UDC 004.42
IRSTI 81.93.29

THEORETICAL APPROACHES TO THE DEFINITION OF BLOCKCHAIN TECHNOLOGIES

O.A. Ussatova[1], İ. Soğukpinar[2], A.Sh. Barakova[3]
[1]Institute of Information and computational technologies of the SC MES RK, Almaty, Kazakhstan,
[2]Gebze Institute of Technology, Turkey
[3]Al-FarabiKazakh National University, Almaty, Kazakhstan
uoa_olga@mail.ru
balia_79@mail.ru
ORCID ID: https://orcid.org/0000-0002-5276-6118
ORCID ID: https://orcid.org/ 0000-0002-0408-0277
ORCID ID: https://orcid.org/0000-0002-0904-745X

Abstract. The article presents an analysis of blockchain technology. Blockchain is the best tool of the current decade. The possibility of using this innovative technology to ensure information security is shown. Blockchain technology was created to store transaction data. However, the structure of block chains using blockchain technology allows you to store various other metadata – catalogs, registries, directories, metadata databases, etc. This makes it possible to use blockchain technology for backup, information protection. The use of blockchain technology can provide complete decentralization of domain names and distribution of content across a larger number of nodes, which will make it virtually invulnerable to cyber attacks The article identifies the technological aspects of the introduction of Blockchain technology, substantiates the main characteristics of this technology, and notes the accepted typology of Blockchain varieties depending on the specifics of implementation and technological features. There are varieties of algorithms for "consensus" agreements, both in the context of technologies.

Key words: blockchain technologies, private, public and consortium Blockchain, consensus matching algorithm

Introduction

Blockchain technology has gained great popularity in various fields of human activity over the past few years. This is largely due to the use of the principles of decentralized data exchange in distributed systems, that is, the absence of an intermediary performing the functions of a center confirming the authenticity of the exchange participants and the information transmitted by them [1]. The popularity of blockchain is also largely due to the fact that it has been developed as a secure technology: it uses both cryptographic methods of protecting information and other ways to ensure the authenticity, confidentiality and integrity of information. Of course, blockchain also has certain limitations compared to centralized exchange technologies. This article does not aim to identify these positive and negative aspects; blockchain technology is considered from the standpoint of information protection: the functioning of protection mechanisms and the prevention of threats to information security. The paper presents a variant of the analysis of information protection mechanisms implemented in blockchain systems, which was performed using functional modeling IDEF0 [2].

Main part

Based on the characteristics of the Blockchain, functional features, three types of networks are distinguished: public, private and consortium [3].

A public Blockchain assumes that it is possible for any participant on the Internet to join or exit the Blockchain network without the need to provide identification forms or request permission [4].

A private blockchain assumes that all network participants are known and trustworthy; belong to a controlled community. Subjects can be both individuals, such as employees and

customers, and organizations (companies or departments within companies). Users of a private network can have certain types of access to write to the registry. Private Blockchain accounts for the majority of corporate, industrial and government projects. Various other parties may have different private read-only representations of the data (e.g. regulatory officials).

The consortium's blockchain combines elements of a public and private blockchain. An authorized group functions as validators, the visibility of the network can be limited by validators, authorized persons or have no restrictions. Based on the features of the Blockchain typology, the following weak and strong characteristics of the corresponding network varieties can be distinguished (Table 1).

Table 1. Theoretical approaches to the definition of Blockchain technologies

Charact eristic	Type of Blockchain		
	pr ivate	p ublic	conso rtium
Strengths	1. Unification of the verified participants underone umbrella with greater control and proof of authority. 2. The ability to cancel Transactions if necessary. 3. A smaller pool of trusted individuals to negotiate software changes (consensus	1. Using the power of the crowd around the world and aligning with a common value. 2. The ability to have immutable data by distributing agreed algorithms on a larger scale	1. A high degree of possible changes to the network. 2.Higher scalability and greater confidentiality of transactions 3. It is most advantageous in conditions when several organizations work in the same industry 4.Reducingtransac tional outages and data redundancy,
Weaknesses	1.The agreed rules can be changeable, threatening the immutability of data where the number of participants is small	1. At the mercy of potentially unknown participants. 2. Changes in the consensus are not possible depending on the architecture of the system	1. Narrow scope of effective application

An important innovation of the Blockchain protocol is the consensus consensus algorithm, which allows you to build an open distributed network where all parties can come to an agreement [3]. This mechanism is designed to ensure the achievement of overall reliability in a distributed network of registers. It is assumed that 51% coordinates the content stored in the register network [5].

In the public Blockchain, the algorithms of "Proof of Work" (Proof of Work (PoW) and "Proof of Ownership" (Proof of Stake (PoS) are the most common and popular consensus algorithms.

The Proof-of-Work (PoW) algorithm is designed in such a way that it requires all nodes in

the network to be supervised for a fee when adding a block of records to the end of the chain. This competition involves finding a one-time number by simply using computing power [1]. This creates a model of stimulation, according to which the winning node, which adds a block to the block chain, receives a reward with digital tokens – a bit of us. To hack the network, an attacker is forced not only to fight for the right to add a block, but also to compete for the creation of the longest chain. This undermines the economic incentives of attacks, making them financially costly (the type of attack is Sybil attack).

The Proof of Stake (PoS) algorithm [1] assumes that the miner or validator who creates a new block is selected in a deterministic manner depending on his wealth or share [15]. The concept of this protocol assumes an increase in the probability of a node's success in creating new digital tokens in proportion to the number of digital tokens already owned by the node. The rationale is that the more digital tokens a node owns, the greater the node's interest in protecting the network

The matching algorithm protects the network without using computing power as a means of protection against attacks and reduces the entry barrier, eliminating the advantages associated with the use of specialized equipment [6]. Thus, PoS is a cheaper and more environmentally friendly distributed form of a consistent algorithm. This protocol was first implemented for the Peercoin cryptocurrency [1]

The Delegated Proof of Stake (DPoS) algorithm [7] serves to stimulate interested parties and encourage them to participate in the network by delegating or transferring their coins to larger interested parties [8].

In a private Blockchain, a common consensus algorithm is the "Byzantine Fault Tolerance Problem" (PBFT), which provides consensus regardless of malicious behavior on the part of some participating nodes [7]. Within the framework of this agreement protocol, all nodes are connected to each other, and legitimate nodes reach a system agreement based on the majority rule. The consensus assumes that the number of malicious nodes cannot be equal to or greater than 33% of all nodes in the network. The consensus protocol requires all clients on the network to authenticate and log in to send transactions to validators [1].

The Proof of Elapsed Time (PoET) algorithm is a private consistent mechanism of the block chain, which requires all participating nodes to identify themselves before they participate in the network [9]. PoET is based on a fair lottery system based on Intel Guard Guard technology , where each participant has an equal opportunity to be a winner among all network participants. The fault-tolerant consensus algorithm "Raft" follows the "leader-follower" model, when the leader is elected to make decisions about the general states of the network and transfers changes to the follower nodes. The selection process, based on random timeout settings, occurs when the leader is absent or unresponsive for a predetermined period of time.

The Ripple matching algorithm (RPCA), developed in 2014 [9], is another well-established protocol based on tokens without the use of mining. Ripple's goal is to provide secure, instant, cheap international financial transactions of any size of non-refundable payments. In addition to the main developed protocols, some less popular ones can be added [10].

The Proof of Activity (PoA) algorithm combines components from PoS and PoW. This hybrid protocol ensures the functioning of the network at a lower cost of electricity.

The Proof of Vote (PoV) algorithm is based on the Bitcoin platform. The mechanism is aimed at "establishing other identification information without danger to network participants so that the decision on the submission and verification of blocks is made by a vote of agencies, regardless of the intermediary activity of a third party or uncontrolled public awareness." Compared to the main protocols, PoV aims to provide more controlled security and low latency during the time required to verify a transaction.

The Proof of Importance (PoI) algorithm uses the importance indicator to select block generators based on ownership of a share of a common crypto currency and interaction with other nodes in order to stimulate the distribution and transit of its own tokens [10]. The consensus mechanism is presented in the NEM blockchain. The "Zero-Knowledge Proof" algorithm allows the certifying party to prove to the verifier that the statement is true without revealing any other

information. A comparison of the various characteristics of the consensus is given in Table 2.

Table 2. Comparison of the basic characteristics of different types of consensus Blockchain technologies

Specifications	oW	PoS	PoET	PBFT	DPOS	Ripple
Transaction cost	High	High	Average	Low	Average	Low
Electricity consumption	High	Average	-	Low	Average	Low
Scalability	High	High	High	Low	Low	Low
Required amount of data storage	High	High	High	High	Average	Average

Conclusion

The introduction of Blockchain technology creates opportunities both at the level of the state, industries, and commercial organizations to use advanced innovations to increase the efficiency of production and business processes, reduce costs, etc. The existing IT potential of our country and the developed digital infrastructure in the conditions of state support create a solid foundation for the effective solution of this problem.

References

[1] Лелу, Л. Блокчейн от А до Я. Все о технологии десятилетия. – М.: Эксмо, 2018. 256.

[2] Integration DEFinition for function modeling (IDEF0). Draft Federal Information Processing Standards Publication. 183. 1993. URL: http://idef.com/wp-content/uploads/2016/02/idef0.pdf. (дата обращения 19.02.2019 г.).

[3] Melanie Swan. Blockchain for Business: Next- Generation Enterprise Artificial Intelligence Systems. Advances in Computers. 2018. Elsevier. 42. DOI: 10.1016/bs.adcom.2018.03.013.

[4] Roy Lai, David Lee, Kuo Chuen. Blockchain – From Public to Private. Handbook of Blockchain, Digital Finance and Inclusion. 2018. 2. Elsevier. 146–177. DOI: 10.1016/B978-0-12-812282-2.00007-3.

[5] Peng Zhang, Douglas C. Schmidt, Jules White, Abhishek Dubey. Consensus mechanisms and information security technologies. Advances in Computers. 2019. 115. 181–209. DOI: 10.1016/bs.adcom.2019.05.001.

[6] Riya Thakore, Rajkumar Vaghashiya, Chintan Patel, Nishant Doshi. Blockchain – based IoT: A Survey. 2nd International Workshop on Recent advances on Internet of Things: Tnrhnology and Application Approaches (IoT-T&A 2019). Halifax, Canada. Procedia Computer Science. 2019. 155. 704–709. DOI: 10.1 016/j. procs.20s9.08.101.

[7] Rakesh Shrestha, Rojeena Bajracharya, Anish P. Shrestha, Seung Yeob Nam. A new type of Blockchain for secure message exchange in VANET. Digital Communications and Networks. 2019. 10. DOI: 10.1016/j.dcan.2019.04.003.

[8] Larimer D. Delegated proof of stake, Bitshares.org, 2014. Online. Available at: http://107.170.30.182/security/delegated-proof-of-stake.php (accessed 10 May 2020).

[9] Intel Corporation. Proof of Elapsed Time, Sawtooth Lake, 2017. Online. Available at: https://sawtooth.hyperledger.org/docs/core (accessed 10 September 2020).

[10] Sophocles Theodorou, Nicolas Sklavos. Blockchain-Based Security and Privacy in Smart Cities. Smart Cities Cybersecurity and Privacy 2019. Elsevier Inc. 21–37. DOI:10.1016/B978- 0-12-815032-0.00003-2.

БЛОКЧЕЙН-ТЕХНОЛОГИЯСЫН АНЫҚТАУДЫҢ ТЕОРИЯЛЫҚ КӨЗҚАРАСТАРЫ

О. А. Усатова[1], И. Согукпынар[2], A.Sh . Баракова[3]
[1]Ақпараттық және есептеуіш технологиялар институты, Алматы, Қазақстан,
[2]Гебзе технологиялық институты, Түркия
[3]Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан
uoa_olga@mail.ru
balia_79@mail.ru
ORCID: https://orcid.org/0000-0002-5276-6118
ORCID ID: https://orcid.org/ 0000-0002-0408-0277
ORCID: https://orcid.org/0000-0002-0904-745X

Аңдатпа. Мақалада Blockchain технологиясын талдау ұсынылған. Блокчейн-бұл онжылдықтың ең жақсы құралы. Ақпараттық қауіпсіздікті қамтамасыз ету үшін осы инновациялық технологияны пайдалану мүмкіндігі көрсетілген. Blockchain технологиясы транзакция деректерін сақтау үшін жасалды. Алайда, блокчейн технологиясын қолданатын блокчейн тізбегінің құрылымы басқа метадеректерді – каталогтарды, тізілімдерді, анықтамалықтарды, метадеректер базасын және т.б. сақтауға мүмкіндік береді. Блокчейн технологиясын қолдану домендік атауларды толық орталықсыздандыруды және мазмұнды көптеген түйіндерге бөлуді қамтамасыз ете алады, бұл оны кибершабуылдарға іс жүзінде қол сұғылмайтын етеді. Мақалада Blockchain технологиясын енгізудің технологиялық аспектілері анықталады және осы технологияның негізгі сипаттамаларын негіздейді және блокчейннің қабылданған типологиясы атап өтіледі. Технология контекстіндегідей "консенсус " келісімдерінің әртүрлі алгоритмдеріне талдаулар жасалады.

Кілттік сөздер: Blockchain технологиясы, жеке, қоғамдық және консорциум блокчейні, консенсус алгоритмі.

ТЕОРЕТИЧЕСКИЕ ПОДХОДЫ К ОПРЕДЕЛЕНИЮ БЛОКЧЕЙН-ТЕХНОЛОГИЙ

О.А. Усатова, И. Согукпынар[2], A.Sh . Баракова[3]
[1]Институт информационных и вычислительных технологий, Алматы, Казахстан,
[2]Технологический институт, Гебзе, Турция
[3]Национальный университет имени Аль-Фараби, Казахстан, Алматы, Казахстан
uoa_olga@mail.ru
balia_79@mail.ru
ORCID: https://orcid.org/0000-0002-5276-6118
ORCID ID: https://orcid.org/ 0000-0002-0408-0277
ORCID: https://orcid.org/0000-0002-0904-745X

Аннотация. В статье представлен анализ технологии блокчейн. Блокчейн - лучший инструмент текущего десятилетия. Показана возможность использования этой инновационной технологии для обеспечения информационной безопасности. Технология блокчейн была создана для хранения данных о транзакциях. Однако структура цепочек блоков с использованием технологии блокчейн позволяет хранить различные другие метаданные – каталоги, реестры, справочники, базы данных метаданных и т.д. Это дает возможность использовать технологию блокчейн для резервного копирования, защиты информации. Использование технологии блокчейн может обеспечить полную децентрализацию доменных имен и распределение контента по большему числу узлов, что сделает его практически неуязвимым для кибератак В статье определены технологические аспекты внедрения технологии блокчейн, обоснованы основные характеристики этой технологии и отмечена принятая типология блокчейна разновидности в зависимости от специфики реализации и технологических особенностей. Существуют различные алгоритмы для "консенсусных" соглашений, как в контексте технологий.

Ключевые слова: блокчейн-технологии, частный, публичный и консорциумный блокчейн, алгоритм согласования консенсуса.

Сведения об авторах

Англ: Olga Aleksandrovna Ussatova- PhD, Institute of Information and computational technologies, Almaty, Kazakhstan

Каз: Усатова Ольга Александрқызы - PhD, Ақпараттық және есептеуіш технологиялар институты, Алматы, Қазақстан

Рус: Усатова Ольга Александровна- PhD, Институт информационных и вычислительных технологий, Алматы, Казахстан

Англ: İbrahim SOĞUKPINAR- professor Computer engineering, Gebze Institute of Technology,Turkey

Каз: Ибрагим Согукпынар-Есептеу техникасының профессоры, Технологиялық институт, Гебзе, Түркия

Рус: Ибрагим Согукпынар – профессор вычислительной техники Технологический институт, Гебзе, Турция

Англ:Aliya Sharizatovna Barakova- doctoral student, Al-Farabi Kazakh National University, Almaty, Kazakhstan

Каз: Баракова Алия Шаризатқызы- докторант, әл-Фараби атындағы ҚазҰУ, Алматы, Қазақстан

Рус: Баракова Алия Шаризатовна- докторант, Казахский национальный университет им. аль-Фараби, Алматы, Казахстан