Astana IT University
ISSN (P): 2707-9031 ISSN (E): 2707-904X
VOLUME 12, DECEMBER 2022

factor since, in case of non-fulfillment of obligations; one of the parties will have to apply to state bodies. All issues of this kind are resolved in court. Going to court requires time and financial costs [2]. This is where blockchain technology saves; it stores contract data in a decentralized manner and eliminates the possibility of making changes to the contract code and allows monitoring of the fulfillment of all obligations of the parties. This integration can reduce costs and various shocks when creating, concluding, and signing contracts. The current program in this direction is the state program "Digital Kazakhstan." The purpose of the program is to accelerate the pace of development of the republic's economy and improve the quality of life of the population through the use of digital technologies in the medium term, as well as create conditions for the transition of the economy of Kazakhstan to a fundamentally new development trajectory, ensuring the creation of the digital economy of the future in the long term [3].

The overall contribution of the article

The study shows that today the study of blockchain technology in the financial system of the Republic of Kazakhstan can have the most important role in the development of the economy through a deeper introduction of blockchain technology, which makes it possible to simplify and ensure the reliability of the activities of financial institutions for both users (citizens) and for all economic entities. From a scientific point of view, this topic may be of value in the implementation and use of the latest mathematical encryption models for regional economies of developing countries, adapting successful Western experience. Blockchain, having data hashing technology in its structure, allows transactions to be carried out most securely, excluding the intervention of third parties by creating unique access keys to user data. In addition, further development and complication of formulas for generating unique key codes will allow Kazakhstan to reduce time costs in the process of internal and external trade turnover, stimulate the banking system, and simplify interaction with all financial institutions of the country at the user level. Creating safer and more attractive conditions for domestic and foreign investors by guaranteeing financial security gives the Kazakh economy new opportunities for international cooperation and attracting foreign companies to the local market. This step is necessary for the formation and strengthening of leadership positions in Central Asia to ensure financial security and stability. The article mentions the method of reinforcement of accounting transactions by introducing a digital signature system into the document flow. More thorough work is needed to introduce blockchain into electronic accounting systems such as 1C: Accounting, Turbo 9, and Info-Accountant to standardize accounting for all economic entities. The development of state programs for the development of this area of financial automation may become one of the priorities for the Ministry of Finance of the Republic of Kazakhstan.

Blockchain Technology

Blockchain is a technology that uses the method of decentralized storage and distributed recording of transactions, based on cryptographic methods of information protection, allowing excluding an intermediary [4]. Blockchain has much greater potential for both private businesses and the state and can become a truly transformational technology [5].

According to developers, the basis of new projects built on the blockchain is openness, security, and security. One of the tasks of information protection is to ensure the reliability of data. In this study, we consider the RSA asymmetric encryption algorithm. This encryption method is actively used in logs-in traditional blockchain systems; for example, the mathematical model will look like this:

DOI: 10.37943/12ZATX3943

$$n = b \cdot c \quad (1)$$
$$\phi(n) = (b-1)(c-1) \quad (2)$$
$$c \cdot e \bmod \phi(n) = 1 \quad (3)$$
$$d = m^e \bmod n \quad (4)$$
$$m = d^c \bmod n \quad (5)$$

Where «b, c» are prime numbers and «n» is the modulus for the public and private key, $\phi(n)$ is the Euler's totient function. After selecting the primes, an integer «e» is selected from 1 to $\phi(n)$. Next is the number «c», which corresponds to the formula (3). So is shaping the private key $\{c, n\}$ and the public key are formed $\{d, n\}$ used for encryption (4) and decryption data (5).

The principle of operation of the encryption algorithm of the signature of the parties.

Blockchain technology relies heavily on cryptographic algorithms, particularly the Elliptic Curve Digital Signature Algorithm. This algorithm utilizes elliptic curves and finite fields to sign data, allowing a third party to verify the authenticity of the signature and prevent any potential forgery. Elliptic curve over a finite field:

Elliptic cryptography involves the use of an elliptic curve over a finite field. In the context of ECC, the finite field is a predetermined set of positive numbers in which the result of each calculation is represented.

$$y^2 = x^3 + ax + b \ (mod\ p) \quad (9)$$

For instance, when we perform the operation 9 mod 7 = 2, we are using a finite field ranging from 0 to 6, and all operations performed modulo 7 on any number will result in a value within this range. All the above-mentioned properties (addition, multiplication, and point at infinity) for such a function remain valid, although the graph of this curve will not resemble an elliptic curve. The elliptic curve of bitcoin, y2 = x3 + 7, defined on a finite field modulo 67, looks like this:

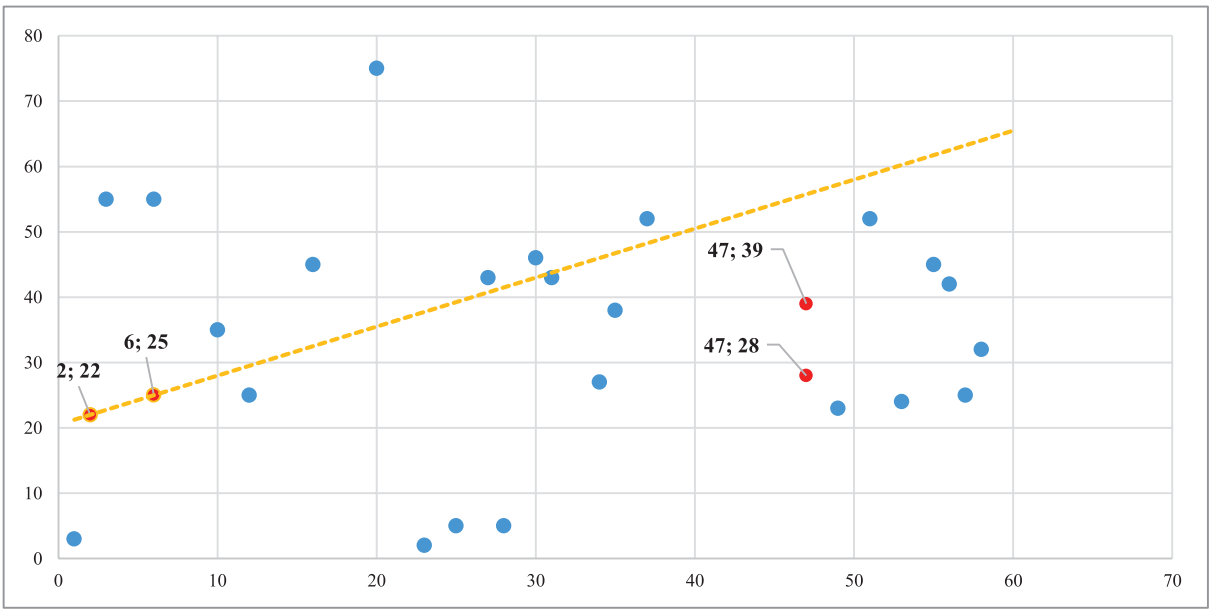


Figure 1. The finite field. (Addition of points (2, 22) and (6, 25).

In this example, we have a finite field with integer values for x and y ranging from 0 to 66. When plotted on a graph, the lines drawn on this graph will "wrap around" the field once they

Scientific Journal of Astana IT University
ISSN (P): 2707-9031 ISSN (E): 2707-904X
VOLUME 12, DECEMBER 2022

reach barrier 67 and continue from the other end with the same slope but with a shift. For instance, the addition of points (2, 22) and (6, 25) in this specific case is shown in Figure 1.

The scope of these models has a very wide range of samples

A digital signature is a method of verifying the authenticity of a digital document or message. It uses cryptographic techniques to ensure that the document or message has not been altered during transmission and that it is authentic. To create a digital signature, the sender first generates a hash of the document or message using a cryptographic hash function. The sender then encrypts the hash using their private key, creating the digital signature. The recipient can verify the authenticity of the document or message by using the sender's public key to decrypt the digital signature and compare it to a new hash of the document or message. If the two hashes match, the document or message is authentic and has not been altered. Digital signatures are often used in electronic commerce transactions to protect the integrity of financial documents and establish the identity of the sender. They are also used in email and other forms of electronic communication to ensure that the message has not been tampered with during transmission. We can see how this works in the accounting transaction:

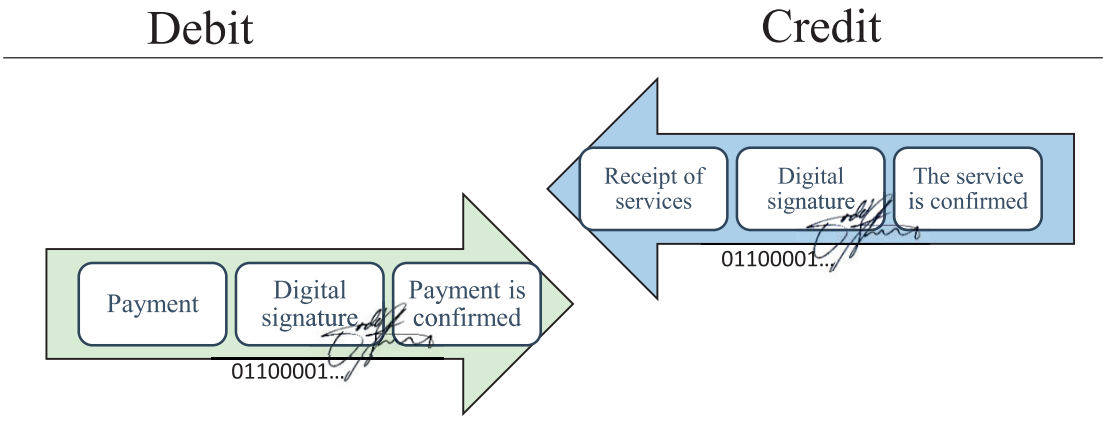


Figure 2. Digital signature in accounting transaction.

The security of a digital signature depends on the strength of the underlying cryptographic algorithms and the security of the private key. It is generally considered very difficult to forge a digital signature, as it requires the attacker to have access to the private key. However, if the private key is compromised or the cryptographic algorithms are weak, it is possible for an attacker to forge a digital signature. Therefore, it is important to protect private keys and regularly update cryptographic algorithms to maintain the security of digital signatures.

Table 1. Secret and public key structure.

Secret key / Public key			
	Person 1	Person 2	Person 3
pk	01000001...	01000001...	01000001...
sk	🔒 10010110...	🔒 10010001...	🔒 11011100...

In a digital signature system, the private key is used to sign a message or document. It is a secret key that only the owner of the private key should know and have access to. The private key is used to create a digital signature by applying a mathematical algorithm to the message

DOI: 10.37943/12ZATX3943

or document being signed and the private key. The resulting digital signature is unique and can only be created using the private key.

$$\text{Sign (Message, sk)} = \text{Signature} \tag{7}$$

A private key is a unique, secret piece of information that is used to authenticate and encrypt messages in a public key encryption system. Private keys are typically generated by the owner of the key and are kept secret. It is essential that the private key is kept secure, as anyone with access to the private key will be able to decrypt messages and access sensitive information. It is generally considered difficult to forge a private key, as it is typically a long, randomly generated string of characters. However, it is possible for a private key to be compromised if it is not kept secure, for example, if it is stolen or guessed.

$$\text{Verify (Message, Signature, pk)} = \text{True/False} \tag{8}$$

When a message or document is signed using a private key, the signature can be verified by anyone using the corresponding public key. This process helps to ensure the authenticity and integrity of the message or document, as it allows anyone to verify that it was indeed signed by the owner of the private key. [6]

The process of obtaining electronic digital signatures:

Choose a prime number p and two random numbers q and x, such that q and x are less than p. For example, p could be 13, q could be 4, and the secret key x could be 15. Calculate the value of the public key y using the equation y = q^x (mod p). In the example given, y would be equal to 10;

$$y = q^x(mod\ p) = 4^5(mod\ 13) = 10 \tag{9}$$

Determine the hash value of the original message M. For this example, let's say m is equal to 5.

$$m = h(M),\ in\ this\ example\ takes\ m{=}5 \tag{10}$$

Choose a random number K that is mutually prime with p-1. In this example, we'll use k=11.

$$a = q^k(mod\ p) = 4^{11}(mod\ \ 13) = 4 \tag{11}$$

To create the electronic digital signature, we need to calculate the signature elements a and b. a is calculated using the equation a = q^k (mod p), which in this case would be 4. b is determined using the extended Euclid algorithm from the following equation values given in the example, we can solve for b to be equal to 5:

$$m = (xa + kb)(mod(p-1)); \tag{12}$$

$$5 = \big((15 * 4 + 11 * b)(mod(12)\big) = \\ = 11 * b = -55(mod\ 12), b\ =\ 5 \tag{13}$$

Once the signed message and the public key y are received, the recipient can verify the authenticity of the signature by checking that the following condition is met:

$$y^a a^b(mod\ p) = q^m(mod\ \ p) \tag{14}$$

$$10^4 4^5(mod\ 13) = 4^5(mod\ \ 13) \tag{15}$$

$$10240000(mod\ 13) = 4^5(mod\ \ 13) \tag{16}$$

$$4(mod\ 13) = 4(mod\ \ 13) \tag{17}$$

In this case, the condition is satisfied and the message is recognized as authentic.

Scientific Journal of Astana IT University
ISSN (P): 2707-9031 ISSN (E): 2707-904X
VOLUME 12, DECEMBER 2022

Key tasks of financial digitalization.

The key tasks of the Ministry of Finance today are increasing the transparency of the quality of public services provided and increasing tax collection, improving the efficiency of the budget process. The current share of the budget revenue is formed from tax revenues and customs duties, as well as from the sale of State property. One of the most effective tools for increasing tax revenues is the national system for monitoring goods, which is a set of information systems.

The first stage.

The initial stage of monitoring should be implemented in an information system that performs automated control of the entire process from the moment of submission of preliminary information to control after the release of goods.

The second stage.

The next stage is the physical labeling of goods, aimed at protecting against counterfeit products and reducing the volume of the shadow economy. Under the "virtual warehouse" system, it is possible to automate the process of arrival and write-off of goods, including based on information from electronic declarations. Thanks to this, it becomes possible to analyze the pricing of goods with tracking of the entire resale chain, which allows for determining the margin when selling goods and, accordingly, the correctness of paying taxes. The information system "electronic invoices" today provides an operational statement of the enclosed documents, including based on data from a virtual warehouse. Due to integration with the blockchain VAT information system, invoices and transactions for payment of transactions are linked in real time using a smart contract based on blockchain technology. No record can be deleted or changed, thereby the full process of creating, transferring, and paying for goods, works and services in a given time period will be visible, which will allow deductions and VAT refunds to be made online, as well as fully automate the process of filling out a VAT return.

Why do we need smart contracts?

In general, "smart contracts" are just lines of code that are stored in the blockchain and subsequently run when pre-defined conditions are met. As a rule, smart contracts are used to automate the execution of an agreement so that all participants can immediately be sure of the result without the participation of any intermediary or loss of time. They can also automate the workflow by launching the next action when the conditions are met [7]. The blockchain in this story, as mentioned above, acts as a decentralized repository – smart contracts must be in a safe place [8].

Final control.

The final link in the goods monitoring system is online cash registers, which are used to write off goods from a virtual warehouse. Information from cash registers automatically gets to the state revenue authorities for remote monitoring. An increase in income is also planned through large-scale updates of information on the property of individuals and legal entities. Moreover, due to integration with external data sources Figure 3.

DOI: 10.37943/12ZATX3943

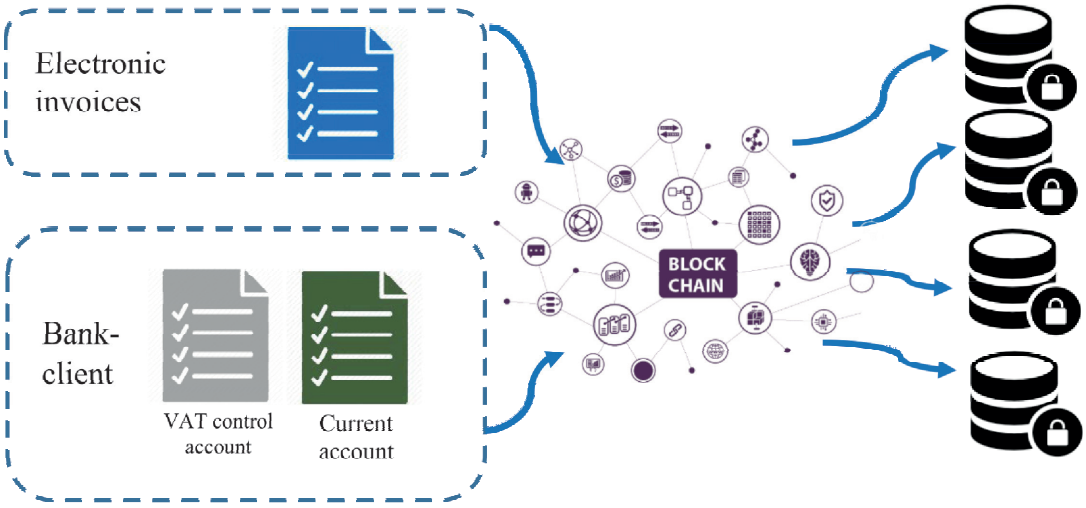


Figure 3. The structure of decentralization.

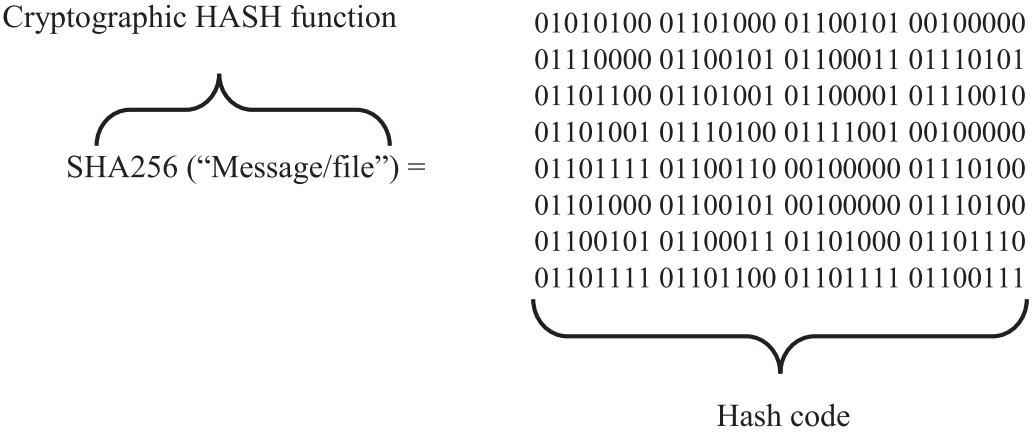
The next step is the digital transformation of the budget process. By eliminating the media gap, the cyclical process of budget formation and execution will be fully automated. The budget planning system automates the process of collecting the needs of state institutions and the formation of electronic budget applications at different levels, from district to republican. This will lead to a significant reduction in paper document flow and approval deadlines. After the budget is approved, the financing obligations will be automatically transferred to the Treasury information system and the acquisition information to the state portal purchases.

When planning the budget, the system will provide the state recommended by the portal. The budget planning system calculates purchases a range of costs, which will solve the problem of inflated prices and daily transmission of information on the development of budget funds to the state portal. Procurement and treasury in the budget planning system will ensure the receipt of operational information on budget execution. Electronic delivery certificates already today allow recording the execution of transactions on the state portal. It is envisaged to integrate the system of electronic invoices. Purchases will be accepted in the register of state property. This will be used to take into account the remaining goods when planning the budget. Through the Internet portal "open budgets", citizens will be able to participate in the planning of the state budget through online voting and monitor the transparency of revenues and the effectiveness of budget funds. This can further increase the confidence of the population in the government as a whole.

Preliminary result of blockchain implementation

"Government for Citizens", with the support of the Ministry of Justice and the Ministry of Digital Development, together with Otbasy Bank, introduced blockchain technology into public services for registering a real estate pledge agreement for individuals [9]. Thus, this technology will reduce all processes related to the provision of services from weeks to one day. The peculiarity of the technology is that the information recorded in the blockchain cannot be changed or deleted. The presence of a "HASHING" algorithm ensures the security of the technology. This mathematical algorithm converts an arbitrary data array into a fixed-length string consisting of letters and numbers [10]. For example, if there is a need to find a message whose SHA-256 hash is some specific string of 256 bits, there is no better method than just guessing and checking random messages, and this will require, on average, 2^256 guesses [11].

Scientific Journal of Astana IT University
ISSN (P): 2707-9031 ISSN (E): 2707-904X
VOLUME 12, DECEMBER 2022



The hashing system allows for storing information about changes in the unique number of a product or service as safely as possible from external attempts to make changes [11].

There are several reasons why the blockchain is considered an effective way to store information: Decentralized nature: The blockchain is a decentralized system, meaning that it is not controlled by a single entity. This makes it more resistant to tampering and manipulation compared to centralized systems. Immutability: The information stored on the blockchain is permanent and cannot be changed once it is recorded. This ensures the integrity and authenticity of the data. Security: The blockchain uses advanced cryptographic techniques to secure information and prevent unauthorized access. Transparency: The blockchain is a transparent system, meaning that all transactions and information are visible to anyone with access to the network. This helps to increase trust and accountability. Efficiency: The blockchain can help streamline processes and reduce the need for intermediaries, which can improve efficiency and reduce costs.

Conclusion. Blockchain technology is the most promising solution for solving a number of problems related to finance. It ensures the reliability, security, and transparency of financial transactions, which contributes to improving interaction with financial institutions and increasing public confidence in them. The use of blockchain technology in finance is a promising direction of development that can bring a number of advantages in the fields of financial management and risk reduction. One of the main advantages is an increase in the security of information and transactions, as well as an improvement in the transparency of operations. There are a number of issues related to the implementation of blockchain technology in finance, such as issues of consistency with the current regulatory framework, issues of data security and confidentiality, as well as issues of compatibility with the current infrastructure. It is necessary to take these issues into account when developing and implementing projects using blockchain technology. Taking into account all of the above factors, it can be concluded that blockchain technology has a number of advantages that can be effectively used in the field of finance. However, in order to avoid risks and ensure the successful implementation of projects, it is necessary to take into account the existing problems and limitations associated with this technology. Despite this, blockchain technology is the optimal solution for many areas of financial transactions, as it provides reliability, security and transparency of transactions. Due to its unique properties, blockchain technology can be effectively used in various areas of financial activity, such as banking, taxation, regulation, etc. However, despite this, blockchain technology represents an important step forward in the development of financial technologies and can play a key role in improving the efficiency and transparency of financial transactions. In

general, blockchain technology can be very effective in financial management and optimization of budget processes, but it is necessary to take into account the potential risks and difficulties associated with its implementation. It is also important to understand that the effectiveness of blockchain technology may vary depending on the specifics of the industry and the specific context.

References

1. Svon, M. (2017). Shema novoj jekonomiki [The scheme of the new economy]. OOO Olimp-Biznes.
2. Gidaspov, I. (2020). Chto takoe smart-kontrakt [What is a smart contract?]. https://currency.com/ru/chto-takoe-smart-kontrakt?utm_medium=cpc&utm_source=googleads_pmax&utm_campaign=CIS_PFM_APP_FTD_RU&utm_content=&campaignid=16914109425&adgroupid=&network=x&keyword=&matchtype=&creative=&adposition=&placement=&device=c&devicemodel=&
3. Governments Republic of Kazakhstan. (2017). Ob utverzhdenii Gosudarstvennoj programmy "Cifrovoj Kazahstan" [On establishing the state program "Digital Kazakhstan"]. https://primeminister.kz/assets/media/gosudarstvennaya-programma-tsifrovoy-kazakhstan-rus.pdf
4. Christopher, A. (2019). Blockchain: How it works. Solutions. https://www2.deloitte.com/kz/en/pages/strategy-operations/solutions/blockchain.html
5. Mark, M. (2019). *Can blockchain give an economy a competitive advantage?* https://www.ey.com/en_kz/government-public-sector/can-blockchain-give-an-economy-a-competitive-advantage
6. Tapscott, A., & Tapscott, D. (2017). How Blockchain Is Changing Finance. *Financial Markets*. https://hbr.org/2017/03/how-blockchain-is-changing-finance
7. Ibm.com. (2018). *What are smart contracts on blockchain?* https://www.ibm.com/topics/smart-contracts
8. Vox, P. (2021). Chto takoe smart-kontrakt i chem on luchshe jurista? [What is a smart contract and how is it better than a lawyer?]. https://voxpopuli.kz/chto-takoe-smart-kontrakty-i-chem-oni-luchshe-notariusa/
9. kapital.kz. (2021). V Otbasy banke vnedrili registraciju zaloga nedvizhimosti cherez Blockchain [Otbasy bank has implemented registration of real estate pledge via Blockchain]. https://kapital.kz/real_estate/99223/v-otbasy-banke-vnedrili-registratsiyu-zaloga-nedvizhimosti-cherez-blockchain.html
10. Donohue, B. (2014). Chudesa heshirovanija. Kriptografija [Wonders of hashing. Cryptography]. https://www.kaspersky.ru/blog/the-wonders-of-hashing/3633/?referer2=tcid_admitad_d23f342e510ad9a5225e6c32d352f23f_606171_x4&tagtag_uid=d23f342e510ad9a5225e6c32d352f23f
11. Howdoesitworktech.com. (2022). How secure is 256 bit security? BITCOIN – CRYPTO. https://howdoesitworktech.com/bitcoin-crypto/how-secure-is-256-bit-security/