УДК 004.056
https://doi.org/10.47533/2023.1606-146X.23

A. M. TURSYNKHAN[1]*, L. M. ALIMZHANOVA[1] ,
MARIA SKUBLEWSKA-PASZKOWSKA[2]

[1]Al-Farabi Kazakh National University, Almaty, Kazakhstan
[2]Lublin University of Technology, Lublin, Poland
Tursynhan.aynur@mail.ru; Lauralim01@gmail.com; maria.paszkowska@pollub.pl

USING BLOCKCHAIN TECHNOLOGY FOR MONITORING BUSINESS PROCESSES IN ERP SYSTEMS

Database protection is one of the most difficult tasks facing the departments responsible for ensuring information security. On the one hand, to work with the database, it is necessary to provide access to data to all employees who, on duty, must collect, process, store and transfer confidential data. On the other hand, the expansion of databases does not always have a centralized architecture, and therefore the actions of violators are becoming more sophisticated. Thus, there is no clear and precise methodology for a comprehensive solution to the problem of protecting databases that could be applied in all cases; in each specific situation, an individual approach has to be found. Blockchain technology can solve some of these problems. The purpose of the study was to show the possibilities of blockchain technology for tracking possible external and internal attacks on Control Systems and their databases. It is proposed to combine and blockchain-based hashing methods in alphanumeric format and explore its application in tracking and monitoring the sequence of business process transactions in ERP systems. A cyber attack on transaction data in ERP systems will immediately affect the root of the Merkle tree, which can serve as a signal that the system has been hacked. We show that blockchain, considered one of the most disruptive technologies in various industries, certainly has the potential to apply and ensure the security of enterprise management systems in the ERP format.

Key words: *blockchain, information security, cyber attacks, distributed ledger, Merkle tree, ERP, hashing.*

Introduction. Cybersecurity is becoming increasingly important for both governments and businesses. Information security, one of the components of cybersecurity, focuses on protecting the integrity and confidentiality of data as it is collected, stored and used. Data-related people, processes, and technologies work together to create and maintain security.

Currently, a large number of cyber attacks are successful for several reasons: they do not depend on the location of the cybercriminal and the remoteness of the potential victim, as well as time frames and time zones. A hacked IT environment can lead to business-critical consequences, including damage to reputation and lowering the level of trust on the part of customers, seizing valuable information, integrating virus and malware, and more, due to the fact that organizations data can get into into the wrong hands. Infrastructure hacking is also associated with financial risks: leakage of confidential information about the company itself, its bank details and financial flows, confidential information of customers and suppliers, as well as the outflow of customers and the loss of the organization's unique innovative developments, its competitiveness can significantly drop in the market. The situation is complicated by the fact that the methods and tactics of attackers are constantly evolving. Hackers are constantly adapting their attacks to new realities and technologies. Modern

* E-mail корреспондирующего автора: Tursynhan.aynur@mail.ru

cyberattacks are automated as much as possible, which allows attackers to accelerate their implementation and use artificial intelligence to increase the success of their implementation. The protection tools used today effectively fulfill their task of ensuring security - they block typical attacks, but they are not yet perfect in relation to point, manual threats.

According to statistics for 2022, DDoS attacks, phishing and videoconferencing attacks topped the list of cyber threats. However, other types of attacks bring no less problems to both businesses and ordinary users.

Security should be both at the technical level, which includes all the necessary tools to protect the infrastructure, and at the organizational level - company employees should always be aware of the latest news in the field of information security and current techniques of cybercriminals. Only a comprehensive and active approach to ensuring information security will achieve a high level of security and keep confidential data within the organization [1].

Regarding the blockchain: it is worth acknowledging that this is a rather familiar concept, which initially surfaced when Satoshi Nakamoto introduced Bitcoin in 2008 [2]. It is known that bitcoin is the most famous implementation of the blockchain, and in fact, it is the implementation of the cryptocurrency. Nevertheless, blockchain extends beyond its association with cryptocurrencies, as it serves as a foundational technology and framework for recording currency transactions between untrusted participants. In present times, blockchain technology, or its derivatives, is integrated into various domains beyond cryptocurrencies. Numerous applications now incorporate blockchain technology, including energy trading, healthcare, supply chain management, manufacturing, identity management, e-government, and many more. This expansion highlights the versatility and potential of blockchain in diverse industries and sectors [18,19].

Blockchain is a distributed ledger, referring to how a database is distributed among multiple peer-to-peer network participants without oversight of the process by a central authority. When it comes to blockchain, the ledger is organized precisely as its name suggests – as an ordered chain of blocks, with each block containing a sequence of transactions. A block is essentially a structure comprising a header and a body that holds the transactions in a specific order. The blocks are timestamped and digitally signed by the entity that creates them. These blocks are linked together to form a chain through a reference to the previous block. The header of each block includes the cryptographic hash of the previous block, ensuring the integrity and immutability of the entire chain. This linkage guarantees that any modification to a previous block would invalidate subsequent blocks, making it extremely difficult to tamper with the data without detection. The first block in a blockchain, which initiates the chain, is referred to as the «genesis block» [3]. It serves as the foundation upon which subsequent blocks are added, creating an unbroken chronological sequence of transactions. This structure of ordered blocks, with cryptographic linkage and timestamping, establishes the core characteristics of a blockchain, enabling secure and transparent record-keeping across a network of participants. (Fig. 1).

Indeed, in blockchain technology, the ledger is distributed among participants in a decentralized network, eliminating the need for central control. In public, non-permissioned blockchains, all network participants possess a copy of the ledger. However, in other types of blockchains, which may be more complex or restrictive, subsets of participants may

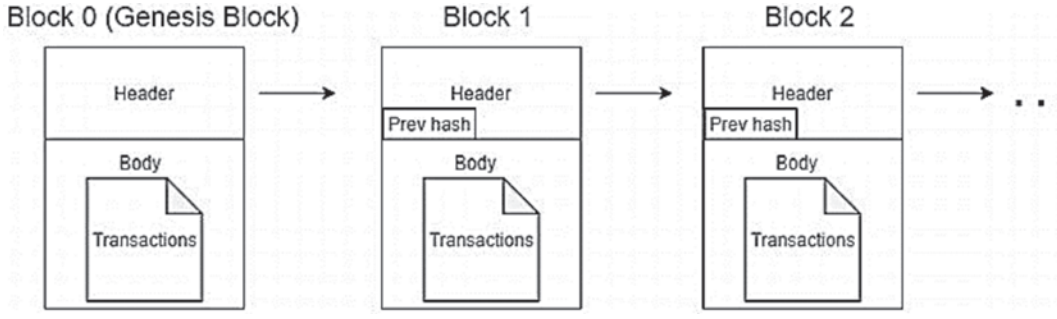

Figure 1 – Blockchain as a chain of blocks

hold different ledgers. Hyperledger Fabric serves as an example of a restricted blockchain technology that allows nodes to be segregated into different channels, with nodes in the same channel maintaining identical copies of the ledger. This segregation ensures privacy and data segregation within the network [4]. While the distribution of ledgers among participants raises concerns about ledger synchronization and the potential for participants to promote their own versions of the ledger or transactions, blockchain employs consensus mechanisms to address these issues [20].

Consensus mechanisms are protocols that enable participants in a blockchain network to agree on the validity and order of transactions. These mechanisms ensure that all participants reach a shared consensus on the state of the ledger. Common consensus mechanisms include Proof of Work (PoW), Proof of Stake (PoS), Practical Byzantine Fault Tolerance (PBFT), and more [5]. By requiring participants to agree on the validity of transactions and the order in which they are added to the ledger, consensus mechanisms prevent individual participants from manipulating the ledger for personal gain. Consensus ensures that any changes to the ledger are agreed upon by a majority of participants, maintaining the integrity and trustworthiness of the blockchain system [6,21]. The proof of work mainly consists of solving a computationally complex problem (related to the block itself) as a condition for inserting the block into the chain. Blockchain participants compete to solve this problem in exchange for a reward. The problem is difficult to solve, but easy to check so that other participants can easily check the solution of the problem and agree on a new block. This algorithm guarantees consensus as long as no single participant has more than half of the computing power of the network due to high power consumption. This high power consumption and wastage of computing power is causing blockchain networks like Ethereum to migrate to lighter consensus algorithms like Proof of Stake [7,22].

The most commonly used cryptographic function in Proof of Work is the hash. The hash or hash function is one of the main components of modern cryptography and the blockchain algorithm. Hashing is the transformation of any amount of information into a unique set of characters that is unique to this array of incoming information. This set of characters will be called a hash.

The hash function has several required properties:

– The hash is always unique for each piece of information. However, sometimes there are so-called collisions, when the same hash codes are calculated for different input blocks of information.

– With the slightest change in the input information, its hash changes completely.

– The hash function is irreversible and does not allow restoring the original array of information from a character string. This can be done only by sorting through all possible options, which, with an infinite amount of information, requires a lot of time and money.

– Hashing allows you to quickly calculate the desired hash for a sufficiently large amount of information.

– The algorithm of the hash function, as a rule, is made open so that, if necessary, it is possible to evaluate its resistance to restoring the initial data using the issued hash.

– A hash function must be able to convert any amount of data to a number of a given length [8].

The use of hashes in blockchain helps guarantee the integrity of the transaction chain and protects it from unauthorized modifications. Each block in the blockchain contains a hash that represents the data within that block. This hash is calculated based on the data's contents using a cryptographic hash function. Any alteration in the data would result in a different hash value, immediately signaling that the data has been tampered with. The distributed nature of blockchain makes it highly resistant to hacking attempts. When a network participant, known as a miner, discovers a hash solution that meets certain criteria, they can assemble a new block and broadcast it to the network. Other participants can then verify the validity of the block by checking its association with the previous block and confirming that it satisfies the network's required properties. Consensus is achieved when all participants have the same set of blocks, forming the longest blockchain [9]. Hashes are also instrumental in verifying data integrity and facilitating the cryptographic signature process. By generating hashes of data and comparing them, the integrity of the data can be verified without revealing the original content. Additionally, cryptographic signatures utilize hash functions to provide authenticity and non-repudiation, ensuring that the data or transaction was indeed generated by the claimed party. When constructing a blockchain architecture, the default structure typically consists of blocks linked together in a sequential chain, with each block containing a hash of its data and a reference to the previous block, establishing a secure and tamper-evident record of transactions[10]. If it builds a blockchain architecture, then by default it looks like this (Fig. 2).

Thus, the benefits that can be obtained using the blockchain are obvious. What makes us accept a network with such a load of processing and redundancy? All this complexity is necessary to create a decentralized network consisting of many participants who reach a common consensus without the intervention of a central authority; create a transparent and immutable ledger that you can check yourself; establish a contract without the intervention of a notary (in fact, applications running on the blockchain are known as smart contracts) [23]. And all these goals are achieved with a sufficient level of reliability and availability. At the same time, blockchain does not solve all problems. This is not a suitable solution for systems managed by a single central authority, or for storing data whose integrity and origin are irrelevant. This is a new paradigm that provides deterministic contract performance and data integrity in the registry with full guarantees and without third party interference.

Research methodology and results. Once blockchain technology has been implemented, the focus is on fulfilling the information security properties that it provides. By focusing on data integrity, the blockchain ledger is immutable. Each transaction in a block

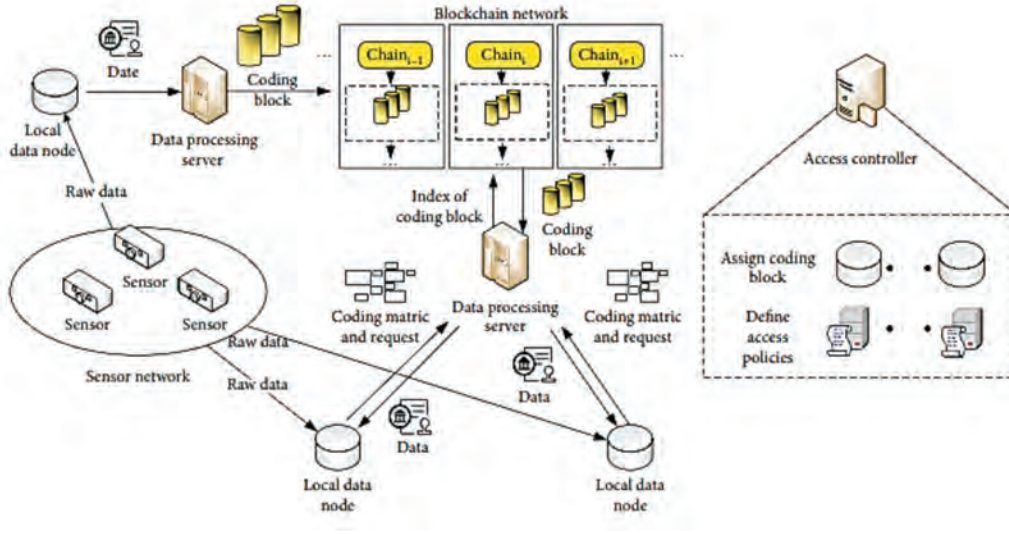

Figure 2 – Architectura of system

is cryptographically signed by its sender, each block in the blockchain is cryptographically signed by its miner, each block contains the hash of the immediately preceding block, and all participants in the blockchain network reach consensus on the chain. In order to change a single transaction on the blockchain, an attacker must change each subsequent block accordingly, solve the consensus problem of this block and subsequent blocks, and convince more than 50% of the network participants to accept the new chain. This situation is almost impossible due to the properties of hashing and the amount of computing and electrical power required to achieve this goal. Blockchain is resistant to hacking, and integrity is its greatest advantage [11,24].

Consider an application of a Merkle tree that uses hashing to transform large amounts of information into a single string. This allows you to prove that the transaction was included in a large data set. The technology is named after Ralph Merkle, who proposed it in 1987. A binary Merkle tree is a data structure that is created by combining hashes [12].

The construction of a Merkle tree involves the following steps (Fig.3):

– Calculate Transaction Hashes: Start by calculating the hash of each individual transaction in the block. For example, hash(L1), hash(L2), hash(L3), and so on, where L1, L2, L3 represent the transactions.

– Pairwise Hash Calculation: Combine the hashes in pairs and calculate the hash of their concatenation. If the number of transactions is odd, duplicate the last transaction and add it to itself before pairing. For example, calculate hash (hash(L1) + hash(L2)), hash(hash(L3) + hash(L3)), and so on. This ensures an even number of elements at each level of the Merkle tree.

– Repeat Hash Calculation: Repeat the pairwise hash calculation process with the newly generated hashes from the previous step until you reach a single hash known as the Merkle root. The Merkle root represents the top-level hash of the Merkle tree and serves as a cryptographic proof of the integrity and order of all transactions in the block. The value of the Merkle root is included in the block header.

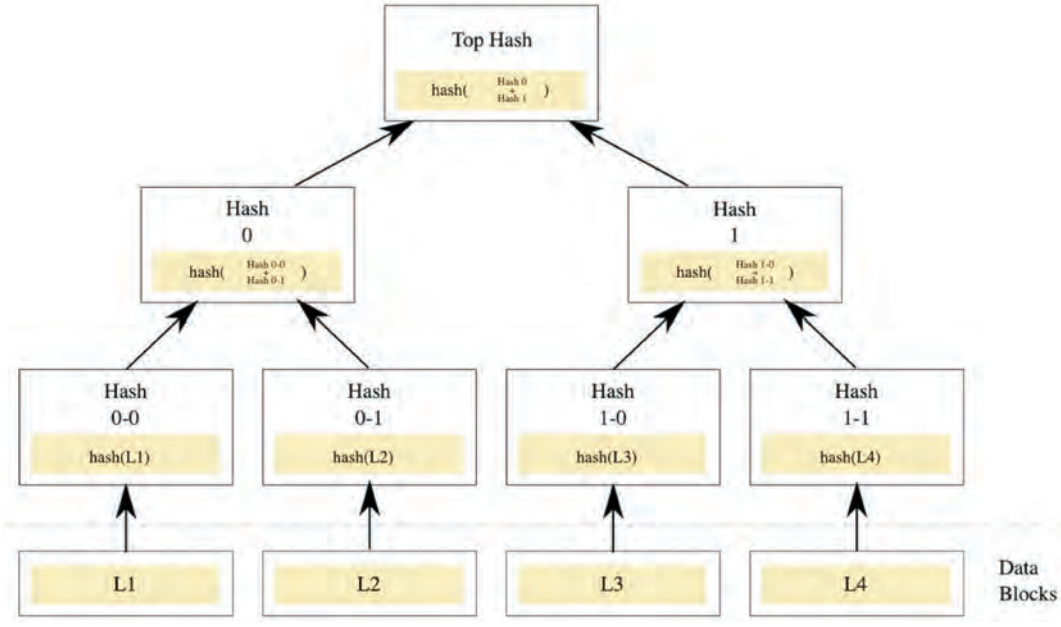

Figure 3 – Merkle tree

A hashing variant is proposed, where each block is formed with an alphanumeric code, where the numerical coefficients will be formed according to the simplest hashing principle as the sum of the initial data from those included in the hash. The literal content of the block will be formed depending on the serial number of this letter in a particular alphabet (for example, in Latin). For example (Fig.4):

Thus, each step will convert not only the numerical coefficient, but also its literal component. In this case, when building a Merkle tree, the main task is not so much to encrypt block data, but rather to track the sequence of transactions. At the same time, one should not forget that modern complex ERP systems, such as Oracle, SAP and others, use transactions with an alphanumeric code to form business processes of various modules, which can allow tracking the irreversible sequence of a transaction using the proposed alphanumeric hashing based on blockchain. This implies the need to provide an unambiguous relationship between alphanumeric hashing and alphanumeric encoding of transactions in the process of functioning of the ERP system [13,14].

It must be understood that the Merkle Root is responsible for summarizing the data present in specific transactions, all of which is stored directly in the block header [15]. This method maintains data integrity. In the event that at some point one detail in a transaction is changed, the Merkle root will automatically change along with it.

The integrity of the transaction is easy to verify in no time. Due to the way the data is structured, the validation process requires very little memory usage and the processing power required is greatly reduced.

Since blockchains are usually composed of hundreds of thousands of blocks, each of which can contain up to several thousand transactions, two main problems appear: memory

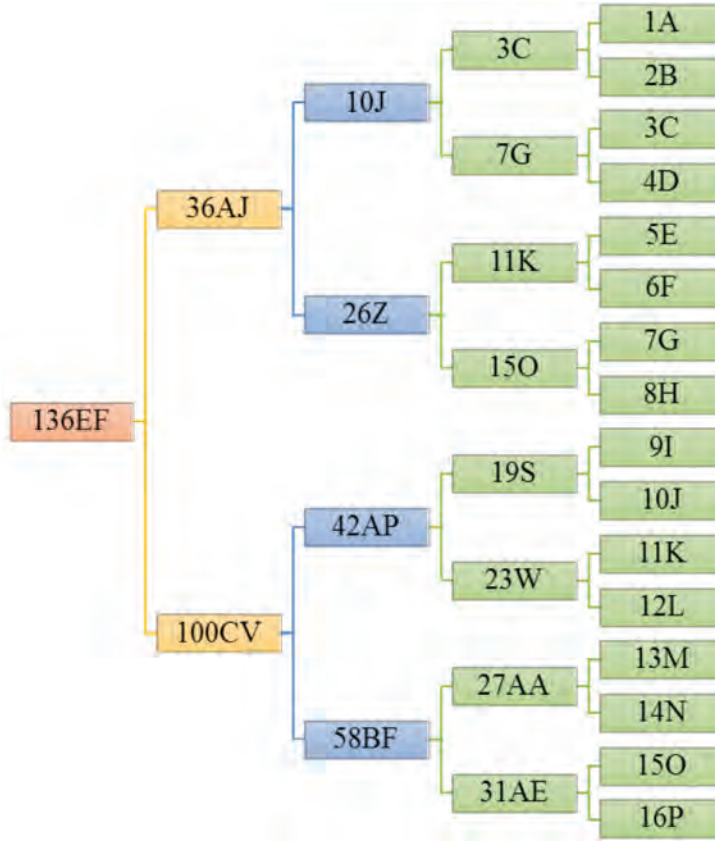

Figure 4 – Merkle tree in our version

size and computing power. Every node in the network would maintain a complete copy of a transaction that ever took place on the blockchain if Merkle trees were not used on the blockchain. The node would have to compare each record line by line when verifying the transaction to make sure they match the network records exactly. Network security can be compromised if there is any discrepancy between the two. To compare the records and make sure that there were no changes, the computer would need much more processing power.

Merkle trees, on the other hand, offer a solution to this problem by drastically reducing the amount of data you need to have on hand. They hash each entry in the registry, effectively separating the data itself from the evidence supporting it [16]. Without knowing each individual TXID in a block, you can check the TXID using a merkle root with a hash tree. A Merkle Tree is a great way to show part of the data without having to download the entire set. Therefore, less processing power is required to verify transactions.

Conclusion. As a result of the study, an alphanumeric hashing scheme using a modified Merkle tree is proposed. Moreover, the literal part of hashing must not only be taken into account, but a logical, analytical justification should be brought under it. There is also a rational basis for the relationship between alphanumeric hashing and alphanumeric encoding of transactions during the operation of an ERP system. This approach can provide some security in tracking irreversibility and monitoring possible cyber attacks that violate

and distort the merkle tree root. This will ensure control over a clear sequence of transactions and their appropriate coding in the main business processes of the ERP system [17]. In this work, the methods associated with ensuring security were used, while the blockchain technology does not have direct access to cryptocurrencies, but goes to a different level and field of application.

REFERENCES

1 The main types of attacks on infrastructure and the concept of protection against them [Electronic resource] / Murad Mustafaev - Access mode: https://onlanta.ru/press/smi/osnovnye-vidy-atak-na-infrastrukturu-i-kontseptsiya-zashchity-ot-nikh/

2 Artem Genkin, Alexei Mikheev. Blockchain. How it works and what awaits us tomorrow. — M.: Alpina Publisher, 2017. — 30-42c.

3 Kim, M. G., Lee, A. R., Kwon, H. J., Kim, J. W. and Kim, I. K.,"Sharing Medical Questionnaries based on Blockchain," IEEE International Conference on Bioinformatics and Biomedicine (2018), 2767-2769.

4 Emelyanov R.V., Rysin M.L., Valenzuela Boldyrev P.P., Shamanin A.Yu., "Blockchain technology to improve the quality of the construction documentation process in the nuclear industry," CHNICAL DEVELOPMENT OF RUSSIA AND THE WORLD: collection of articles of the IV International Scientific and Practical Conference. - Saratov: NOP "Digital Science". - 2023. - 299 p.

5 Habib, G.; Sharma, S.; Ibrahim, S.; Ahmad, I.; Qureshi, S.; Ishfaq, M. Blockchain Technology: Benefits, Challenges, Applications and Integration of Blockchain Technology with Cloud Computing. Future Internet 2022, 14, 341.

6 Kiayias, A.; Russell, A.; David, B.; Oliynykov, R. Ouroboros: A provably secure proof-of-stake blockchain protocol. In Proceedings of the Advances in Cryptology—CRYPTO 2017: 37th Annual International Cryptology Conference, Santa Barbara, CA, USA, 20–24 August 2017; Proceedings, Part I.. Springer: Berlin/Heidelberg, Germany, 2017.

7 Vairagade, R.S.; Brahmananda, S.H. Enabling machine learning-based side-chaining for improving QoS in blockchain-powered IoT networks. Trans. Emerg. Telecommun. Technol. 2022, 33, e4433.

8 Хеширование // wikipedia.org URL: https://ru.wikipedia.org/wiki/Хеширование (дата обращения: 26.06.18).

9 Jahan F, Mostafa M, Chowdhury S (2020) SHA-256 in parallel blockchain technology: storing land related documents. Int J Comput Appl 975:8887

10 Alsunaidi SJ, Alhaidari FA (2019) A survey of consensus algorithms for blockchain technology. In: 2019 International conference on computer and information sciences (ICCIS). IEEE, Apr 2019, pp 1–6

11 J. Wang, W. Ou, W. Wang, R. Simon Sherratt, Y. Ren et al., «Data security storage mechanism based on blockchain network,» Computers, Materials & Continua, vol. 74, no.3, pp. 4933–4950, 2023.

12 P. Dhiman, S. K. Henge, S. Singh, A. Kaur, P. Singh et al., «Blockchain merkle-tree ethereum approach in enterprise multitenant cloud environment,» Computers, Materials & Continua, vol. 74, no.2, pp. 3297–3313, 2023.

13 Dasaklis, T.; Voutsinas, T.; Mihiotis, A. Integrating blockchain with Enterprise Resource Planning systems: Benefits and challenges. In Proceedings of the 25th Pan-Hellenic Conference on Informatics, Volos, Greece, 26–28 November 2021; pp. 265–270.

14 Bjelland, E.; Haddara, M. Evolution of ERP systems in the cloud: A study on system updates. Systems 2018, 6, 22.

15 A. S. Yahaya, N. Javaid, R. Khalid, M. Imran and N. Naseer, “A blockchain based privacy-preserving system for electric vehicles through local communication,” in Proc. of IEEE Int. Conf. on Communications (ICC), Ireland, pp. 1–6, 2020.

16 P. C. Wei, D. Wang, Y. Zhao, S. K. S. Tyagi and N. Kumar, “Blockchain data-based cloud data integrity protection mechanism,” Future Generation Computer Systems, vol. 102, pp. 902–911, 2020.

17 Kitsantas, T. Exploring Blockchain Technology and Enterprise Resource Planning System: Business and Technical Aspects, Current Problems, and Future Perspectives. Sustainability 2022, 14, 7633.

18 Bodkhe U, Tanwar S, Parekh K et al (2020) Blockchain for industry 4.0: a comprehensive review. IEEE Access 8:79764–79800

19 Tan C, Chen M-j, Ackah AE (2020) Research on distributed identity authentication mechanism of IoT device based on blockchain. Chin J Internet Things 4(02):70–77

20 Cao S-y, Yao Y-y, Chang X-l (2020) Lightweight secure authentication scheme using blockchain for RFID system in smart factory. Cyberspace Secur 11(09):70–77+93

21 Le L, Yong S (2020) Intelligent device authentication scheme based on blockchain technology. Comput Digit Eng 48(07):1722–1726

22 Xiong Z, Zhang Y, Niyato D, Wang P, Han Z (2018) When Mobile Blockchain meets edge computing. IEEE Commun Mag 56(8):33–39.

23 N. Khoshavi, G. Tristani and A. Sargolzaei, “Blockchain applications to improve operation and security of transportation systems: A survey”, Electronics, vol. 10, no. 5, pp. 629, 2021.

24 Feng, Y., Zhong, Z., Sun, X. et al. Blockchain enabled zero trust based authentication scheme for railway communication networks. J Cloud Comp 12, 62 (2023).

А. М.ТҰРСЫНХАН[1], Л. М. АЛИМЖАНОВА[1], М. СКУБЛЕВСКАЯ-ПАШКОВСКАЯ[2]

[1]әл-Фараби атындағы Қазақ ұлттық университеті, Алматы қаласы,Қазақстан
[2]Люблин технологиялық университеті, Люблин, Польша

ERP ЖҮЙЕЛЕРІНДЕГІ БИЗНЕС-ПРОЦЕСТЕРДІ БАҚЫЛАУ ҮШІН БЛОКЧЕЙН ТЕХНОЛОГИЯСЫН ҚОЛДАНУ

Мәліметтер қорын қорғау – ақпараттық қауіпсіздікті қамтамасыз етуге жауапты бөлімшелердің алдында тұрған ең күрделі міндеттердің бірі. Бір жағынан, деректер қорымен жұмыс істеу үшін кезекшілік кезінде құпия деректерді жинауға, өңдеуге, сақтауға және беруге тиіс барлық қызметкерлерге деректерге қолжетімділікті қамтамасыз ету қажет. Екінші жағынан, деректер қорын кеңейту әрқашан орталықтандырылған архитектураға ие бола бермейді, сондықтан бұзушылардың әрекеттері күрделірек болады. Осылайша, барлық жағдайларда қолдануға болатын мәліметтер қорын қорғау мәселесін кешенді шешудің нақты және тұрақты әдістемесі жоқ, әрбір нақты жағдайда жеке тәсілді табу керек. Блокчейн технологиясы осы мәселелердің кейбірін шеше алады. Зерттеудің мақсаты басқару жүйелеріне және олардың дерекқорларына ықтимал сыртқы және ішкі шабуылдарды бақылау үшін блокчейн технологиясының мүмкіндіктерін көрсету болды. Әріптік-цифрлық форматта блокчейн негізіндегі хэшинг әдістерін біріктіру және ERP жүйелеріндегі бизнес-процестердің транзакцияларының реттілігін қадағалау және бақылауда қолдануды зерттеу ұсынылады. ERP жүйелеріндегі транзакция деректеріне кибершабуыл Merkle ағашының тамырына дерегу әсер етеді, бұл жүйе бұзылғандығы туралы сигнал бола алады. Біз әртүрлі салалардағы ең серпінді технологиялардың бірі болып саналатын блокчейннің ERP фор-

матында кәсіпорынды басқару жүйелерін қолдану және қауіпсіздікті қамтамасыз ету мүмкіндігі бар екенін көрсетеміз.

***Түйін сөздер**: блокчейн, ақпараттық қауіпсіздік, кибершабуылдар, таратылған реестр, Merkle ағашы, ERP, хэшинг.*

А. М. ТҰРСЫНХАН[1], Л. М. АЛИМЖАНОВА[1], М. СКУБЛЕВСКАЯ-ПАШКОВСКАЯ[2]

[1]Казахский национальный университет им. аль-Фараби, г. Алматы
[2]Люблинский технологический университет, Люблин, Польша

ИСПОЛЬЗОВАНИЕ ТЕХНОЛОГИИ БЛОКЧЕЙН ДЛЯ МОНИТОРИНГА БИЗНЕС-ПРОЦЕССОВ В ERP-СИСТЕМАХ

Защита баз данных является одной из самых сложных задач, стоящих перед подразделениями, отвечающими за обеспечение информационной безопасности. С одной стороны, для работы с базой необходимо предоставлять доступ к данным всем сотрудникам, кто по долгу службы должен осуществлять сбор, обработку, хранение и передачу конфиденциальных данных. С другой стороны, укрупнение баз данных далеко не всегда имеет централизованную архитектуру, в связи с чем действия нарушителей становятся все более изощренными. Таким образом, четкой и ясной методики комплексного решения задачи защиты баз данных, которую можно было бы применять во всех случаях, не существует, в каждой конкретной ситуации приходится находить индивидуальный подход. Технология блокчейн может решить некоторые из этих проблем. Цель исследования состояла в том, чтобы показать возможности технологии блокчейн для отслеживания возможных внешних и внутренних атак на Системы управления и их базы данных. Предлагается объединить и методы хэширования на основе блокчейна в буквенно-числовом формате и исследовать его применение в отслеживании и мониторинге последовательности транзакций бизнес-процессов в ERP системах. Кибератака на данные по операциям в ERP системах сразу отразится на корне дерева Меркла, что может служить сигналом, что система подверглась внешнему взлому. Мы показываем, что блокчейн, считающийся одной из самых прорывных технологий в разных отраслях, безусловно, обладает потенциалом для применения и обеспечения безопасности систем управления организаций в формате ERP.

***Ключевые слова:** блокчейн, информационная безопасность, кибератаки, распределенный реестр, дерево Меркла, ERP, хеширование.*