Application of blockchain technology as a connecting digital technology

Natalya Kolyeva[1*], *Mikhail* Panov[1], *Evgeny* Ishchenko[1], *Ilgiziar* Husnetdinov[1], and *Vsevolod* Shaykin[1]

[1]Ural State University of Economics, Ulitsa 8 Marta, 62/45, 620144, Yekaterinburg, Russian Federation

Abstract. The growing problems of software security require innovative solutions. One of the methods of distributed data storage - blockchain - is considered. The focus is on promising areas of development where blockchain technology is already being applied and where it can bring maximum benefit to users. It will also highlight the main challenges that are inhibiting the development of the technology, and preventing widespread adoption of existing practices. This research explores the potential of blockchain technology to improve software security, its impact at both the technical and organizational level. By analyzing current challenges, blockchain principles, and successful integration examples, this study aims to bridge the gap between theory and practice in digital security. Emphasis is placed on the security benefits of blockchain and how they can be used to improve authentication, access control, threat monitoring, and guaranteed storage of digital information. Cases of blockchain applications in this context are presented and the challenges and prospects for the future development of this exciting field are discussed. The paper aims to highlight the relevance and promise of integrating blockchain technologies into software security.

1 Introduction

With the onset of the digital age, software security problems are becoming more and more acute, thus presenting an increasing need for innovative solutions. The main purpose of this research is to provide an in-depth study of blockchain technology as a potential tool to improve software security.

Blockchain technology is a peculiar set of innovative technologies based on the idea of a decentralized distributed ledger. They provide reliability, transparency and ensure that data cannot be tampered with.

One of the options for information protection is the innovative technology “blockchain”. It is a kind of aggregate of blocks connected in a single chain, which is stored by the system without a single server. All blocks in the blockchain are linked, with each subsequent block pointing to the previous one, which in turn creates the possibility of building a continuous and sequential chain of blocks, prearranged in accordance with

* Corresponding author: nkoleva@mail.ru

agreed rules. Using sequential hashing together with cryptography in a decentralized structure, it is possible to build a system, the third-party management of which will be virtually impossible. The main advantage is based on the fact that the blockchain is not controlled by anyone, as all calculations are under the control of an automated system, so in this case the possibility of data falsification is excluded, and the multi-level encrypted chain, in turn, will prevent information leakage [1, 2].

Consider the application of blockchain technology at both a technical and organizational level. By analyzing current problems combined with an understanding of blockchain principles and examining integration examples, this research will provide practical suggestions for improving software security and provides an opportunity to establish the relationship between theory and practice in digital security.

Innovative solutions are needed to realize software security challenges. Blockchain is a type of distributed ledger. It is a technology that creates a distributed and scalable digital transaction registry [3-4].

According to [5-7] blockchain technology is a potential solution to improve software security due to its distributed, decentralized and tamper-proof characteristics.

Implementing blockchain technologies in software systems will effectively combat complex network threats and ensure data integrity and security. In this regard, consider the potential of applying blockchain technologies to improve software security to provide promising solutions to current and future digital security challenges.

First, it is necessary to understand how blockchain technology fits into an organization's existing architecture. This may involve restructuring the existing information technology infrastructure to accommodate the distributed and decentralized nature of blockchain.

Second, consideration should be given to training the organization's employees to understand and effectively use this new technology.

Regulatory and compliance issues must also be addressed to ensure blockchain integration complies with regulations and avoids potential legal risks. In order to successfully implement blockchain technology to improve software security, it is necessary to investigate possible obstacles and ways to overcome them [8, 9].

Regulatory and compliance issues are also an important factor. There is a need to ensure that blockchain integration complies with certain regulations and can adapt quickly when regulations change.

Blockchain technology offers unique opportunities for the guaranteed and secure storage of digital information. Let us present several aspects that emphasize this opportunity [10]:

1. Data immutability - creates a continuous history of change and, thanks to the principle of immutability, data once recorded on a blockchain is virtually impossible to change without the consent of the majority of the network.

2. Digital signatures and cryptography - provides strong protection against information tampering and ensures that data remains genuine.

3. Decentralization - information is distributed across multiple nodes and hence there is no single point of failure. This increases the resilience and security of data storage.

4. Resistance to censorship - blockchain technology prevents censorship of data because information is stored in a decentralized network and changing or deleting data requires the consent of the majority of the network participants.

5. Transparency and verifiability - creates transparency and the ability to verify digital information at any point in time.

6. Smart contracts for automation - allows automation of data storage and management processes. Smart contracts can define conditions for accessing, storing, or modifying data, ensuring that agreements are automatically enforced.

Collaboration with other organizations can face trust and security issues, so technical means, such as encryption and authentication, must be used to ensure security when exchanging information and building inter-organizational blockchain networks. Through in-depth research and understanding of these potential obstacles, targeted strategies should be developed to better overcome these challenges and ensure the successful integration of blockchain technologies into organizations to improve software security [11, 12].

2 Research results

Analyzing case studies of successful applications of blockchain technology in information systems programming and security is critical to the research. Consider the application of blockchain in the healthcare industry. The security of medical information is critical, and the transparency and immutability of blockchain make it ideal for securing patient data, such as electronic health records, medication dispensing tracking, and medical supply chain management. With blockchain technology, transparency can be provided at all stages of the supply chain, thereby increasing the security of the entire chain.

In the table we present the advantages and limitations associated with the use of blockchain technology for software security.

Table 1. Advantages and limitations of blockchain technology

Advantages	Limitations
ensures transparency and immutability of data	scalability issues (as the number of participants and data volume increase)
use of cryptographic elements improves identification and authentication processes, enhancing security	legal uncertainty
smart contracts are used to effectively manage access to data and functionality in the software	depending on the configuration of the blockchain network, there is a risk of data privacy violations (especially in public networks)
cyber resistance	

Based on this analysis, we highlight the following specific recommendations for improving software security [8-9].

First, before implementing blockchain technology, the goals and scope of the project should be clarified to ensure that blockchain is the right tool for solving real-world security problems.

Second, it is necessary to provide comprehensive training to employees within the organization so that they understand how blockchain technology works and the potential security benefits. When selecting a blockchain platform, it is necessary to comprehensively consider the performance, security, and applicability of the platform based on the needs of the project, and weigh the advantages and disadvantages of different platforms. You should also focus on compliance aspects, ensuring that blockchain integration complies with relevant regulations.

Smart contracts are also being developed to better control access to data and functions based on specific security needs. In terms of data sharing, effective privacy protection measures should be implemented to ensure that information is protected from unauthorized

access. It is recommended to establish a mechanism for regular review of security policies to maintain sensitivity to new threats and make timely adjustments [13-15].

3 Conclusion

Thus, the recommendations presented above are intended to provide practical guidelines for implementing blockchain technologies to improve software security and ensure successful project implementation.

It is especially important to discuss the future prospects of blockchain technology in enhancing software security. With the development of digitalization, blockchain technology has broad application prospects in software security. First, we can foresee a continued role for blockchain in ensuring data integrity and resilience to unauthorized access, providing strong security guarantees for software systems.

However, future development also faces some challenges. Blockchain technology needs continuous innovation to address current performance and scalability issues and to ensure its effectiveness in large-scale applications. Regulatory and compliance issues also need to be addressed more comprehensively to facilitate the legal application of blockchain technology worldwide. In addition, user education will also be key to increasing the understanding and acceptance of blockchain technology to better promote its application in software security.

Overall, blockchain technology holds great promise for improving software security, but continuous efforts must be made to address technical, regulatory, and educational challenges to ensure its comprehensive and sustainable development.

Second, the development of smart contracts will further strengthen security controls over access to data and functional operations, as well as improve the overall security of software systems. In addition, the distributed nature of blockchain is expected to further reduce the risks of centralized systems and increase system reliability and availability.

The results of the study emphasize the significant potential of blockchain technologies in improving software security. By analyzing existing software security issues, we determined that blockchain technologies are uniquely positioned to address this problem. Specific suggestions cover clear project objectives, comprehensive staff training, selection of the right platform, attention to regulatory compliance, development of smart contracts, and privacy protection. And they also provide practical recommendations for implementing blockchain technology to improve software security. Despite the technical, regulatory, and educational challenges, we expect blockchain technology to play an even greater role in the future as it continues to innovate and solve problems to make software systems more secure.

References

1. I. Semenchukova, “Prospects for the use of blockchain and cryptocurrencies technology in Belarus,” Education and science in the 21st century: Articles of the V International Scientificand Practical Conference, Vitebsk. 2020. P. 119-122.
2. N. Kolyeva, “Organization of multi-access in databases,” E3S Web of Conferences **270**, 01006 (2021). https://doi.org/10.1051/e3sconf/202127001006.
3. Swan M. Blockchain: Blueprint for a New Economy. O’Reilly Media. 2015. [Electronic resource]. URL: https://www.scirp.org/reference/ReferencesPapers.aspx?ReferenceID=2529258.

4. M.G. Abugsesa, “How can blockchain technology improves the performance of organizations?” News of Scientific Achievements. Economics and Law. 2020. **No. 6.** P. 323-331. DOI 10.36616/2686-9837-2020-6-323-331.
5. N. Kolyeva, V. Gorodnichev, M. Panova “Fundamental factors of the p/e multiplier and their use in search for undervalued assets,” Moscow economic journal. 2022. Vol. **7**, no. 12. P. 598-604.
6. E.I Bych, N.S. Moskvicheva, V.A. Svadkovski, “Application of blockchain technology in small and large businesses,” Actual Problems and Prospects of Economic Development: Russian and Foreign Experience. 2020. No. **3(28).** P. 83-86.
7. M.A. Morozova, Yu.G. Stepanov, D.I. Burlov “Innovations in Tourism and Hospitality through Modern Information Systems and Blockchain Technologies,” Components of Scientific and Technological Progress. 2021. No**. 11(65).** P. 42-46.
8. T. Pyatkova, N. Kolyeva, M. Panova, “Conceptual approach to the development of technology for virtual mobility modeling of distance learning students,” E3S Web of Conferences **376**, 05041 (2023). https://doi.org/10.1051/e3sconf/20233760504
9. A.D. Dziatkovskii, V.A. Hruneuski, “The use of blockchain technology and homeostatic principles in the monetary policies of states” Financial Markets and Banks. 2021. N**o. 8.** P. 3-10..
10. L. Kortenko, N. Kolyeva, E. Radkovskaya, “Designing a microservice architecture on the example of an automated application for the HR department,” E3S Web of Conferences, **402**, 03043 (2023). https://doi.org/10.1051/e3sconf/202340203043
11. N. Firsova, J. Abrham “Economic perspectives of the Blockchain technology: Application of a SWOT analysis,” Terra Economicus. 2021. **Vol. 19,** No. 1. P. 78-90. DOI 10.18522/2073-6606-2021-19-1-78-90.
12. N. Kolyeva, “Development of a model for assessing the complexity of learning information, AIP Conference Proceedings **2812(1),** 020071 (2023). https://doi.org/10.1063/5.0162508
13. A.A. Stepanyan, R.G. Neychev “AI applications in blockchain technology,” Proceedings of National Polytechnic University of Armenia. Information Technologies, Electronics, Radio Engineering. 2023. No. **1**. P. 51-58. DOI 10.53297/18293336-2023.1-51.
14. N. Kolyeva, V. Gorodnichev, “Analysis of using queuing systems for estimating the performance of computing systems,” AIP Conference Proceedings 2812(1), 020088 (2023). https://doi.org/10.1063/5.0161392
15. A.G. Aliyev, “Research of risks and threats of using cryptocurrency and blockchain technologies in the digital environment,” Information Technology. Problems and Solutions. 2022. No. **4(21).** P. 55-61.