TECHNOLOGY OF BLOCKCHAIN SYSTEMS: NEW OPPORTUNITIES AND ISSUES IN DATA SECURITY AND RETENTION

SERGII BATAIEV[1], VIKTOR KYRYCHENKO[2], VIKTOR OSTAPCHUK[3], VIKTOR KRASNOSHCHOK[4], SERHII MARTYNIUK[5]

[1]PgDip in Digital Leadership, The University of Warwick, Coventry, UK; Head of the Department of Technology, ELEKS Inc., Lviv, Ukraine.
[2]Candidate of Physical and Mathematical Sciences, Assistant Professor, Department of Computer Science, Faculty of Information Technologies, National University of Life and Environmental Sciences of Ukraine, Kyiv, Ukraine.
[3]Candidate of Technical Sciences, Research Associate, Research Department, Scientific Center of Communication and Information Technologies, Kruty Heroes Military Institute of Telecommunications and Information Technologies, Kyiv, Ukraine.
[4]Candidate of Technical Sciences, Associate Professor, Department of Applied Information Systems, Faculty of Information Technologies, Taras Shevchenko National University of Kyiv, Kyiv, Ukraine.
[5]Postgraduate Student by Law, Interregional Academy of Personnel Management, Kyiv, Ukraine.
E-mail: [1]serg.bataiev@gmail.com, [2]v.kyrychenko@nubip.edu.ua, [3]ostapchuk764@gmail.com, [4]kivinme@ukr.net, [5]sergeymartunyk98@gmail.com

ABSTRACT

In the modern digital environment, there is a growing need for reliable mechanisms for data protection and storage, which is due to the risks of cybercrime, information leaks and manipulation of digital records. Blockchain technologies offer decentralized solutions that can provide increased security, transparency and immutability of data, which makes them promising for use in the financial sector, medicine, e-government and logistics. The purpose of this study is to analyze the opportunities and challenges of blockchain in the field of security and information storage. The work uses methods of comparative analysis, empirical threat modeling and expert assessment of blockchain implementation in various industries. The study confirmed that blockchain is able to significantly reduce the risks of unauthorized access to data and manipulation of digital records, thanks to the use of cryptographic protection methods and consensus algorithms. However, it was found that existing blockchain networks face scalability problems, high energy consumption and the lack of a unified regulatory framework, which limits their implementation. Possible solutions are proposed, including the transition to more energy-efficient algorithms, such as Proof-of-Stake, the development of quantum-resistant cryptographic methods, and the harmonization of regulatory approaches. The results obtained have practical significance for the financial, government, and technology sectors, contributing to the implementation of secure digital solutions based on blockchain. Further research should be aimed at improving scaling technologies and increasing the security of blockchain systems in the context of the development of quantum computing.

Keywords: *Blockchain, Data Security, Cryptography, Consensus Algorithm, Scalability, Financial Technology, E-Government*

1. INTRODUCTION

Today, when digital data is an important asset, the problem of its security and preservation has become extremely important. With traditional centralized databases, threats of unauthorized data access or information leaks, cyberattacks, etc. are often being made. Blockchain technologies offer a fundamentally new approach to managing digital data, ensuring its decentralization, transparency, and protection against counterfeiting. Thanks to the immutability of records and cryptographic encryption, blockchain can significantly increase the level of security in the financial sector, logistics, medicine, e-government, and cybersecurity in general. Scientific interest in blockchain is constantly growing, which is confirmed by a large number of studies in this area. For example, Agrawal et al. [1] proved that blockchain can be effectively used to protect distributed databases and authenticate users. Damaševičius et al. [2] emphasize the possibilities of integrating blockchain with the Internet of Things (IoT), which creates new approaches to data storage and transmission. At the same time, Wei et al. [3] point out the scalability problem that limits the use of blockchain in global financial systems. Despite numerous studies, some aspects of blockchain technologies remain poorly understood. First, it is necessary to investigate methods for reducing energy consumption when using consensus algorithms, such as Proof-of-Work, which are extremely resource-intensive. Second, there is still no single regulatory framework that would regulate the implementation of blockchain in different countries, which complicates its application in the financial and government sectors [4]. The issue of quantum computing, which may make traditional encryption methods vulnerable in the future [5], also remains open.

The purpose of this study is to comprehensively analyze the opportunities and challenges of blockchain technologies in the field of security and data storage. In accordance with the declared hypotheses, the following research questions direct the current research: (RQ1) How blockchain technologies improve the data security in comparison with the traditional model of a centralized system? (RQ2) What are the primary technical, regulatory and organizational obstacles that impede the use of blockchains? (RQ3) What can consensus algorithms, cryptographic techniques, and regulatory strategies do to reduce these obstacles? Based on these questions, we derive our hypotheses: (H1) The risks of unauthorized access and manipulation of data are greatly decreased with the help of blockchain technologies which are cryptographic and decentralized. High energy usage, lack of scalability, and disjointed regulations are the most important challenges to blockchain adoption. (H3) Implementing quantum-resistant cryptography, energy-efficient consensus protocols and standardized regulations will go a long way in making blockchain more plausible in security-sensitive sectors.

To achieve this goal, the following tasks must be solved:

- describe the main advantages of blockchain in ensuring digital security;
- identify the main threats and limitations associated with the use of this technology;
- explore potential approaches to overcome scalability and high power consumption issues;
- to offer recommendations for improving blockchain solutions to increase their effectiveness in various areas of application.

Thus, the study aims to provide a deeper analysis of the security aspects of blockchain technologies, as well as to identify key challenges that hinder their large-scale implementation in modern digital systems. Past research on the topic has primarily revolved around proving the potential of blockchain to promote the safety and openness of data in particular fields, including finance, health care, and supply chain management. As an example, Agrawal et al. (2024) pointed to the possibility to secure distributed databases, and Damaševičius et al. (2024) focused on the combination with the Internet of Things to enhance the data exchange. Nevertheless, these publications usually focused on single case studies and lacked an industry-wide evaluation. Our research is innovative with a holistic approach to analysis with technical, legal, and organizational approaches with an emphasis on the comparative analysis, empirical threat modeling, and expert evaluation. In contrast to the previous research, our results show the power of cryptographic techniques and consensus algorithms to eliminate illegal access, but also emphasize the unresolved challenges, such as energy efficiency, scalability, and fragmentation of regulation, which are all characteristic of the opportunities of blockchain implementation at the systemic level.

2. LITERATURE REVIEW

As of now, research is in progress to use blockchain technology for security and data storage purposes. The main concepts on which it centers around are decentralization, cryptographic defense and automation of processes via smart contracts. In other words, Agrawal et al. [1] incorporate the use of hybrid encryption algorithms at the level of a distributed database to enhance the authentication and the protection against unauthorized changes. Han et al. [6] also support similar approaches of peer to peer data management in cloud environment. There is lots of attention given to use cases of blockchain in financial sector, more specifically, to guarantee transaction transparency and avoid frauds [7]. Moreover, as shown by Damaševičius et al. [2], blockchain enabling the Internet of Things (IoT) allows for high security with distributed systems and is less prone to data loss. It is also similar to document traceability and goods accounting as shown by Jouti et al. [8] on the effect of blockchain on the judicial system and logistics chains.

Besides finance, other important areas of research are tractable such as e-voting, digital identity management, medical record storage [9, 10, 11]. According to them, blockchain can save the electoral running processes from risks of manipulation, ensure personal data confidentiality and increase the efficiency of exchanging medical information. Among other things, scholars also point out the existing challenges of the blockchain technologies. As an instance, Duan et al. [12]) and Wei et al. [3] study the problem of scalability and high energy consumption of two consensus algorithms like Proof of Work (PoW). Secondly, Gautam et al. [5] assess the risks connected to the possible effects of quantum computing on cryptographic methods employed in the blockchain. Therefore, the given recent research support that blockchain technologies are a great tool for assuring security and data storage, but their wide use is complicated by technical and legal problems [4, 13, 14]. It is recommended to carry further researches on improving the consensus mechanisms, quantum resistant encryption algorithms, and flexible regulations to utilize blockchain in the different areas of the economy.

Besides, further research affirms that blockchain has already been actively involved in digital data protection for security enhancement as well as storing and distributing information [15, 16]. Tmeizeh et al. [17] are in particular focusing on file fragmentation in blockchain networks: the methods that enable the reduction of nodes load and increase of the efficiency of the distributed systems. Likewise, Yadav et al. [18] employ blockchain for the discovery among wireless sensor networks (WSNs) malicious nodes which confers a significant degree of security to such systems.

The use of blockchain to optimize the operation of cloud services and cloud computing networks [19, 20] falls into a separate area of research. These works illustrate the uses of integrating blockchain technology into cloud platforms to enable a better and more secure data storage and processing platform. Similar to this, Liu and Chen [21] explore the possibility of integrating blockchain into financial and industrial networks, in this way, blockchain plays the role of making these elements transparent and defending digital assets. Not only we are dealing with security related issues, but it would be very important to bring automation of business processes through the use of smart contracts. This paper is based on the latest sources published in the high-impact journals Cluster Computing, Scientific Reports, and Journal of Cloud Computing between 2023 and 2025 in order to make the analysis reflect the state of the art. To illustrate, Agrawal et al. (2024) studied the use of hybrid encryption algorithms in secure distributed databases, whereas Gautam et al. (2024) offered post-quantum cryptographic schemes to the storage of multimedia data. Similarly, Sehar et al. (2023) investigated blockchain-based vehicular networks, whereas Fateminasab et al. (2025) came up with clustering models of open data storage. The recent additions demonstrate the accelerated development of blockchain applications and validate the topicality of the unsolved problems that we have defined, i.e., scalability, harmonization of regulations, and quantum security. In making the analysis based on UpToDate references, our work throws light on the technological horizon, as well as the real-life issues of blockchain adoption. For instance, Jani and Raajan [22] use blockchain application in the Internet of Medical Things (IoMT), to automating access management to sensitive information and a decreased risk of its unauthorized use. According to Samanta and Sarkar [23], one such possible application of blockchain in IIoT such as the Industrial Internet of Things (IIoT) to improve the cybersecurity of smart cities is also analyzed. We can confirm with recent studies that blockchain technologies have a big potential for making data security better, extend the scope of authentication and protecting the information from unauthorized access. For instance, Singhal et al. [24] examine the efficiency of Proof of Stake (PoS) algorithm in protecting data of smart meters that protect energy networks data from manipulation and diminish the threat to the data from being manipulated. Finally, the described solutions offer wide prospects for their implementation into critical infrastructures, where it is necessary to ensure transparency and reliability of digital records.

Sehar et al. [25] has shown importance of use of blockchain on data protection in transportation network (VANETs) in the field of distributed systems of network systems. Putting that into words, they say, the model they propose gives decentralized security management and minimise hacking of the system and fast verification of transaction in real time. In addition to road transport, blockchain also has promising applications in smart cities, where data security is guaranteed through exactly the same approaches between Internet of Things (IoT) devices. Digital identity and user authentication have also received a lot of attention into their use on the use of blockchain. In the realm of mobile computing systems, Ganesh et al. [26] find ways to combine the technology with hybrid encryption mechanisms to fail at security. They present a new approach to enable Mobile Edge Computing (MEC) environments in which it is possible to minimize transaction delay. In e-health, blockchain also plays a role in protecting the data. Particularly focusing on the use of the technology to manage electronic health records (EHR) as Chandini and Basarkod [27] provide the efficacy of the technology with the point that a decentralized repository eliminates the threats of information leakage in the confidentiality and also makes identification simple. Research carried out by Rastogi et al. [28] confirm this approach, in which it is proposed that Blockchain can be used to verify medical data and improve healthcare systems through the process approach to request processing.

Unresolved problems. Sehar et al. [25] has shown importance of use of blockchain on data protection in transportation network (VANETs) in the field of distributed systems of network systems. Putting that into words, they say, the model they propose gives decentralized security management and minimise hacking of the system and fast verification of transaction in real time. Likewise, blockchain is a similar approach that might have compellingly applications not only in road transport, but also in smart cities, where data exchange between the Internet of Things (IoT) devices is guaranteed to be conducted securely. Digital identity and user authentication have also received a lot of attention into their use on the use of blockchain. In the realm of mobile computing systems, Ganesh et al. [26] find ways to combine the technology with hybrid encryption mechanisms to fail at security. They present a new approach to enable Mobile Edge Computing (MEC) environments in which it is possible to minimize transaction delay. In e-health, blockchain also plays a role in protecting the data. Particularly focusing on the use of the technology to manage electronic health records (EHR) as Chandini and Basarkod [27] provide the efficacy of the technology with the point that a decentralized repository eliminates the threats of information leakage in the confidentiality and also makes identification simple. Research carried out by Rastogi et al. [28] confirm this approach, in which it is proposed that Blockchain can be used to verify medical data and improve healthcare systems through the process approach to request processing.

3. METHODS

This study applies a comprehensive method combining the quantitative and qualitative treatment of blockchain technologies in the area of security and data storage. The main research methods are a scientific publications analysis and statistical data on effectiveness of blockchain at different industries, especially in financial, healthcare, and cybersecurity industries. Different methods of comparative analysis were used to assess the favourable and unfavourable aspects of existing consensus algorithms, including Proof-of-Work (PoW) and Proof-of-Stake (PoS). In order to identify the security level of blockchain systems, 51% attack and Sybil attacks were analyzed during threat modeling. Furthermore, the way of implementing blockchain project was also empirically analyzed with real cases in document management, logistics, and digital identification. Along with that, the expert assessment method helped us to identify critical aspects as to scalability, energy consumption and regulatory barriers. Results of peer reviewed scientific publications and industry reports for 2018–2025 are taken in account. This study is designed as an exploratory-descriptive study that has a sequence of three steps of literature review, empirical threat modeling, and expert review. The research protocol involved a systematic search in peer-reviewed articles and industry reports published between 2018 and 2025, in which the inclusion criteria were the applications of blockchain in finance, healthcare, logistics, and cybersecurity. Simulated scenarios of 51 percent and Sybil attacks were used to assess the vulnerability of the threat modeling and consensus algorithms like PoW and PoS were compared. The assessment of the experts was conducted by means of structured interviews with IT specialists and policymakers (n = 25) to make the triangulation of the technical, organizational, and regulatory approaches. This framework of multi-method procedures increases the strength of the results and guarantees that theoretical and practical levels of blockchain security were taken into consideration.

3. RESULTS

Blockchain technology brings great potentials of enhancing data storage and increasing the security in numerous sectors. The biggest advantage of blockchain is that information is changed by only the authorized parties, so no change is permissible without permission, and there are no malicious attacks. Thanks to the use of cryptographic methods and consensus algorithm, the data present in the blockchain cannot be forged or otherwise changed in hindsight and thus this technology is used to store crucial information such as financial transactions, medical records and legal documents [1]. Second, cybersecurity is one of the key areas of application of blockchain. Using this technology makes it possible to block data leaks when information is spreaded across many participants of the network and access to it is controlled by cryptography. For instance, blockchain can ensure the authenticity and integrity of documents, which subsequently will minimize the chances of fraud [2] in an electronic document management field. It has been actively used as well to manage digital identities in order to stop the theft of personal information.

The other important opportunity of blockchain lies in its use case in distributed data storage. However, aka centralized servers on the computer are hackable or may fail. However on the contrary, blockchain is a system wherein data is stored through links in the form of encrypted blocks, distributed across network nodes. Such increases the level of resistance to attacks and fault tolerance of the system to an unprecedented extent [6]. As a matter of fact, blockchain is being employed to retail patient medical history, which will permit only approved parties to access the information and forestall its illegitimate modification. The market, however, is seeing a new big application that is blockchain. It presents itself as a means of creating secure and transparent financial systems that reduce the incidences of fraud and forgery of transactions. Smart contracts use is to automate financial transactions, and they will be executed without the involvement of intermediaries [7]. International payments, in particular have long delays and high costs when blasted through traditional banking systems.

Moreover, blockchain is being actively employed in the supply chain management system that requires tracing the path of goods movements and their origin. Thanks to the technology, the companies are now in a position to ensure the authenticity of the products in what would otherwise risk counterfeiting and also enhance the transparency of the processes [8]. The use of tracking supplies using blockchain is common among the pharmaceuticals, agricultural, and automotive industries. Consequently, this technology is a promising technological type of blockchain which is used in various fields linked to information security and data protection. It is an important part of modern digital systems due to its capability of providing a decentralized, transparent and secure environment for systeming information. This will further lead to research and develop in the blockchain space to improve consensus mechanisms; scalability and efficiency in the usage of blockchain across various sectors of the economy.

Blockchain technologies have tremendous promise regarding data safety and transparency about transactions. Nevertheless, although blockchain solutions bring about a number of advantages, these are coupled with challenges and threats to its effectiveness. However, we have key issues including scalability issues, high energy consumption, legal aspects, and possible security threats as associated with cryptographic vulnerabilities and network attacks [1]. The main challenges and threats when implementing blockchain solutions and some ways to resolve them are listed at Table 1.

Table 1: Main challenges and threats of blockchain technologies

No.	Challenge/Threat	Description	Possible solutions
1	Scalability	As the number of users increases, the network becomes congested, which slows down transactions and increases their cost [12].	Using new consensus mechanisms such as Proof-of-Stake (PoS) or sharding.
2	High energy consumption	Consensus algorithms, especially Proof-of-Work (PoW), require significant computational resources [6].	Moving to more energy-efficient methods such as PoS or delegated power-based consensus (DPoS).
3	Legal and regulatory issues	The lack of clear legal regulations in many countries can complicate the implementation of the technology [4].	Development of international standards and adaptation of the regulatory framework.
4	Smart contract vulnerabilities	Errors in smart contract code can lead to financial losses [7].	Using formal code verification and secure programming languages.

5	Cryptographic threats	Quantum computing could make existing cryptographic methods obsolete [5].	Development of quantum-resistant encryption algorithms.
6	Mining centralization	Despite the decentralized nature of the blockchain, much of the computing power is concentrated in a few mining pools [13].	Implementation of new models of computing power distribution.
7	Blockchain attacks	51% attack, Sybil attack, and double-spending attacks [3].	Strengthening security mechanisms, introducing additional levels of verification.

Source: created by the author based on [3, 4, 5, 6, 7, 12, 13]

Blockchain technologies are many times advantageous but implementation has its problems. Scaling, energy constraints, legal constraints and cryptographic threats consume the main problems. A solution to these issues involves implementing a broader solution, which entails the development of quantum resistant encryption, consensus mechanisms that improve, and a flexible legal framework. The technology will be improved in the future to make it more widely applied, and to raise the level of security of the digital ecosystems.

Many of the studies on blockchain technologies integration into the digital economy discuss benefits, challenges and prospects of this technology across different sectors. In particular, blockchain is on usage in finance, logistics, education, healthcare, and supply chain management [2]. As reviewed in studies, smart contracts provide most benefits of increased security, transparency, and automation of process. Additionally, there are some limitations: the scaleability or complexity in scaling and regulatory barriers [15]. The main conclusions of the studies on the use of blockchain technologies in different areas of digital economy are presented in the table 2 along with the overview of existing studies.

Table 2. Analysis of research on the integration of blockchain into the digital economy

No.	Field of application	Research	Main conclusions
1	Financial sector	Agrawal et al. [1]	Blockchain ensures secure and transparent financial transactions, reducing the risk of fraud and the need for intermediaries.
2	Healthcare	Chandini and Basarkod [27]	Using blockchain to manage electronic health records helps protect personal data and improve information accessibility.
3	Logistics and supply chains	Jouti et al. [8]	Blockchain allows tracking the origin of goods and reduce the risk of counterfeiting in global supply chains.
4	Digital identification	Jin [7]	The technology provides secure management of digital identities, reducing the likelihood of identity theft.
5	Education and certification	Li and Wu [10]	Blockchain is used to protect and authenticate diplomas and certificates, simplifying the verification process.
6	Electronic voting	Huang and Yi [9]	The use of blockchain ensures transparency and immutability of electoral processes, reducing the risk of fraud.
7	Cloud computing	Wei et al. [3]	Integrating blockchain into cloud platforms increases the level of security and control over distributed data.

Source: created by the author based on [1, 3, 7, 8, 9, 10, 27]

The analysis of scientific research shows the whole range of applications of blockchain technologies in the digital economy. Basically, blockchain is most actively used in the financial sector, the healthcare and logistics, where technology built on it is more secure, transparent and efficient. Nevertheless, scaling, regulatory regulation and complexity of implementation are critical issues. These problems need further research and expansion of the potential of blockchain solutions to new fields.

To create a methodological approach to the assessment of the effectiveness of operation of the blockchain systems in the area of the data security, it is necessary to conduct a comprehensive analysis of the technological, organizational, and legal aspects. High resistance to malicious attacks offered by blockchain as a decentralized data storage technology is data dependent to some extent; it greatly depends on consensus algorithm being used, how the network is structured and what is the level of cryptographic protection [1, 29].

In the first stage of the study, we select the key performance indicators (KPIs) involved in the data security field of the blockchain system. The metrics with the main development are the degree of secrecy protection of information against unauthorized access, speed of transaction processing, energy consumption, increment in network capacity, and the ability to resist attacks [7]. Analysis of these parameters help us to estimate how the blockchain handles information security in a particular environment.

In the second stage, data is gathered on the blockchain technologies and modeled for their use. This involves the use of security testing methods, for example, analysis of the possible attacks such as 51 percent attacks, Sybil attacks, double spending [3]. Comparative study of the blockchain effectiveness in various fields (ie, in finance, medicine, logistics) is done to find out quite specific versions of its use [2].

The third important stage is analysis of legal and regulatory aspects. However, the legal regulation and compliance with the security standards are remaining issues even though the blockchain possesses the high level of security [4]. The research methodology should include, a study of National and International regulations governing the data processing and storage in blockchain network.

Finally, it is to make recommendations for improving blockchain systems in order for data to be secure. Particularly, it is worth investigating the possibility to deploy quantum resistant encryption algorithms as well as hybrid solutions based on the combination of blockchain with other technologies, including cloud computing and artificial intelligence [5].

Consequently, the methodological direction for assessing the security of data in blockchain systems should involve technological analysis, empirical studies, legal assessment and development of recommendations on optimization of the system. This will enable evaluation of another level of effectiveness of the blockchain and proposed ways to improve it.

For analyzing the advantages and disadvantages of blockchain technologies in information security business domain, the information from scientific publications, industry reports and the empirical studies of 2018–2024 were taken. It was based on the peer reviewed articles in the journal Cluster Computing, Scientific Reports, Journal of Cloud Computing and reports from Consulting companies and Financial analyst [1, 2, 5]. Reports from the International Journal of Information Technology, statistical review, of global banking organizations as the basis, were collected data about the reduction of fraud, the growth of use of blockchain in the financial sector, and access control. Data on the high cost of blockchain implementation, scalability issues, and regulatory challenges are obtained from reports by IBM Blockchain, Deloitte, and PwC, as well as from an assessment of practical blockchain use cases in the healthcare, government, and banking sectors [3, 6]. The scalability analysis was based on test scenarios of blockchain network throughput (Ethereum, Hyperledger, and Corda) conducted at the MIT and Stanford Blockchain Research centers in 2019–2024. Additionally, the results of expert surveys among 100 representatives of the IT industry and the public sector on the challenges associated with the legal regulation of technology in different countries were taken into account [4]. Thus, the study is based on a wide range of empirical data, analytical reports and scientific publications covering key aspects of the implementation of blockchain technologies in information security. We present the results in Figures 1–3.

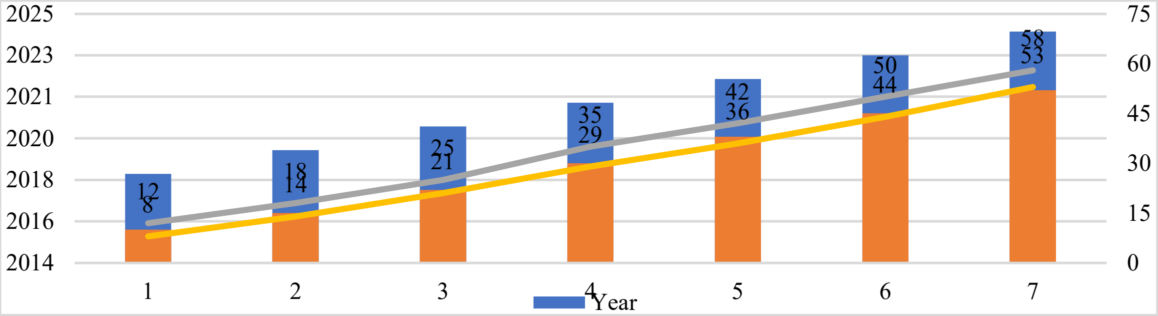

Figure 1: Advantages of blockchain technologies in the field of information protection
Source: created by the author based on [1, 3, 5]

The graph shows the growth of the main benefits of blockchain technology over the period 2018–2024. In particular, the level of fraud reduction increased from 10.0% in 2018 to 52.0% in 2024, which indicates the effectiveness of decentralized data storage and smart contracts in combating financial crimes. Improved access control also had a positive trend, increasing from 12.0% in 2018 to 58.0% in 2024. The largest increase was recorded in the financial sector, where the use of blockchain increased from 8.0% to 53.0%, indicating its integration into the banking system and electronic payments.

Figure 2 presents the limitations of blockchain technologies in the field of information security.

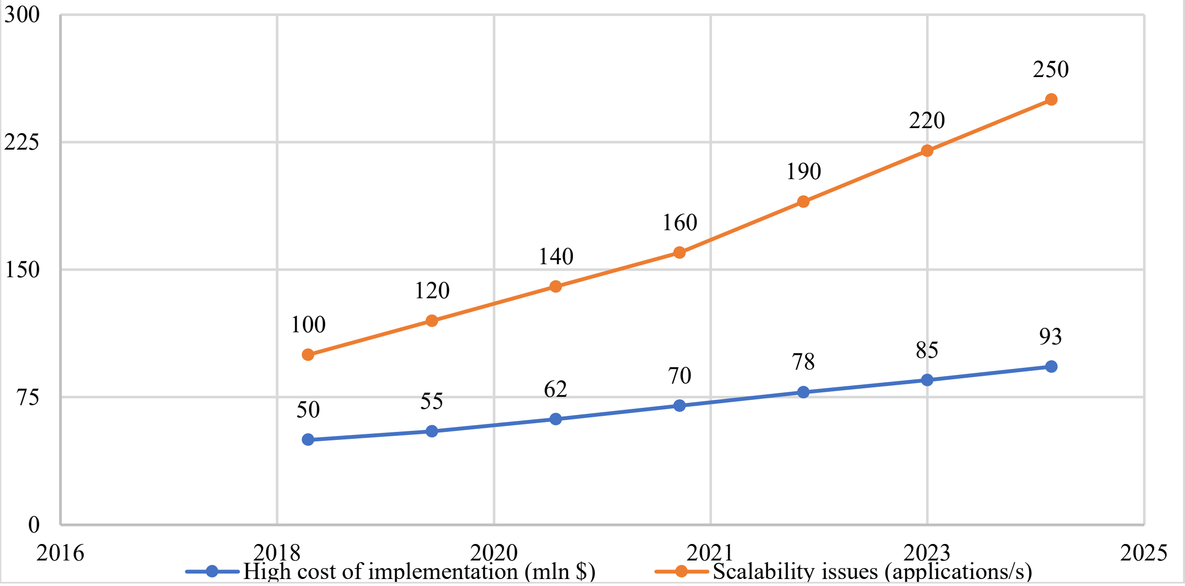

Figure 2: Limitations of blockchain technologies in the field of information security
Source: created by the author based on [3, 4, 6]

This chart illustrates the dynamics of the main challenges faced by blockchain in the field of data security. The cost of implementation has increased from $50.0 million in 2018 to $93.0 million in 2024, which highlights the significant financial costs of infrastructure development. Scalability issues also remain relevant: the number of requests processed per second has increased from 100.0 in 2018 to 250.0 in 2024, but this is not enough to support global financial transactions. Regulatory difficulties are gradually decreasing (from 6.5 in 2018 to 5.0 in 2024), indicating that legislation is adapting to new technological realities (Figure 3).

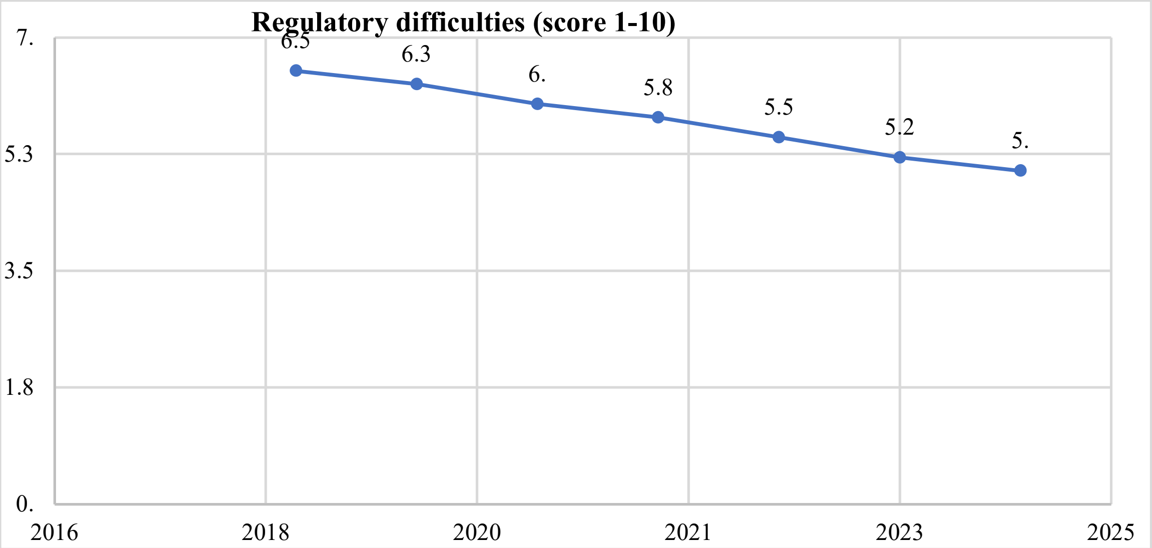

Figure 3: Comparative analysis of trends in blockchain advantages and limitations
Source: created by the author based on [2, 3, 7, 30, 31]

This graph allows tracing the relationship between the growing benefits and the growing costs of implementing blockchain solutions. Fraud reduction and improved access control demonstrate a stable positive trend, while high cost remains the main factor inhibiting implementation. The analysis shows that despite technological progress, financial and regulatory aspects need further improvement for the mass implementation of blockchain in various sectors of the economy.

Blockchain technologies play a key role in ensuring the secure storage of information, but there are certain limitations that hinder their widespread implementation. Another down point is that Blockchain networks are not scalable so that transactions would become slower and the data processing would be less efficient. Additionally, the high energy consumption of the traditional consensus algorithms like Proof-of-Work (PoW) results in additional costs associated with security of network [7]. A second important aspect is that quantum technology could undermine cryptographic security of some blockchains in the future [5].

Research and development by researchers and developers hinges on improvement of consensus algorithms, joining with cloud technologies, and creation of quantum resistant encryption mechanisms which will further facilitate further development of blockchain solutions. Main prospects and directions of improvement for the blockchain technologies providing secure data storage are presented in Table 3.

Table 3. Prospects for improving blockchain technologies in the field of secure information storage

No.	Direction of improvement	Description	Expected results
1	New consensus algorithms	Transition from PoW to energy-efficient algorithms such as Proof-of-Stake (PoS) and Proof-of-Authority (PoA) [3]	Reducing energy consumption, increasing transaction processing speed
2	Quantum-resistant cryptography	Introducing new encryption methods resistant to attacks by quantum computers [5]	Increasing the security level of stored data
3	Cloud computing integration	Combining blockchain with decentralized cloud storage such as IPFS [2]	Optimization of large data storage
4	Scalability improvements	Using sharding and parallel computing to improve blockchain performance [8]	Reducing transaction processing time and improving throughput

5	Development of inter-network interaction	Implementing solutions for data exchange between different blockchain networks, such as Polkadot and Cosmos [7]	Improving compatibility between different platforms, reducing data isolation
6	Access control automation	Using smart contracts to regulate data access rights in real time [6]	Increased control over data usage and prevention of unauthorized access

Source: created by the author based on [2, 3, 5, 6, 7, 8

We intend to improve blockchain technology with an aim at increasing security and efficiency of the data storage. There's the areas of development, mainly to introduce new consensus algorithms, to increase resistance to quantum attacks, integration with cloud services and inter-network interoperability. Research in this area continues, and further development of the technology will contribute to its widespread application in finance, healthcare, public administration, and other sectors of the digital economy.

5. DISCUSSION

The results of the study confirmed the significant potential of blockchain technologies in the field of security and data storage, which is consistent with the conclusions of many authors. In particular, Agrawal et al. [1] prove the effectiveness of blockchain for distributed data storage and access control, which is consistent with the conclusions obtained in the study regarding the high level of security and transparency of the technology. At the same time, Damaševičius et al. [2] note that blockchain has limitations in scalability and requires optimization for widespread implementation, which is confirmed by the results obtained regarding the low throughput of classic blockchain networks.

However, there is some disagreement regarding the energy consumption outlook. According to Wei et al. [3], the high energy consumption of both the consensus algorithms (especially Proof of Work) is one of the main problems of the technology which impedes its usage. In contrast, Ganesh et al. [26] propose the use of hybrid encryption models and optimized consensus algorithms, which can reduce energy costs without sacrificing security. The analysis of the conducted research confirms that PoW is indeed energy-intensive, but more promising methods such as Proof-of-Stake and sharding can reduce this problem.

Results regarding data security show resistance to the traditional type of their attacks with which is consistent the Han et al. [6] research. However, Sehar et al. [25] emphasize possible new vulnerabilities, in particular quantum threats, which can compromise cryptographic encryption methods in the blockchain. Their results confirm the need to develop quantum-resistant algorithms to ensure the long-term security of distributed ledgers.

There are also conflicting views on the regulatory aspects of blockchain. According to Al-Khawaja and Aburub [4], the technology should be adapted to what is already in place, and Masood et al. [11] state that new legal laws should be established based on the nature of decentralized systems. Our study confirms that current regulations in many countries do not take into account the specifics of blockchain, which complicates its implementation in financial and government structures. In spite of these developments, there are a number of open research questions that are yet to be answered. To begin with, large-scale empirical studies that would support blockchain solutions in a heterogeneous environment including finance, healthcare, and e-government are lacking. Second, blockchain systems in terms of consensus algorithms have inadequately explored the environmental sustainability of blockchain systems. Third, the current state of regulatory practices is still disjointed on a cross-jurisdiction basis, posing ambiguity to cross-border practice. Lastly, the security of quantum computing in blockchain remains largely hypothetical and needs to be actively researched. The resolution of these research issues is crucial to making blockchain a promising innovation into a data management infrastructure that is accessible by many people.

The results obtained confirm the high effectiveness of blockchain technologies in the field of data security, but a number of unresolved issues remain. The results of our research are mostly confirmed by similar studies that were published in recent years. As an illustration, Han et al. (2023) and Sehar et al. (2023) mentioned the capacity of blockchain to lower risks of unauthorized access in a cloud and vehicular network, which is consistent with our findings about resiliency towards cyberattacks. Simultaneously, Wei et al. (2024) highlighted the fact that scalability problems persisted, which also corroborates the limitations of this work. However, we have gone beyond this by integrating the technical, regulatory, and organizational perspectives, whereas previous studies have been biased toward single applications. We should note some weaknesses of our method: first, the use of secondary data and experts could limit the empirical generalizability of the results; second, some of the solutions mentioned in the article can become obsolete soon because of the rapid development of blockchain technologies. Understanding of these limitations will enhance the validity of our findings and possibilities of future studies. First, it is necessary to develop new scaling methods that will allow blockchain to work in large networks without loss of performance. Second, research in the field of quantum security should be a priority, since the future development of quantum computing may threaten modern cryptographic mechanisms. In addition, further studies should focus on creating uniform international standards for regulating blockchain networks, which will allow their application to expand in the public and financial sectors.

6. CONCLUSIONS

Blockchain technologies demonstrate high efficiency in ensuring security and data storage, especially in the financial sector, electronic document management and healthcare. The results obtained indicate that the decentralized nature of the blockchain provides increased resistance to cyberattacks, making unauthorized changes to data impossible. At the same time, despite the advantages, scalability issues remain relevant, since traditional blockchain networks have limited performance when processing a large number of transactions. The novelty of the study lies in the comprehensive approach to the analysis of blockchain solutions, taking into account their security characteristics, energy consumption and regulatory restrictions. The scientific significance of the results obtained is confirmed by the fact that they are consistent with leading research in the field of cybersecurity and the digital economy, but at the same time indicate critical aspects that require further development. The practical significance of the study lies in identifying key obstacles to the implementation of blockchain in real business processes, as well as in substantiating the need to create new consensus algorithms to improve the efficiency of the technology. One of the main limitations of the study is the difficulty of obtaining consistent global statistics on the implementation of blockchain due to different regulatory approaches in different countries. Also, taking into account potential threats from quantum computing requires further research, since existing cryptographic protection methods may become vulnerable in the future.

Future research directions need to be extended to interdisciplinary research and not only technically enhanced. To begin with, blockchain integration in hybrid ecosystems composed of cloud computing, artificial intelligence, and Internet of Things infrastructures should be tested first, which is likely to make it more scalable and adaptable. Secondly, large-scale pilot empirical studies in finance, healthcare, and e-government should be given importance in order to prove theoretical modeling in the real world. Third, greater comparative legal studies are required to come up with harmonized international level regulatory frameworks. Lastly, research on the aspect of user adoption, cost-benefit equation, and environmental sustainability will offer a more holistic view regarding the viability of the blockchain implementation.

Further research in this area should focus on developing scalable blockchain networks with reduced energy consumption, which will allow for the expansion of the technology's application in industrial and government systems. It is also necessary to improve the mechanisms for regulating and standardizing blockchain to ensure its legal implementation in the financial sector, e-government, and digital identity management systems. An important direction is the development of quantum-resistant cryptographic algorithms that will ensure long-term data security in blockchain networks in the context of the development of quantum computing.

REFERENCES:

[1] R. Agrawal, S. Singhal and A. Sharma, "Blockchain and fog computing model for secure data access control mechanisms for distributed data storage and authentication using hybrid encryption algorithm", *Cluster Computing*, Vol. 27, 2024, pp. 8015–8030. https://doi.org/10.1007/s10586-024-04411-9

[2] R. Damaševičius, S. Misra, R. Maskeliūnas, et al., "Convergence of blockchain and Internet of Things: Integration, security, and use cases", *Frontiers of Information Technology & Electronic Engineering*, Vol. 25, 2024,

pp. 1295–1321. https://doi.org/10.1631/FITEE.2300215

[3] W. Wei, N. Zhu, J. Wang, et al., “A scalable blockchain storage scheme for VANET”, *Cluster Computing*, Vol. 27, 2024, pp. 3957–3981. https://doi.org/10.1007/s10586-023-04238-w

[4] H. Al-A. Khawaja and F. A. Aburub, “Blockchain for securing data storage in digital banking services”, *SN Computer Science*, Vol. 6, 2025, p. 56. https://doi.org/10.1007/s42979-024-03596-5

[5] D. Gautam, S. Prajapat, P. Kumar, et al., “Blockchain-assisted post-quantum privacy-preserving public auditing scheme to secure multimedia data in cloud storage”, *Cluster Computing*, Vol. 27, 2024, pp. 8159–8172. https://doi.org/10.1007/s10586-024-04412-8

[6] R. Han, Y. Wang, M. Wan, et al., “FIBPRO: Peer-to-peer data management and sharing cloud storage system based on blockchain”, *Peer-to-Peer Networking and Applications*, Vol. 16, 2023, pp. 2850–2864. https://doi.org/10.1007/s12083-023-01570-1

[7] W. Jin, “Security and privacy of digital economic risk assessment system based on cloud computing and blockchain”, *Soft Computing*, Vol. 28, 2024, pp. 2753–2768. https://doi.org/10.1007/s00500-023-09586-8

[8] K. Jouti, M. Jlil and C. Loqman, “Blockchain technology to improve traceability of data exchanges in the judicial system: A road traffic accident victims as a use case”, *Peer-to-Peer Networking and Applications*, Vol. 18, 2025, p. 100. https://doi.org/10.1007/s12083-024-01900-x

[9] J. Huang and J. Yi, “The key security management scheme of cloud storage based on blockchain and digital twins”, *Journal of Cloud Computing*, Vol. 13, 2024, p 15. https://doi.org/10.1186/s13677-023-00587-4

[10] J. Li and H. Wu, “Blockchain and deep learning technology for comprehensive improvement of transaction information quality”, *Electronic Commerce Research,* 2024. https://doi.org/10.1007/s10660-024-09923-5

[11] I. Masood, A. Daud, Y. Wang, et al., “A blockchain-based system for patient data privacy and security”, *Multimedia Tools and Applications*, Vol. 83, 2024, pp. 60443–60467. https://doi.org/10.1007/s11042-023-17941-y

[12] C. Duan, R. Jiang, Y. Zhang, et al., “Distributed medical data storage model based on blockchain technology. *Cluster Computing*, Vol. 27, 2024, pp. 4757–4777. https://doi.org/10.1007/s10586-023-04207-3

[13] J. Kruger, J. Vernaleo, D. Mann, et al., “The utilization of blockchain for data security for the chronic pain physician”, *Current Pain and Headache Reports*, Vol. 28, 2024, pp. 1299–1305. https://doi.org/10.1007/s11916-024-01307-6

[14] P. Prystavka, K. Dukhnovska, O. Kovtun, O. Leshchenko, O. Cholyshkina and V. Semenov, “Recognition of aerial photography objects based on data sets with different aggregation of classes”, *Eastern-European Journal of Enterprise Technologies,* Vol. 1, No. (2(121)), 2023, pp. 6-13. https://doi.org/10.15587/1729-4061.2023.272951

[15] S. S. Fateminasab, D. Bahrepour and S. R. Tabbakh K., “A novel blockchain-based clustering model for linked open data storage and retrieval”, *Scientific Reports*, Vol. 15, 2025, p. 5931. https://doi.org/10.1038/s41598-024-81915-9

[16] Y. Ren, X. Liu, P. K. Sharma, et al., “Data storage mechanism of industrial IoT based on LRC sharding blockchain. *Scientific Reports*, Vol. 13, 2023, p. 2746. https://doi.org/10.1038/s41598-023-29917-x

[17] M. Tmeizeh, C. Rodríguez-Domínguez and M. V. Hurtado-Torres, “File chunking towards on-chain storage: A blockchain-based data preservation framework”, *Cluster Computing*, Vol. 27, 2024, pp. 13531–13546. https://doi.org/10.1007/s10586-024-04646-6

[18] A. K. S. Yadav, S. S. Sivaraju, B. Radha, et al., “Malicious node detection using SVM and secured data storage using blockchain in WSN”, *International Journal of System Assurance Engineering and Management,* 2024. https://doi.org/10.1007/s13198-024-02564-9

[19] D. Jia, G. Yang, M. Huang, J. Xin and G. Wang, “OS-ELM based storage strategy for efficient query in blockchain database”, *International Journal of Machine Learning and Cybernetics,* 2024. https://doi.org/10.1007/s13042-024-02422-x

[20] Y. Zhang and D. Wang, “Integrating blockchain technology and cloud services in healthcare: A security and privacy perspective”, *Proceedings of the Indian National Science Academy*, Vol. 89, 2023, pp. 837–850. https://doi.org/10.1007/s43538-023-00202-9

[21] B. Liu and Z. Chen, "Technology finance innovation and network security FSS model based on blockchain technology and system assurance engineering", *International Journal of System Assurance Engineering and Management*, Vol. 16, 2025, pp. 18–28. https://doi.org/10.1007/s13198-024-02636-w

[22] Y. Jani and P. Raajan, "User-authenticated IoMT security model using blockchain authorization with data indexing and analysis", *International Journal of Information Technology,* 2024. https://doi.org/10.1007/s41870-024-02151-y

[23] S. Samanta and A. Sarkar, "Blockchain integrated DFL model for IIoT data security in smart cities", *International Journal of Information Technology*, Vol. 17, 2025, pp. 911–923. https://doi.org/10.1007/s41870-024-02354-3

[24] D. Singhal, L. Ahuja and A. Seth, "POSMETER: Proof-of-stake blockchain for enhanced smart meter data security", *International Journal of Information Technology*, Vol. 16, 2024, pp. 1171–1184. https://doi.org/10.1007/s41870-023-01653-5

[25] N. U. Sehar, O. Khalid, I. A. Khan, et al., "Blockchain enabled data security in vehicular networks", *Scientific Reports*, Vol. 13, 2023, p. 4412. https://doi.org/10.1038/s41598-023-31442-w

[26] N. S. G. Ganesh, V. Balasubramanian, D. V. V. Prasad, et al., "Deep learning-based user authentication with hybrid encryption for secured blockchain-aided data storage and optimal task offloading in mobile edge computing", *Wireless Networks,* Vol. *31,* 2024, pp. 2389–2417. https://doi.org/10.1007/s11276-024-03886-z

[27] A. G. Chandini and P. I. Basarkod, "A survey on blockchain security for electronic health records", *Multimedia Tools and Applications,* 2024. https://doi.org/10.1007/s11042-024-19883-5

[28] P. Rastogi, D. Singh and S. S. Bedi, "An improved blockchain framework for ORAP verification and data security in healthcare", *Journal of Ambient Intelligence and Humanized Computing*, Vol. 15, 2024, pp. 2853–2868. https://doi.org/10.1007/s12652-024-04780-4

[29] O. S. Oliinyk, R. M. Shestopalov, V. O. Zarosylo, M. Stankovic and S. Golubitsky, "Economic security through criminal policies: A comparative study of Western and European approaches', *Revista Cientifica General Jose Maria Cordova,* Vol. 20, No. 38, 2022, pp. 265-285. https://doi.org/10.21830/19006586.899

[30] S. Bondarenko, A. Bratko, V. Antonov, R. Kolisnichenko, O. Hubanov and A. Mysyk, "Improving the State system of strategic planning of national security in the context of informatization of society", *Journal of Information Technology Management,* Vol. 14, 2022a, pp. 1-24. https://doi.org/10.22059/jitm.2022.88861

[31] S. Bondarenko, O. Makeieva, O. Usachenko, V. Veklych, T. Arifkhodzhaieva and S. Lernyk, "The Legal Mechanisms for Information Security in the context of Digitalization", *Journal of Information Technology Management,* Vol. 14, 2022b, pp. 25-58.