UDC 657.6:008

JEL classification: M41, M42, D24

DOI: https://doi.org/10.35774/visnyk2021.04.156

Volodymyr MURAVSKYI,
Ds (Economics), Associate Professor,
Professor at the Department of Accounting and Taxation,
Western Ukrainian National University;
st. Lvivska, 11, Ternopil, 46020, Ukraine,
e-mail:vavanm@gmail.com
ORCID ID: 0000-0002-6423-9059

Nadiia KHOMA,
Candidate of Physico-Mathematical Sciences, Associate Professor,
Associate Professor at the Department of Economic Cybernetics and Informatics,
Western Ukrainian National University;
st. Lvivska, 11, Ternopil, 46020, Ukraine,
e-mail:nadiiakhoma@gmail.com
ORCID ID: 0000-0003-2981-0296

Larysa KHOKHLOVA,
Candidate of Physico-Mathematical Sciences, Associate Professor,
Associate Professor at the Department of Mathematics and Methods of Teaching,
Ternopil Volodymyr Hnatiuk National Pedagogical University;
st. Maxyma Kryvonosa 2, Ternopil, 46027, Ukraine,
e-mail: larysa_khokhlova@tnpu.edu.ua
ORCID ID: 0000-0002-9818-1051

Liu CHENGYU,
PhD student of the Department of Accounting and Taxation,
West Ukrainian National University,
Intermediate accountant, Lecturer,
Nanchang Institute of Science and Technology,
Nanchang City, Jiangxi Province, China,
e-mail: 1657426641@qq.com
ORCID ID: 0000-0002-0572-9322

OPEN DOCUMENT FLOW BASED ON BLOCKCHANE TECHNOLOGY FOR CYBER SECURITY OF THE ACCOUNTING SYSTEM

Muravskyi, V., Khoma, N., Khokhlova, L., Liu Chengyu. (2021). Vidkrytyi dokumentoobih na osnovi tekhnolohii blokchein dlia kiberzakhystu systemy obliku. [Open document

flow based on blockchane technology for cyber security of the accounting system]. *Visnyk economiky – Herald of Economics*, 4, 156–170. DOI: https://doi.org/10.35774/visnyk2021.04.156

Муравський В., Хома Н., Хохлова Л., Лю Чен'ю. Відкритий документообіг на основі технології блокчейн для кіберзахисту системи обліку. *Вісник Економіки*. 2021. Вип. 4. С. 156–170. DOI: https://doi.org/10.35774/visnyk2021.04.156

Abstract

Introduction. *To ensure cyber protection, the company's management resorts to isolating accounting information containing trade secrets from other information flows. However, confidential document management attracts significant attention from internal users and outsiders in order to gain unauthorized access. Due to active cyber threats, the isolation practice in the implementation of electronic information communications is ineffective for cybersecurity, which requires the development of new methods documentation and document circulation at the enterprise.*

The purpose of the *article is to study the benefits of open document management of enterprises based on blockchain technology to abandon the isolation of information flows in order to ensure cybersecurity of enterprises.*

Methods. *In the process of researching the disadvantages and advantages of isolation and open document management, general theotrtical(empirical, logical and historical) methods of cognition of reality are used. The research is based on scientifical methods of dislosing the economic processes, facts and phenomena from the standpoint of accounting and cybersecurity of enterprises. The information base of the article is selected historical documents on the development of blockchain technology, scientific works of scientists on block-chain structuring of accounting information, etc.*

Results.*The fundamental principles of blockchain technology in the conditions of its use for the organization of cybersecurity of accounting information are formed. The expediency of refusing to isolate information in favor of open document management in terms of maintaining trade secrets of the enterprise is substantiated. The method of documenting and document circulation on the principles of block-chain structuring of the database, which determines the order of fragmentation and recombination of accounting information at the internal and external levels of electronic communications, is studied. The procedure for using the electronic key system to gain access to confidential accounting information in accordance with the information needs of users and their classification in the enterprise management system.*

Perspectives. *In order to organize cybersecurity of enterprises, it is important to improve the methodology of implementation of other elements of the method of accounting in the process of automated information processing, which requires further research.*

Keywords: *accounting, cybersecurity, blockchain, document flow, cyber risks of accounting information.*

Formula: 0; fig .: 2; tab .: 1; bibl .: 24.

JEL classification: M41, M42, D24

Introduction. In order to ensure cybersecurity, business management, regardless of the size of the business, resorts to isolating confidential information from other information flows. Corporate associations create a separate confidential document management service. For this purpose, use specialized software for processing, movement and storage of confidential documents isolated from the general document management system. Employees who handle information containing trade secrets are prohibited from using media and the Internet for personal purposes in the workplace. Temporal and semantic regulations of information processing are introduced. In particular, it regulates the time of access and content of information, access to which must be limited.

In addition to the above approaches to cybersecurity of information, document management is protected, as proved by V. A. Shpak, based on the implementation of additional rules:

– personal responsibility of employees for the preservation of the media and the secrecy of information;

– restriction of business necessity of access of personnel to documents, cases and databases;

– strict regulation of the procedure for working with documents, files and databases for all categories of staff [1].

However, the isolation approach to documentation and document management does not guarantee effective cybersecurity of the enterprise. Separate credential databases are attracting the attention of cybercriminals. There is also always an insider influence on cybersecurity, which is realized through the possible recruitment of employees by third parties. Insiders with access to confidential information may pass it on to cybercriminals. Another option is to secretly embed malicious software in the system of confidential document management for the purpose of information espionage by regular officials. As a result, there are cyber threats to the isolated information flows of enterprises. Therefore, to ensure effective cybersecurity, it is necessary to study new formats of documentation and document management.

Analysis of research and problem statement. Scientists have studied various aspects of the use of blockchain technology in accounting. For example, Bansal S. K., Batra R. Jain N. [2] and Bonson E., Bednarova M. [3] investigated promising trends in accounting development; O'Leary D. E. – technology architecture with the definition of flows of accounting information [4]; Rındasu S. M. - benefits and threats to accounting [5]; Cai C. W. – the ability to implement a triple account [6]; Coyne J. G. and McMickle P. L. – overcoming organizational barriers to accounting [7]; Sarkar S. – transformation of knowledge, skills and professional skills of accounting professionals [8]; Karajovic M., Kim H. M. and Laskowski M. – a new way of structuring accounting information [9]; Sheldon M.D. [10] and Sinha S. [11] – threats to the accounting profesion; Kokina J., Mancha R. and Pachamanova D. – threats to the accounting system [12].

There are also studies on the use of blockchain technology to improve information systems that are informationally related to accounting: Schmitz J. and Leoni G. – prospects for the development of audit and other types of control [13]; Kozlowski S. – permanent audit with the formation of the control ecosystem of the enterprise [14]; Liu M., Wu K. and Xu J. – synergetic relationship of accounting and auditing [15]; Gomaa A. A., Gomaa M. I.

ISSN 2786-4537 (print). Вісник економіки № 4, 2021 р.
ISSN 2786-4545 (online). Herald of Economics № 4, 2021

and Stampone A. – implementation of ERP systems and the role of accounting information in enterprise management [16]; Tan B. S. and Low K. Y. – formation of databases for the purposes of different user groups [17]; Wu J., Xiong F. and Li C. – the relationship with other types of computer and communication technology for variable information users [18] and other scientists.

In the scientific space there are generalizing and review works concerning the application of blockchain technology in accounting. In particular, Pimentel Erica and Bouliann Emilio identified seven main areas of implementation of blockchain structuring of accounting information: the future of accounting, accounting functions, audit and control procedures, the display of cryptocurrencies in enterprise reporting, training of accounting professionals, administrative management, taxation. Scientists summarize the need to establish parity between theoretical research and practical developments on the implementation of blockchain technology in accounting [19].

Alsaqa Zeyad Hashim, Hussein Ali Ibrahim and Mohammed Mahmood Saddam concluded that the use of blockchain technology radically changes the accounting information system in the enterprise. In other words, the use of the principles of chain-block structuring of accounting information is impossible in the traditional accounting system, and requires a radical improvement of methodology, methodology and organization of accounting [20].

Tiron Tudor Adriana, Deliu Delia, Farcane Nicoleta and Donțu Adelina explored the main obstacles to the introduction of blockchain technology in accounting and auditing organizations. Scientists have identified the unwillingness of enterprises to innovate as the main organizational constraint on the use of innovative technologies and formed a method of SWOT-analysis of the use of blockchain technology for various accounting and auditing organizations. There are also seven promising areas of research on the implementation of blockchain technology in accounting practice: ensuring information transparency and accessibility; formation of start-up contracts between participants of contractual relations; participation of accounting specialists in the formation of the blockchain ecosystem; optimization of daily operation of accounting staff; providing training and retraining on activities with innovative technologies; transformation of accounting and auditing professions; institutional changes and improvements of regulatory and legal support [21].

Intensification of scientific research on the peculiarities of the use of blockchain technology for accounting purposes took place in 2018. The most relevant research on the implementation of accounting and auditing functions in terms of block-chain structuring of information. The problem of formation of primary and reporting documents and training and retraining of accounting specialists in the conditions of implementation of the newest computer and communication technologies has appeared as unpopular research objects. The peak of activity in the formation of global scientific thought on the accounting aspect of the implementation of blockchain technology was in 2021, due to significant public attention to cryptographic assets (Fig. 1).

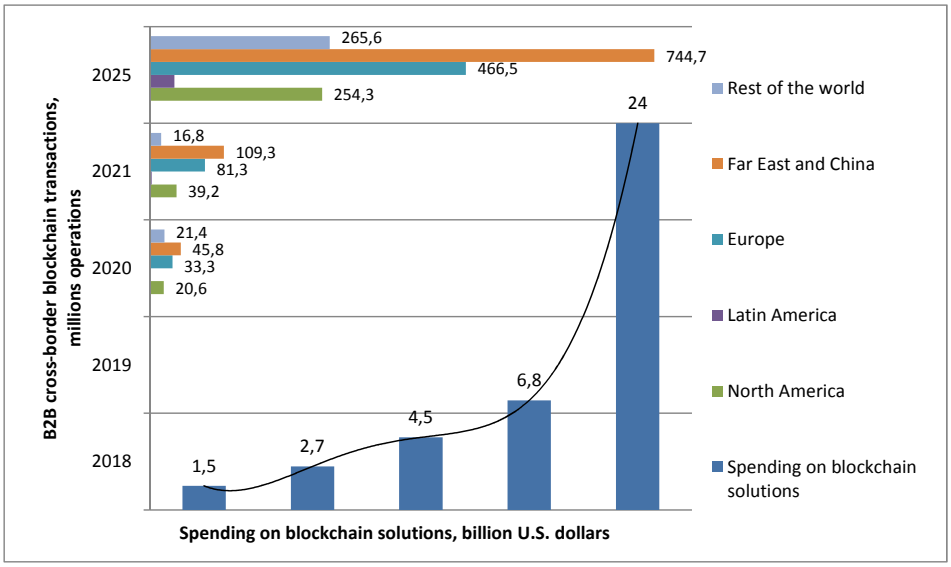

Fig. 1. Popularization of blockchain technology in 2018–2025
Source: formed on the basis of [22; 23].

Investment in blockchain technology is expected to increase from $ 4.5 billion to $ 6.8 billion in 2021, and will reach $ 24 billion in 2025. The number of information operations using the principles of block-chain structuring of information is increasing in each of the geographical regions. The leaders in the introduction of blockchain technology are the countries of the Far East and China and Europe, which is confirmed by the nationality of researchers in the field of blockchain structuring of information.

However, scientists in the field of accounting and related research and application areas have paid inadequate attention to the possibilities of using blockchain technology to ensure cybersecurity of accounting information.

Summarizing the work of scientists in the field of blockchain technology, it is possible to systematize its fundamental principles for positioning the possibility of cybersecurity of information in table. 1.

Table 1

Principles of blockchain technology in terms of cybersecurity of accounting information

№ s / n	Fundamental principle	Implementation for purposes cybersecurity accounting information
1.	Fragmentation	Division of accounting information into separate fragments (blocks), which separately have no value for cyber attackers
2.	Mutual complement	Each block complements other blocks of information through a chain combination. When creating a new block, data about it is entered into all other related blocks, which prevents the fictitious appearance of new credentials

ISSN 2786-4537 (print). Вісник економіки № 4, 2021 р.
ISSN 2786-4545 (online). Herald of Economics № 4, 2021

continuation of table 1

3.	Scalability	New blocks and modules can be added to the database without restrictions, which facilitates the use of unified cybersecurity systems for accounting information in all enterprises, regardless of business size, legal form or other organizational factors.
4.	Duplication	Each block can be duplicated in other storage locations, allowing you to recover accidentally lost or destroyed credentials
5.	Chronology	A chronological list of changes in accounting information is maintained, which allows to detect unauthorized actions that led to deviations from the reference sample
6.	Confidentiality	All accounting information processing operations are performed outside of official or government services, which makes it impossible to control and track the actions of accounting or management professionals.
7.	Distribution	Accounting information is placed in a distributed database, in which each of the fragments can be stored on many directly unrelated technical devices that are not owned by the enterprise. Cyber threats to software and hardware are impossible.
8.	Accessibility	Credentials are stored in public cloud databases, which prevents cybercriminals from blocking access
9.	Openness	The technology is open to use, making it popular in the financial, commercial, fiscal, administrative and, most importantly, security sectors.

Source: systemized and improved by the author.

In the scientific search for prospects for cybersecurity of enterprises based on the use of blockchain technology in accounting, it is necessary to focus on its fundamental principles: fragmentation, complementarity, scalability, duplication, chronology, confidentiality, distribution, accessibility, openness of accounting information processing. Adherence to and disclosure of the above principles is a necessary prerequisite for achieving the goal of the scientific article.

The purpose of the article is to study the benefits of open document management of enterprises based on blockchain technology to abandon the isolation of information flows in order to ensure cybersecurity of enterprises.

Research results. Most of the documents in the information cycle of enterprises are of accounting origin. Accounting generates primary economic information. Documentation of economic processes and phenomena is a primary element of the method of accounting. Therefore, economic data collected and documented are called «primary». Primary documentation is the initial stage of processing accounting information. Cybersecurity of the entire information system of the enterprise depends on the reliability and reliability of the information contained in the primary documents.

Cyber threats to paper documentation and document management have traditionally been positioned as internal malicious manipulation of employees or accidental errors. Another source of external receipt of unreliable documents are the company's counterparties, which may change the credentials for a certain economic gain. Instead, in the conditions of transition to electronic documentation and document circulation, external cyber threats of the enterprise become more active. Primary credentials become a valuable information resource and, accordingly, the object of cyberattacks.

In traditional document management with elements of isolation of accounting information, it is mandatory to regulate the path of the document from sender to recipient. Potential recipients of credentials generate information requests and send them to the database. From the general information array is a selection of indicators that are useful and necessary for a particular type of stakeholders. Restricting access to confidential documents is important to ensure cybersecurity. Dosing of accounting information takes place through a system of filters that select and block documents on the way to the recipient. That is, the stakeholder receives information in accordance with information requests and access rights. The initiator of the information process in terms of traditional document management at the enterprise are users of accounting information, which is detrimental to the timeliness and security of accounting.

Instead, the organization of document flow based on blockchain technology minimizes the need to regulate information flows. The fact of occurrence of a financial and economic phenomenon or event and its reflection in the primary documents triggers a further information process. Based on the study of information preferences of stakeholders, identification of the right of access to trade secrets, job descriptions, an automated management system is able to cluster and distribute information. The documented array of credentials at the time of its occurrence and fixation in the accounting system can be automatically sent to the target user.

Accounting information is promptly received by the stakeholder, who is responsible for its processing or requires a full information resource for timely management decisions. The time criteria for processing accounting information are optimized. Unlike traditional document management, documented data with a small time lag is transmitted simultaneously for further processing or consumption. In the system of electronic document management, it is advisable to provide a method of controlling the feedback to the accounting information received by stakeholders. It is necessary to control the fact that the user receives primary data, their processing by officials, the availability of appropriate management decisions to adjust the activities of the business entity, etc. Errors are impossible when controlling feedback; information duplication;

With blockchain technology, accounting information is fragmented into numerous components, which can be duplicated with the accumulation in different blocks and supplemented for future integration into a single set. Each piece of information can be stored on various technical devices or cloud information processing services. With the use of blockchain structuring information, the need for additional means of cyber security of the enterprise disappears.

Enterprise cybersecurity based on blockchain technology is implemented through fragmentation and random distribution of accounting information immediately at the time of its documentation. After collection, the primary data are broken down into separate information arrays, directly unrelated to each other. Additionally, it is possible to encrypt information and write to a distributed cloud environment. Each piece of credentials does not carry a semantic load. Only the end user integrates the elements of accounting information into a single information model, which can be useful and valuable for further use. Fragmented credentials can be open because without further aggregation it has no informational value for cybercriminals. The need for the organization of isolated document management systems decreases,

ISSN 2786-4537 (print). Вісник економіки № 4, 2021 р.
ISSN 2786-4545 (online). Herald of Economics № 4, 2021

Through the use of blockchain technology, reliable security protection of business communications is implemented. Documentary support of business relationships requires effective cyber defense in order to prevent the manifestation of cyber threats. Documents entered by the counterparty must be fragmented and encrypted when entered into a single database. Contractual relations contracted in the documents are protected from third-party changes. Unconditional changes by the parties to the business relationship are also impossible. It is expedient to control the fulfillment of contractual obligations on the basis of monitoring of primary documents on realization of material values (works, services) and monetary transactions.

To implement cyber protection of accounting information between counterparties by mutual agreement, it is advisable to use a single cloud document management service. In other words, all parties to the contractual relationship choose the Internet platform for joint paperwork for the execution and execution of commercial agreements. It is advisable to integrate cloud document management services into the internal information systems of enterprises. As a result, the original design or incoming receipt of electronic copies of documents are recorded simultaneously in two databases: each company and the information association of contracting companies. Promising in the context of the digital economy is also the information integration of all counterparties into a single database of electronic document management based on blockchain technology.

Blockchain technology detects arrays of information that have been the object of internal or external cyberattacks. For example, on the basis of monitoring the history of changes in certain documents and comparing them with reference samples, it is advisable to identify persons - violators of the information regime. Instead, the fact of the appearance of unauthorized external changes in the information environment of the enterprise, which differ from similar information arrays from other sources, may be evidence of cyber intervention. The detected incident, which took place in violation of the time, information and legal regulations, should be regarded as a cyberattack. In case of loss, distortion or destruction of information fragments by attackers, their automatic recovery from the distributed database is possible.

Chain-block structuring of accounting information simplifies the process of archival storage of documents. The distributed database of credentials should be placed in a network of interconnected cloud services, which ensures the availability of archival information for users. Cloud archiving of electronic documents on a network of interconnected servers guarantees their storage, round-the-clock access and cyber security. At the request of stakeholders, disparate arrays of archival accounting information are removed from electronic archives and recombined to display the document in the traditional form as a set of certain details. Such stakeholders can be both internal users of information (accounting or management specialists) and external – controlling or fiscal institutions.

To access electronic documents, a system of digital signatures is used, which is already actively used for fiscal purposes and to obtain various government administrative services. The use of electronic keys should take place in two stages: the formation of primary documents and their recovery from a distributed database. After collecting the credentials, it is advisable to digitally sign the persons responsible for the formation of primary documents, which provides control of information authorship. Then there is the

fragmentation and encryption of accounting information, which after reaching the target consumer is recombined to the original form. To gain access, the user of the recovered information also uses a personalized digital signature, which is evidence of the fact of information processing or consumption.

It is advisable to restrict the access rights of stakeholders to the credential database by setting the validity period of electronic keys. The need to organize cybersecurity encourages frequent changes in the digital signature of staff. The need to reissue digital signatures encourages stakeholders to update security discipline. Each user is forced to apply to the issuer for a new electronic key, which facilitates permanent control and verification of stakeholders. The company's management has an effective method of controlling the legality of the use of electronic formats for verification of a person trying to gain access to confidential information.

Through the use of electronic key systems, users gain access to the dosed amount of information within the open document flow. The proposed information scheme of open document management based on blockchain technology is shown in Fig. 2.

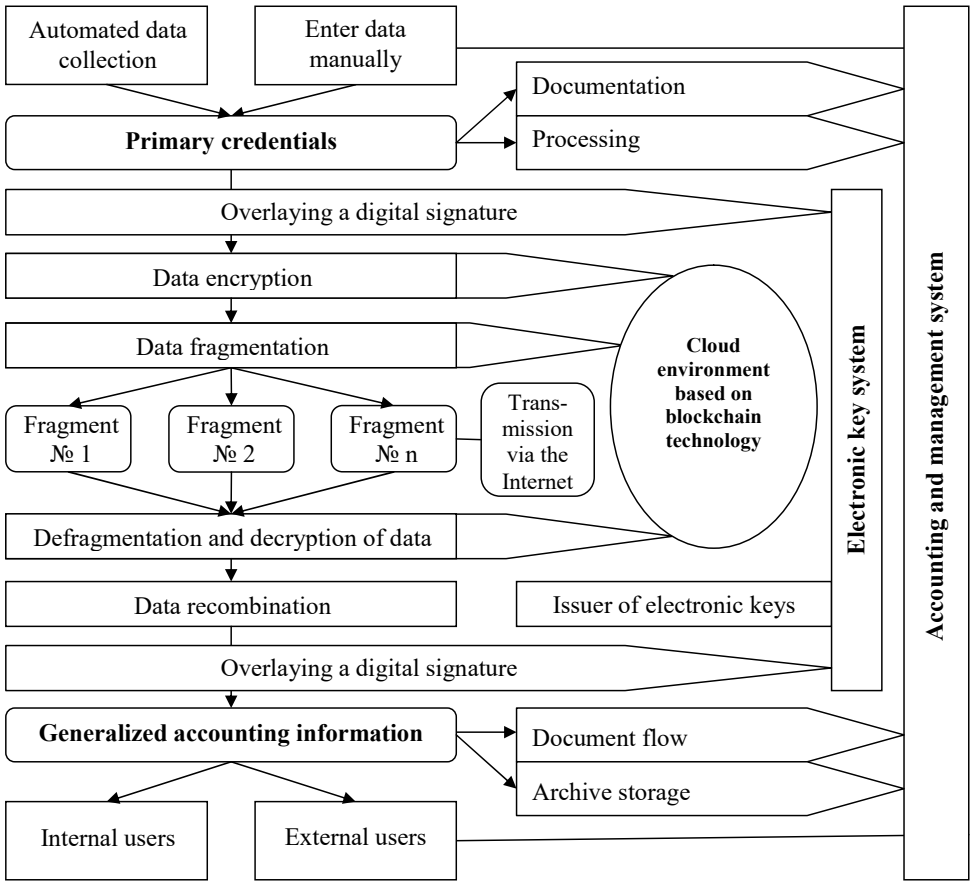

Fig. 2. Information scheme of open document flow based on blockchain technology
Source: developed by the author.

ISSN 2786-4537 (print). Вісник економіки № 4, 2021 р.
ISSN 2786-4545 (online). Herald of Economics № 4, 2021

Implementation of electronic documentation and document management based on the principles of data openness using blockchain technology is the main organization of cybersecurity in all enterprises, regardless of ownership, business size, etc. The rejection of isolation practices in the organization of information exchange in the business environment of enterprises is an element of the formation of an open national economy. The circulation of accounting information in terms of effective cybersecurity at the internal and external levels is an incentive for further development of new technologies in the financial and economic sphere («fintech industry»). Further implementation of computer and communication technologies with the development of effective methods of cybersecurity of information helps to avoid obstacles to the further development of the digital economy and information society. Consequently,

Conclusions. Traditional electronic document management in accounting has a number of functional limitations, which is the cause of cybersecurity vulnerabilities of enterprises. To implement effective internal and external electronic communications, it is advisable to implement blockchain technology in document management, which meets modern requirements for cybersecurity of enterprises. The fact of collecting primary data initiates the start of further information processes of processing and distribution of accounting information. Documented data using blockchain technology is fragmented, encrypted and sent in dosed form to internal and external users in accordance with the information needs and access rights to trade secrets. The permissive mode of accounting information processing should be implemented using a system of digital signatures and cloud placement of distributed databases.

The use of blockchain technology in electronic documentation and document management provides: fragmentation, complementarity, scalability, duplication, chronology, confidentiality, distribution, accessibility, openness of accounting information processing, which is the basis for effective cybersecurity of the enterprise. The organization of cybersecurity in the conditions of distributed structuring of the accounting information promotes openness of document circulation at the enterprise that reduces need for application of isolating information practices. The openness of information exchange using blockchain technology for cybersecurity of information minimizes organizational constraints in the formation of the digital economy and creates favorable conditions for the progressive innovative development of social formation.

Література

1. Шпак В. А. Організація захисту облікової інформації. *Бухгалтерський облік, аналіз та аудит: проблеми теорії, методології, організації.* 2015. № 2. С. 181–187.
2. Bansal, S. K., Batra, R., Jain, N. (2018). Blockchain and the future of accounting. *The Management Accountant Journal*, 6, 60–66.
3. Bonson E., Bednarova, M. (2019). Blockchain and its implications for accounting and auditing. *Meditari Accountancy Research.* Vol. 27, № 5, pp. 725–740. DOI: https://doi.org/10.1108/MEDAR-11-2018-0406.
4. O'Leary, D. E. (2017). Configuring blockchain architectures for transaction information in blockchain consortiums: the case of accounting and supply chain

systems. *Intelligent Systems in Accounting, Finance and Management.* Vol. 24, № 4, pp. 138–147. DOI: https://doi.org/10.1002/isaf.1417.

5. Rındasu, S. M. (2019). Blockchain in accounting: trick or treat? *Quality Access to Success.* Vol. 20, № 170, pp. 143–147.
6. Cai, C. W. (2021). Triple-entry accounting with blockchain: how far have we come? *Accounting Finance.* DOI: https://doi.org/10.1111/acfi.12556
7. Coyne J. G., McMickle, P. L. (2017). Can Blockchains serve an accounting purpose. *Journal of Emerging Technologies in Accounting.* Vol. 14, № 2, pp. 101–111. DOI: https://doi.org/10.2308/jeta-51910.
8. Sarkar, S. (2018). Blockchain accounting the disruption ahead. *The Management Accountant Journal,* 6, 73–78.
9. Karajovic, M., Kim, H. M., Laskowski, M. (2019). Thinking outside the block: projected phases of Blockchain integration in the accounting industry. *Australian Accounting Review*. Vol. 29, № 2, pp. 319–330. DOI: https://doi.org/10.2139/ssrn.2984126
10. Sheldon, M. D. (2019). Using Blockchain to aggregate and share misconduct issues across the accounting profession. *Current Issues in Auditing.* Vol. 12, № 2, pp. 27–35. DOI: https://doi.org/10.2308/ciia-52184
11. Sinha, S. (2019). Blockchain – opportunities and challenges for accounting professionals. *Journal of Corporate Accounting and Finance.* Vol. 31, pp. 65–67. DOI: https://doi.org/10.1002/jcaf.22430.
12. Kokina, J., Mancha, R., Pachamanova, D. (2017). Blockchain: emergent industry adoption and implications for accounting. *Journal of Emerging Technologies in Accounting.* Vol. 14. № 2, pp. 91–100. DOI: https://doi.org/10.2308/jeta-51911.
13. Schmitz, J. and Leoni, G. (2019). Accounting and auditing at the time of Blockchain technology: a research agenda. *The Management Accountant Journal.* Vol. 29. № 2, pp. 331-342. DOI: https://doi.org/10.1111/auar.12286
14. Kozlowski, S. (2018). An audit ecosystem to support Blockchain-based accounting and assurance book continuous auditing: theory and application. *Continuous Auditing: Theory and Application (Rutgers Studies in Accounting Analytics), Emerald Publishing, Bingley,* pp. 299–313. DOI: https://doi.org/10.1108/978-1-78743-413-420181015
15. Liu M., Wu K. and Xu J. (2019). How will Blockchain technology impact auditing and accounting: permissionless vs. permissioned Blockchain, Current Issues in Auditing. 2019. Vol. 13. №. 2, pp. 19–29. DOI: https://doi.org/10.2308/ciia-52540
16. Gomaa A. A., Gomaa M. I., Stampone A. A. (2019). transaction on the Blockchain: an AIS perspective, intro case to explain transactions on the ERP and the role of the internal and external auditor, Journal of Emerging Technologies in Accounting. Vol. 16, № 1, pp. 47–64. DOI: https://doi.org/10.2308/jeta-52412
17. Tan B.S., Low K.Y. Blockchain as the database engine in the accounting system, Australian Accounting Review. 2019. Vol. 29. №. 2, pp. 312–318. DOI: https://doi.org/10.1111/auar.12278

18. Wu J., Xiong F., Li C. (2019). Application of internet of Things and blockchain technologies toimprove accounting, IEEE Access, 20, pp. 1–10. DOI: https://doi.org/10.1109/ACCESS.2019.2930637
19. Pimentel, E., Bouliann, E. (2019). Blockchain in Accounting Research and Practice: Current Trends and Future Opportunities. *Accounting Perspectives*, 19 (3), pp. 325–361. DOI: https://doi.org/1111/1911-3838.12239
20. Alsaqa Zeyad H., Hussein A. I. & Mohammed Mahmood S. (2020). The Impact of Blockchain on Accounting Information Systems. *Journal of Information Technology Management,* 11, pp. 62–80. DOI: https://doi.org/10.22059/jitm.2019.74301
21. Tiron Tudor A., Deliu D., Farcane N., Donțu A. Managing change with and through blockchain in accountancy organizations: a systematic literature review. Journal of Organizational Change Management. ahead-of-print. 2021. DOI: https://doi.org/10.1108/JOCM-10-2020-0302
22. Worldwide spending on blockchain solutions from 2017 to 2025. Statista. Retrieved from: https://www.statista.com/statistics/800426/worldwide-blockchain-solutions-spending/
23. B2B cross-border transactions on blockchain in various regions worldwide in 2020 with forecasts from 2021 to 2025. Statista. Retrieved from: https://www.statista.com/statistics/1228825/b2b-cross-border-transactions-on-blockchain-worldwide/
24. Zadorozhny, Z., Muravskyi, V. V., Shevchuk, O. A., Sudyn, Y. A.. Management accounting of the settlements with contractors in innovative environment of business communications. Marketing and Management of Innovations. 2018. 2. pp. 103–112. DOI: https://doi.org/10.21272/mmi.2018.2-09.

References

1. Shpak, V. A. (2015). Organization of protection of accounting information. *Accounting, analysis and audit: problems of theory, methodology, organization,* 2, 181–187 [in Ukrainian].
2. Bansal, S. K., Batra, R., Jain, N. (2018). Blockchain and the future of accounting. *The Management Accountant Journal*, 6, 60-66 [in English].
3. Bonson, E., Bednarova, M. (2019). Blockchain and its implications for accounting and auditing. *Meditari Accountancy Research.* Vol. 27, No. 5, 725-740. DOI: https://doi.org/10.1108/MEDAR-11-2018-0406
4. O'Leary, D.E. (2017). Configuring blockchain architectures for transaction information in blockchain consortiums: the case of accounting and supply chain systems. *Intelligent Systems in Accounting, Finance and Management.* Vol. 24, No. 4, 138-147. DOI: https://doi.org/10.1002/isaf.1417
5. Rındasu, S.M. (2019). Blockchain in accounting: trick or treat? *Quality Access to Success.* Vol. 20, No. 170, 143-147.
6. Cai, C. W. (2021). Triple-entry accounting with blockchain: how far have we come? *Accounting Finance.* DOI: https://doi.org/10.1111/acfi.12556
7. Coyne, J. G., McMickle, P. L. (2017). Can Blockchains serve an accounting purpose. Journal of Emerging Technologies in Accounting. Vol. 14, No. 2, 101-111. DOI: https://doi.org/10.2308/jeta-51910

8. Sarkar, S. (2018). Blockchain accounting the disruption ahead. *The Management Accountant Journal,* 6, 73-78.
9. Karajovic, M., Kim, H. M., Laskowski, M. (2019). Thinking outside the block: projected phases of Blockchain integration in the accounting industry. *Australian Accounting Review.* Vol. 29, No. 2, 319-330. DOI: https://doi.org/10.2139/ssrn.2984126
10. Sheldon, M. D. (2018). Using Blockchain to aggregate and share misconduct issues across the accounting profession. *Current Issues in Auditing.* Vol. 12, No. 2, 27-35. DOI: https://doi.org/10.2308/ciia-52184
11. Sinha, S. (2020). Blockchain – opportunities and challenges for accounting professionals. *Journal of Corporate Accounting and Finance* 31, 65-67. DOI: https://doi.org/10.1002/jcaf.22430
12. Kokina, J., Mancha, R., Pachamanova, D. (2017). Blockchain: emergent industry adoption and implications for accounting. *Journal of Emerging Technologies in Accounting.* Vol. 14 No. 2, 91-100. DOI: https://doi.org/10.2308/jeta-51911
13. Schmitz, J., Leoni, G. (2019). Accounting and auditing at the time of Blockchain technology: a research agenda. *The Management Accountant Journal.* Vol. 29 No. 2, 331-342. DOI: https://doi.org/10.1111/auar.12286
14. Kozlowski, S. (2018). An audit ecosystem to support Blockchain-based accounting and assurance book continuous auditing: theory and application. *Continuous Auditing: Theory and Application (Rutgers Studies in Accounting Analytics), Emerald Publishing, Bingley,* 299-313. DOI: https://doi.org/10.1108/978-1-78743-413-420181015
15. Liu, M., Wu, K., Xu, J. (2019). How will Blockchain technology impact auditing and accounting: permissionless vs. permissioned Blockchain. *Current Issues in Auditing.* Vol. 13, No. 2, 19-29. DOI: https://doi.org/10.2308/ciia-52540
16. Gomaa, A.A., Gomaa, M.I., Stampone, A. (2019). A transaction on the Blockchain: an AIS perspective, intro case to explain transactions on the ERP and the role of the internal and external auditor. *Journal of Emerging Technologies in Accounting.* Vol. 16, No. 1, 47-64. DOI: https://doi.org/10.2308/jeta-52412
17. Tan, B.S., Low, K.Y. (2019). Blockchain as the database engine in the accounting system. *Australian Accounting Review.* Vol. 29 No. 2, 312-318. DOI: https://doi.org/10.1111/auar.12278
18. Wu, J., Xiong, F., Li, C. (2019). Application of internet of Things and blockchain technologies toimprove accounting. *IEEE Access*, 20, 1-10. DOI: https://doi.org/10.1109/ACCESS.2019.2930637
19. Pimentel, E., Bouliann, E. (2020). Blockchain in Accounting Research and Practice: Current Trends and Future Opportunities. *Accounting Perspectives*, 19 (3), 325–361. DOI: https://doi.org/10.1111/1911-3838.12239
20. Alsaqa Zeyad, H., Hussein, A. I., Mohammed Mahmood, S. (2020). The Impact of Blockchain on Accounting Information Systems. *Journal of Information Technology Management,* 11, 62-80. DOI: https://doi.org/10.22059/jitm.2019.74301
21. Tiron Tudor, A., Deliu, D., Farcane, N., Donțu, A. (2021). Managing change with and through blockchain in accountancy organizations: a systematic literature review.

Journal of Organizational Change Management. ahead-of-print. DOI: https://doi.org/10.1108/JOCM-10-2020-0302
22. Worldwide spending on blockchain solutions from 2017 to 2025. Statista. Retrevied from: https://www.statista.com/statistics/800426/worldwide-blockchain-solutions-spending/
23. B2B cross-border transactions on blockchain in various regions worldwide in 2020 with forecasts from 2021 to 2025. *Statista.* DOI: https://www.statista.com/statistics/1228825/b2b-cross-border-transactions-on-blockchain-worldwide/
24. Zadorozhny, Z., Muravskyi, V. V., Shevchuk, O. A., Sudyn, Y. A. (2018). Management accounting of the settlements with contractors in innovative environment of business communications. *Marketing and Management of Innovations,* 2, 103-112. DOI: https://doi.org/10.21272/mmi.2018.2-09

Володимир МУРАВСЬКИЙ,
доктор економічних наук, доцент,
професор кафедри обліку і оподаткування,
Західноукраїнський національний університет,
вул. Львівська, 11, м. Тернопіль, 46020, Україна,
e-mail: vvvmur@gmail.com
ORCID ID: https://orcid.org/0000-0002-6423-9059

Надія ХОМА,
кандидат фізико-математичних наук, доцент,
доцент кафедри економічної кібернетики та інформатики
Західноукраїнський національний університет,
вул. Львівська, 11, м. Тернопіль, 46020, Україна,
e-mail: nadiiakhoma@gmail.com
ORCID ID: 0000-0003-2981-0296

Лариса ХОХЛОВА,
кандидат фізико-математичних наук, доцент,
доцент кафедри математики та метидики її навчання,
Тернопільський національний педагогічний університет
ім. Володимира Гнатюка,
вул. Максима Кривоноса, 2, м. Тернопіль, 46027, Україна,
e-mail: larysa_khokhlova@tnpu.edu.ua
ORCID ID: 0000-0002-9818-1051

Лю Чен'юй,
аспірант кафедри обліку і оподаткування,
Західноукраїнський національний університет,
практичкуючий бухгалтер, викладач,
Нанчанський науково-технічний інститут,
Наньчан, провінція Цзянсі, Китай,
e-mail: 1657426641@qq.com
ORCID ID: 0000-0002-0572-9322

ВІДКРИТИЙ ДОКУМЕНТООБІГ НА ОСНОВІ ТЕХНОЛОГІЇ БЛОКЧЕЙН ДЛЯ КІБЕРЗАХИСТУ СИСТЕМИ ОБЛІКУ

Анотація

Вступ. *Для забезпечення кіберзахисту менеджмент підприємства вдається до ізоляції облікової інформації, що містить комерційну таємницю, від інших інформаційних потоків. Проте конфіденційний документообіг привертає значну увагу внутрішніх користувачів та зовнішніх осіб з метою отримання несанкціонованого доступу. Унаслідок активних кіберзагроз ізоляційна практика в реалізації електронних інформаційних комунікацій є недієвою для цілей кібербезпеки, що потребує розробки нових методик документування й документообігу на підприємстві.*

Мета статті *полягає у дослідженні переваг відкритого документообігу підприємств на основі технології блокчейн для відмови від ізоляційних інформаційних потоків з метою забезпечення кіберзахисту підприємств.*

Методи. *У процесі дослідження недоліків й переваг ізоляційного та відкритого документообігу використані загальнотеоретичні (емпіричні, логічні та історичні) методичні прийоми пізнання дійсності. Дослідження базуються на основі концепутальних методів абстрактного вивчення економічних процесів, фактів та явищ з позиції бухгалтерського обліку та кібербезпеки підприємств. Інформаційною базою статті обрано історичні документи щодо розвитку технології блокчейн, наукові праці учених щодо блоково-ланцюгового структурування облікової інформації тощо.*

Результати. *Сформовано фундаментальні принципи технології блокчейн в умовах її використання для організації кіберзахисту облікової інформації. Обґрунтовано доцільність відмови від ізоляції інформації на користь відкритого документообігу в умовах збереження комерційної таємниці підприємства. Досліджено методику документування та документообігу на принципах блоково-ланцюгового структурування бази даних, що визначає порядок фрагментування та рекомбінації облікової інформації на внутрішньому та зовнішньому рівнях електронних комунікацій. Встановлено порядок використання системи електронних ключів для отримання доступу до конфіденційної облікової інформації відповідно до інформаційних потреб користувачів та їхньої класифікації у системі управління підприємством.*

Перспективи. *З метою організації кібербезпеки підприємств важливим є удосконалення методики реалізації інших елементів методу бухгалтерського обліку у процесі автоматизованої обробки інформації , що потребує подальших наукових досліджень.*

Ключові слова: *облік, кібербезпека, блокчейн, документообіг, кіберризики облікової інформації.*

Формули: 0; рис.: 2; табл.: 1; бібл.: 24.

Статтю отримано 13 вересня 2021 р.
Article received September 13, 2021.