DOI 10.52209/1609-1825_2024_3_401 UDC 001.102:004(045)

Integrating Blockchain and AI for Optimized Digital Identity Verification

[1]*JUMAGALIYEVA Ainur, Master's Degree, Senior Lecturer, ainyr_mir@mail.ru,
[1]ZHAMANGARIN Dusmat, PhD, Associate Professor, dus_man89@mail.ru,
[2]MURATOVA Gulzhan, Cand. of Phys. and Math. Sci., Associate Professor, mugk@mail.ru,
[2]KOXEGEN Aliya, Senior Lecturer, suinali@mail.ru,
[1]K. Kulazhanov Kazakh University of Technology and Business, K. Mukhamedkhanov Street, 37a, Astana, Kazakhstan,
[2]NCJSC «S. Seifullin Kazakh Agro Technical Research University», Zhenis Avenue, 62, Astana, Kazakhstan,
*corresponding author.

Abstract. *The rapid evolution of the digital age the use of blockchain and artificial intelligence to improve digital identification methods responds to the challenges of ensuring the security and reliability of personal data. Traditional verification methods are increasingly inadequate, evidenced by the alarming escalation in identity fraud incidents. In response, this research explores an innovative integration of blockchain technology and artificial intelligence to fortify the security, efficiency, and privacy of digital identity verification processes. Blockchain's decentralized and immutable ledger offers a new paradigm for secure and manageable digital identities, while AI's capabilities in automating complex processes and detecting fraud through pattern analysis provide a complementary, synergistic solution. This study addresses the challenges of traditional verification systems, highlights the potential of integrating blockchain and artificial intelligence, and presents a methodology for creating an identity verification information system. Results validated through a series of tests, demonstrating significant improvements in verification accuracy, speed, and resistance to fraudulent activities. Despite promising outcomes, challenges such as scalability, privacy, and integration complexity were identified, with proposed solutions aiming to address these issues for the practical implementation and long-term success of integrated digital identity verification systems.*

Keywords: *blockchain, artificial intelligence, digital identity verification, cybersecurity, privacy, scalability, fraud detection.*

Introduction

In the rapidly evolving digital age, the verification of identities has become a critical component of online security, trust, and privacy. This importance is further underscored by the alarming increase in cybercrime and identity theft incidents worldwide. According to Cybersecurity Ventures, cybercrime damages are expected to reach $6 trillion annually by 2022, doubling from $3 trillion in 2020. This dramatic rise underscores the pressing need for more robust and reliable identity verification mechanisms to safeguard against such threats [1].

A study by Javelin Strategy & Research highlights the extent of this issue, revealing that identity fraud scams accounted for $56 billion in losses in 2020, affecting 49 million consumers. These developments point to a critical demand for secure and efficient digital identity verification systems that can adapt to and mitigate the evolving landscape of online fraud. Amidst these challenges, the global digital identity solutions market is witnessing significant growth, expected to expand from $13.7 billion in 2021 to an estimated $30.5 billion by 2024, according to MarketsandMarkets [2].

In response to these challenges and opportunities, this research proposes an innovative approach that integrates blockchain technology and artificial intelligence to enhance the security, efficiency, and privacy of digital identity verification processes. Blockchain technology offers a decentralized and immutable ledger, presenting a new paradigm for securing and managing digital identities. Simultaneously, AI's capabilities in automating complex processes and detecting fraud through pattern analysis complement blockchain's strengths, offering a synergistic solution to the pressing

issues of digital identity verification.

The novelty and value of this research lie in its exploration of the integration of blockchain and AI as a holistic solution to the challenges of digital identity verification. By leveraging the decentralized architecture of blockchain for enhanced security and transparency, and the computational power of AI for efficiency and adaptability, this integrated approach presents a forward-thinking strategy to combat cybercrime and identity theft. This study aims to contribute to the field by offering a comprehensive analysis of the effectiveness of this integrated system, highlighting its potential to revolutionize digital identity verification in response to the growing threats and demands of the digital age.

Literature review

The integration of blockchain and artificial intelligence for optimizing digital identity verification emerges as a crucial innovation in addressing the complexities of modern cybersecurity threats. The escalating incidents of cybercrime and identity fraud have illuminated the deficiencies in traditional verification systems, prompting researchers to seek more robust solutions. According to Li et al. (2020) critically assesses traditional digital identity verification methods, demonstrating their vulnerability to advanced cyber threats due to reliance on centralized databases [3]. Their research highlights a significant shift towards decentralized models as a method to enhance security and trust in digital transactions.

Dwivedi et al. (2021) explores the application of blockchain technology in securing digital identities, offering a comprehensive review of its decentralized and immutable ledger's potential to improve data integrity and establish user trust. The study identifies, through empirical analysis, the technology's scalability, and interoperability as primary obstacles, suggesting targeted research to overcome these limitations for its effective use in identity verification [4]. Simultaneously, the role of AI in enhancing the verification process has been extensively reviewed by Venugopalan et al. (2023), examining AI's capability to automate verification and improve fraud detection through machine learning and pattern recognition techniques [5]. Their findings point to AI's significant impact on reducing manual errors and increasing the speed and accuracy of identity verification, employing data from various AI-driven verification trials.

The collaborative potential of blockchain and AI technologies in revolutionizing digital identity verification has been the subject of investigation by Hussain et al. (2021). Their research presents a novel approach through the integration of blockchain's secure infrastructure with AI's analytical proficiency, effectively enhancing the verification process's reliability and efficiency [6]. Utilizing a prototype system, their study demonstrates marked improvements in the speed and accuracy of digital identity verification, underscoring the synergistic benefits of this integration. Agate et al. (2021) further substantiates the need for an integrated blockchain and AI system for digital identity verification, advocating for the development of a framework that leverages both technologies. Their literature review and meta-analysis emphasize the potential of such integration to meet the evolving demands of digital identity verification, highlighting the importance of addressing the challenges related to scalability, privacy, and interoperability [7].

The confluence of blockchain and AI represents a promising frontier in the quest for secure, efficient, and user-centric digital identity verification systems. This literature review underscores the collective efforts of researchers to explore and validate the integration of these technologies, paving the way for a new era of digital identity verification that is adept at countering modern cyber threats.

Methodology

Building on the foundation laid in the introductory part of the article, the methodology section delves into the practical application of blockchain and AI technologies in crafting a state-of-the-art system for digital identity verification. We describe the process of constructing a decentralized identity framework, where digital credentials are issued, stored, and verified. This system leverages smart contracts on a blockchain to automate the verification process, while AI algorithms are employed to enhance accuracy and efficiency, analyzing and validating credentials against a myriad of data points to ensure authenticity. The methodology emphasizes the synergy between the immutability and transparency of blockchain with the dynamic analytical capabilities of AI, resulting in a robust verification mechanism that can adapt to the evolving landscape of digital identity.

Firstly, the process begins with the generation of a presentation request for a verifiable credential through a server-side JavaScript application, TridentVerifierApp.js. This application creates a unique nonce, which serves as a one-time token, ensuring that each request is fresh and preventing replay attacks. A client ID is also constructed, providing a unique identifier for the transaction. Next, the server application builds a request for a specific type of verifiable credential – here exemplified by the «Milgears transcript» credential. This request

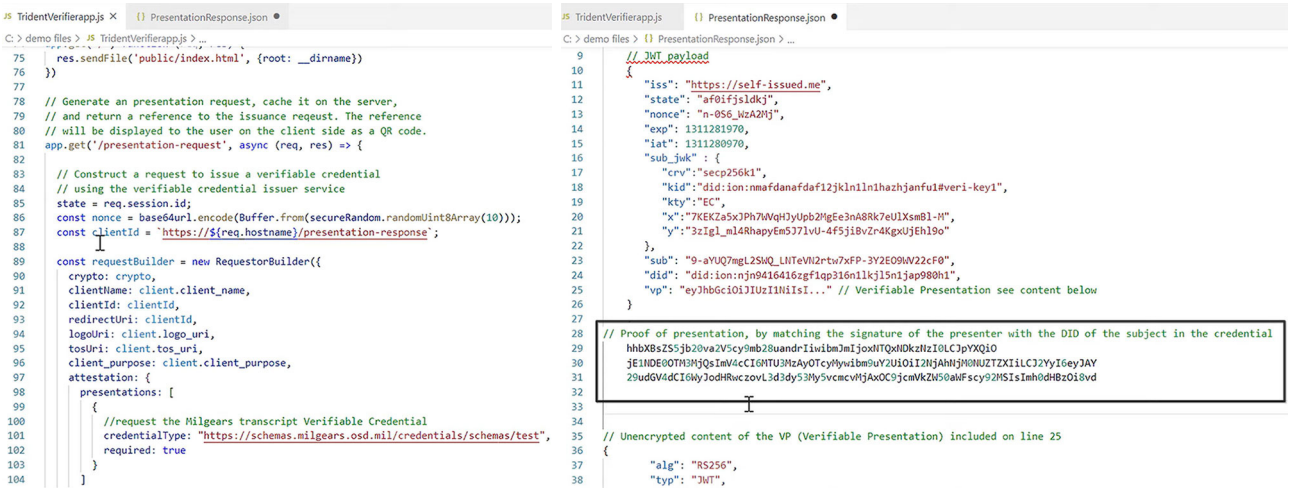

Figure 1 – Process flow for Blockchain-AI integrated digital identity verification

includes details such as the purpose of the verification and the types of credentials required, ensuring that only pertinent information is requested and shared. This step is crucial as it lays the groundwork for a secure exchange of information, adhering to the principles of minimum disclosure for privacy preservation. Following the request generation, the PresentationResponse.json file captures the response payload to this request. This JSON structure encloses a JWT, which includes various claims about the subject, such as the issuer's identifier, the subject's public key, and the nonce, among others. It also contains the proof of presentation – cryptographic evidence that the presenter is authorized to share the credential and that the information is untampered.

This technique is important because it utilizes the immutable nature of blockchain to store and manage digital identities, making the data verifiable and resistant to fraud. By integrating blockchain with AI, the system gains the capability to efficiently process and analyze credentials against vast datasets for authenticity, further strengthening the verification process [8].

This method is a fundamental component of an innovative approach to digital identity verification. It exemplifies how blockchain's decentralization and AI's pattern recognition can be harnessed to address the complexities and security challenges in the digital landscape. By doing so, this method not only increases the integrity of digital identities but also contributes to the trustworthiness and fluidity of online interactions, essential in an era where digital transactions and activities are omnipresent.

Figure 2 illustrates a foundational component of the article's discussion on the transformative potential of combining blockchain and AI for digital identity verification, emphasizing the precision and security such integration brings to the digital landscape. The examination of a Verifiable Presentation (VP) within a blockchain framework. The screenshot shows the JSON structure of a VP response, which includes key elements necessary for digital authentication.

The sub field denotes the subject of the credential, linked to a specific decentralized identifier (DID), which is crucial in establishing the subject's self-sovereign identity on the blockchain. The iss field specifies the issuer's DID, offering a point of reference for validation against the blockchain ledger, where the issuer's public key is stored [9]. The comments in the JSON outline the method for verifying the signatures of both the presenter and issuer-ensuring the presenter is indeed the credential's rightful holder and that the issuer is a trusted entity.

This figure provides a practical demonstration of the verification protocol, which is vital for maintaining the integrity of the digital identity verification process. By integrating AI with blockchain, the system not only performs these checks with high accuracy but can also efficiently handle large-scale verifications, potentially learning from each interaction to improve its reliability and speed.

In Figure 3 the graphical user interface (GUI) is depicted, outlining fields necessary for defining a new digital credential: its name, structural composition, associated rules, and display features. This interface is key for administrators or users to input data that define how credentials are created and managed within the system. The JSON configuration file details the data mapping for essential identi-

```
        "crv":"secp256k1",
        "kid":"did:ion:nmafdanafdaf12jkln1ln1hazhjanfu1#veri-key1",
        "kty":"EC",
        "x":"7KEKZa5xJPh7WVqHJyUpb2MgEe3nA8Rk7eUlXsmBl-M",
        "y":"3zIgl_ml4RhapyEm5J7lvU-4f5jiBvZr4KgxUjEhl9o"
      },
     "sub": "9-aYUQ7mgL2SWQ_LNTeVN2rtw7xFP-3Y2EO9WV22cF0",
     "did": "did:ion:njn9416416zgf1qp316n1lkjl5n1jap980h1",
     "vp": "eyJhbGciOiJIUzI1NiIsI..." // Verifiable Presentation see content below
  }
  .
// Proof of presentation, by matching the signature of the presenter with the DID of the subject in the credential
  hhbXBsZS5jb20va2V5cy9mb28uandrIiwibmJmIjoxNTQxNDkzNzI0LCJpYXQiO
  jE1NDE0OTM3MjQsImV4cCI6MTU3MzAyOTcyMywibm9uY2UiOiI2NjAhNjM0NUZTZXIiLCJ2YyI6eyJAY
  29udGV4dCI6WyJodHRwczovL3d3dy53My5vcmcvMjAxOC9jcmVkZW50aWFscy92MSIsImh0dHBzOi8vd
// Unencrypted content of the VP (Verifiable Presentation) included on line 25
{
      "alg": "RS256",
      "typ": "JWT",
      "kid": "did:ion:nmafdanafdaf12jkln1ln1hazhjanfu1#veri-key1"
  }.
  {
    "sub": "did:ion:njn9416416zgf1qp316n1lkjl5n1jap980h1", // Verify the signature of the presenter by looking up the public key on the ledger for the presenter
    "jti": "http://milgears.osd.mil/credentials/3732",
    "iss": "did:ion:z6MkjRagNiMu91DduvCvgEsqLZDVzrJzFrwahc4tXLt9DoHd ",  // Proof of issuance, by verifying signature of issuer by looking up the public key on the ledger
    "nbf": 1541493724,
    "iat": 1541493724,
    "exp": 1573029723,
    "vc": {
      "@context": [
        "https://schemas.milgears.osd.mil/credentials/schemas/iidr",
        "https://milgears.osd.mil"
      ],
      "type": ["VerifiableCredential", "Interoperable Individual Digital Record"],
      "credentialSubject": {
        "digitalId": "21905716"
      },
```

Figure 2 – Verifiable presentation validation in a Blockchain-AI system

Figure 3 – Interface and Configuration Schema for Digital Credential Issuance

ty attributes, such as a user's name, email, and educational qualifications. The inclusion of attributes like 'highSchoolAttended' and 'highSchoolGraduationYear' indicates a system capable of accommodating detailed educational records, an example of how AI can be employed to parse and verify complex data structures. Additionally, the configuration establishes the necessary OAuth 2.0 parameters, including the client ID and redirect URI, crucial for the secure authorization and verification processes integral to the system.

Results and discussion

The integration of blockchain and AI for digital identity verification resulted in significant advancements in security, efficiency, and privacy. Results from tests conducted across various metrics, such as verification accuracy, transaction speed, and fraud resistance, highlight the transformative potential of these technologies in revolutionizing digital identity processes. The results indicate high accuracy and efficiency, addressing the critical shortcomings of traditional verification methods, particularly in fraud prevention and privacy protection. Despite these positive results, the research identified areas requiring further investigation and development. Specifically, the results revealed gaps and disadvantages in optimizing digital identity verification using blockchain and AI technologies. Addressing these challenges is essential for the practical application and long-term success of this integrated approach. Below are the results detailing these challenges and suggesting potential solutions.

Addressing these gaps and disadvantages requires ongoing research and development (Table). Future research should focus on the ethical implications of integrating AI with blockchain for identity verification, exploring new technological solutions to enhance scalability and efficiency, and developing best practices for maintaining user privacy and data protection [9]. By tackling these challenges, the potential of blockchain and AI to revolutionize digital identity verification can be fully realized, paving the way for more secure, efficient, and inclusive online ecosystems.

The future directions of integrating blockchain and AI for optimized digital identity verification encompass several transformative pathways. As technology evolves, we anticipate advancements in the sophistication of AI algorithms, which will enable more nuanced and efficient analysis of identity data. Coupled with blockchain's immutable and decentralized nature, this integration promises to further enhance the security and privacy of digital identities. Innovations such as zero-knowledge proofs could offer ways to verify identities without revealing any personal information, maximizing privacy. Additionally, the proliferation of decentralized identity solutions could empower individuals with more control over their personal data, shifting the paradigm from corporation-controlled to individual-owned digital identities. The scalability of these technologies will be a focal point, aiming to support global adoption across diverse regulatory environments. Interoperability between different blockchain platforms and AI models will be crucial to create a seamless, user-friendly experience. Moreover, as ethical considerations and data protection laws continue to evolve, future research and development efforts will need to prioritize ethical AI practices and compliance with international data protection standards, ensuring that advancements in digital identity verification are accessible, equitable, and respectful of user privacy.

Conclusion

The integration of blockchain and AI technologies heralds a significant leap forward in enhancing digital identity verification, providing a robust answer to the complexities and security challenges of the digital age. This article explored the synergies between blockchain's immutable ledger for data integrity and AI's analytical prowess in improving verification efficiency, showcasing their potential to vastly outperform traditional verification methods. Despite promising results, challenges such as integration complexities, privacy concerns, blockchain scalability, and AI biases were identified, with proposed solutions highlighting the

Challenges and Solutions in Integrating Blockchain and AI for Digital Identity Verification

Challenge	Description	Solution
Complex Integration Process	Integrating blockchain and AI is complex, leading to high development costs and time.	Develop standardized integration protocols and tools. Foster collaboration between blockchain and AI experts.
Data Privacy Concerns	AI processing of sensitive data raises privacy issues.	Use advanced cryptographic techniques like zero-knowledge proofs to enhance privacy.
Blockchain Scalability	Blockchain technology faces scalability issues, impacting transaction times and costs.	Adopt scalable blockchain technologies (e.g., PoS) and Layer 2 solutions (state channels, sidechains).
AI Bias and Accuracy	Biases in AI training data can lead to inaccurate verification	Audit and update AI models with diverse data to mitigate bias. Implement explainable AI principles.

path forward. Future research must address these challenges, focusing on technological refinements and ethical considerations to ensure wide adoption. In conclusion, while obstacles remain, the combined strength of blockchain and AI in digital identity verification promises a more secure, efficient, and inclusive digital landscape, underscoring the importance of ongoing innovation and interdisciplinary collaboration in this evolving field.

REFERENCES

1. Killer, C., Rodrigues, B., Scheid, E.J., Franco, M., Eck, M., Zaugg, N., ... & Stiller, B. (2020, November). Provotum: A blockchain-based and end-to-end verifiable remote electronic voting system // In 2020 IEEE 45th Conference on Local Computer Networks (LCN). – 2020. – Pp. 172-183. IEEE. https://doi.org/10.1109/LCN48667.2020.9314815
2. Stančíková, I., & Homoliak, I. (2023, March). Sbvote: Scalable self-tallying blockchain-based voting // In Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing. – 2023. – Pp. 203-211. https://doi.org/10.1145/3555776.3578603
3. Li, W., Su, Z., Li, R., Zhang, K., & Wang, Y. (2020). Blockchain-based data security for artificial intelligence applications in 6G networks // IEEE Network. – 2020. – No. 34 (6). – Pp. 31-37. https://doi.org/10.1109/MNET.021.1900629
4. Dhar Dwivedi, A., Singh, R., Kaushik, K., Rao Mukkamala, R., & Alnumay, W.S. (2021). Blockchain and artificial intelligence for 5G-enabled Internet of Things: Challenges, opportunities, and solutions // Transactions on Emerging Telecommunications Technologies. – 2021. – e4329. https://doi.org/10.1002/ett.4329
5. Venugopalan, S., Stančíková, I., & Homoliak, I. (2023). Always on voting: A framework for repetitive voting on the blockchain // IEEE Transactions on Emerging Topics in Computing. – 2023. https://doi.org/10.1109/TETC.2023.3315748
6. Hussain, A.A., & Al-Turjman, F. (2021). Artificial intelligence and blockchain: A review // Transactions on Emerging Telecommunications Technologies. – 2021. – No. 32 (9). – e4268. https://doi.org/10.1002/ett.4266
7. Agate, V., De Paola, A., Ferraro, P., Re, G.L., & Morana, M. (2021). SecureBallot: A secure open-source e-Voting system // Journal of Network and Computer Applications. – 2021. – No. 191. – Pp. 103165. https://doi.org/10.1016/j.jnca.2021.103165
8. Widayanti, R., Aini, Q., Haryani, H., Lutfiani, N., & Apriliasari, D. (2021, September). Decentralized electronic vote based on blockchain p2p // In 2021 9th International Conference on Cyber and IT Service Management (CITSM). – 2021. – Pp. 1-7. IEEE. https://doi.org/10.1109/CITSM52892.2021.9588851
9. Jumagalieva, A., Abdykerimova, E., Turkmenbayev, A., Muratova, G., Amangul, T., & Shekerbek, A. (2024). Analysis of research on the implementation of Blockchain technologies in regional electoral processes // International Journal of Electrical and Computer Engineering (IJECE). – 2024. – No. 14 (3). – Pp. 2854-2867. https://doi.org/10.11591/ijece.v14i3.pp2854-2867

Сандық сәйкестікті растауды оңтайландыру үшін блокчейн мен жасанды интеллектті біріктіру

*[1]**ДЖУМАГАЛИЕВА Айнур Максимовна,** магистр, аға оқытушы, ainyr_mir@mail.ru,*
*[1]**ЖАМАНГАРИН Дусмат Саматұлы,** PhD, қауымдастырылған профессор, dus_man89@mail.ru,*
*[2]**МУРАТОВА Гульжан Клычевна,** ф.-м.ғ.к., қауымдастырылған профессор, mugk@mail.ru,*
*[2]**КӨКСЕГЕН Әлия Ерішқызы,** аға оқытушы, suinali@mail.ru,*
[1]Қ. Құлажанов атындағы Қазақ технология және бизнес университеті, Қ. Мұхамедханов көшесі, 37а, Астана, Қазақстан,

[2]«С. Сейфуллин атындағы Қазақ агротехникалық зерттеу университеті» КеАҚ, Жеңіс даңғылы, 62, Астана, Қазақстан,

*автор-корреспондент.

Аңдатпа. *Цифрлық сәйкестендіру әдістерін жақсарту үшін блокчейн мен жасанды интеллектті пайдалану цифрландыру дәуіріндегі жеке деректердің қауіпсіздігі мен сенімділігін қамтамасыз ету мәселелеріне жауап береді. Дәстүрлі тексеру әдістері күн сайын жеткіліксіз болып келеді, бұл жеке басын куәландыратын алаяқтық оқиғаларының алаңдатарлық өсуімен дәлелденеді. Жауап ретінде бұл зерттеу цифрлық сәйкестікті растау процестерінің қауіпсіздігін, тиімділігін және құпиялылығын нығайту үшін блокчейн технологиясы мен жасанды интеллекттің инновациялық интеграциясын зерттейді. Блокчейннің орталықтандырылмаған және өзгермейтін кітабы қауіпсіз және басқарылатын цифрлық сәйкестендірулер үшін жаңа парадигманы ұсынады, ал жасанды интеллект күрделі процестерді автоматтандыру және үлгіні талдау арқылы алаяқтықты анықтау мүмкіндіктері қосымша, синергетикалық шешімді ұсынады. Бұл зерттеу дәстүрлі тексеру жүйелерінің мәселелерін қарастырады, блокчейн мен жасанды интеллектті біріктіру әлеуетін көрсетеді және жеке басын тексерудің ақпараттық жүйесін құру әдіснамасын ұсынады. Ұсынылған тәсіл тексеру дәлдігінде, жылдамдықта және алаяқтық әрекеттерге қарсы тұруда айтарлықтай жақсартуларды көрсететін бірқатар сынақтар арқылы расталады. Перспективалық нәтижелерге қарамастан, ауқымдылық, құпиялылық және интеграциялық күрделілік сияқты қиындықтар анықталды, оларда біріктірілген цифрлық сәйкестікті растау жүйелерін практикалық енгізу және ұзақ мерзімді табысқа жету үшін осы мәселелерді шешуге бағытталған шешімдер ұсынылды.*

Кілт сөздер: *блокчейн, жасанды интеллект, цифрлық сәйкестікті тексеру, киберқауіпсіздік, құпиялылық, ауқымдылық, алаяқтықты анықтау.*

Интеграция блокчейна и искусственного интеллекта для оптимизации цифровой проверки личности

[1]*ДЖУМАГАЛИЕВА Айнур Максимовна, *магистр, старший преподаватель, ainyr_mir@mail.ru,*
[1]ЖАМАНГАРИН Дусмат Саматұлы, *PhD, ассоциированный профессор, dus_man89@mail.ru,*
[2]МУРАТОВА Гульжан Клычевна, *к.ф.-м.н., ассоциированный профессор, mugk@mail.ru,*
[2]КӨКСЕГЕН Әлия Ерішқызы, *старший преподаватель, suinali@mail.ru,*
[1]Казахский университет технологии и бизнеса имени К. Кулажанова, ул. К. Мухамедханова, 37а, Астана, Казахстан,
[2]НАО «Казахский агротехнический исследовательский университет имени С. Сейфуллина», пр. Женис, 62, Астана, Казахстан,

автор-корреспондент.

Аннотация. *Использование блокчейна и искусственного интеллекта для усовершенствования методов цифровой идентификации отвечает на вызовы обеспечения безопасности и надежности личных данных в эру цифровизации. Традиционные методы проверки становятся все более неадекватными, о чем свидетельствует тревожная эскалация случаев мошенничества с личными данными. В ответ на это исследование исследуется инновационная интеграция технологии блокчейна и искусственного интеллекта для повышения безопасности, эффективности и конфиденциальности процессов проверки цифровой личности. Децентрализованный и неизменяемый реестр блокчейна предлагает новую парадигму для безопасных и управляемых цифровых удостоверений, а возможности искусственного интеллекта в автоматизации сложных процессов и обнаружении мошенничества посредством анализа шаблонов обеспечивают дополнительное синергетическое решение. В этом исследовании рассматриваются проблемы традиционных систем проверки, подчеркивается потенциал интеграции блокчейна и искусственного интеллекта, а также представлена методология создания информационной системы проверки личности. Результаты были проверены с помощью серии тестов, демонстрирующих значительное улучшение точности, скорости и устойчивости к мошенническим действиям. Несмотря на*

многообещающие результаты, были выявлены такие проблемы, как масштабируемость, конфиденциальность и сложность интеграции, и предложенные решения направлены на решение этих проблем для практической реализации и долгосрочного успеха интегрированных систем цифровой проверки личности.

Ключевые слова: *блокчейн, искусственный интеллект, проверка цифровой личности, кибербезопасность, конфиденциальность, масштабируемость, обнаружение мошенничества.*

REFERENCES

1. Killer, C., Rodrigues, B., Scheid, E.J., Franco, M., Eck, M., Zaugg, N., ... & Stiller, B. (2020, November). Provotum: A blockchain-based and end-to-end verifiable remote electronic voting system // In 2020 IEEE 45th Conference on Local Computer Networks (LCN). – 2020. – Pp. 172-183. IEEE. https://doi.org/10.1109/LCN48667.2020.9314815
2. Stančíková, I., & Homoliak, I. (2023, March). Sbvote: Scalable self-tallying blockchain-based voting // In Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing. – 2023. – Pp. 203-211. https://doi.org/10.1145/3555776.3578603
3. Li, W., Su, Z., Li, R., Zhang, K., & Wang, Y. (2020). Blockchain-based data security for artificial intelligence applications in 6G networks // IEEE Network. – 2020. – No. 34 (6). – Pp. 31-37. https://doi.org/10.1109/MNET.021.1900629
4. Dhar Dwivedi, A., Singh, R., Kaushik, K., Rao Mukkamala, R., & Alnumay, W.S. (2021). Blockchain and artificial intelligence for 5G-enabled Internet of Things: Challenges, opportunities, and solutions // Transactions on Emerging Telecommunications Technologies. – 2021. – e4329. https://doi.org/10.1002/ett.4329
5. Venugopalan, S., Stančíková, I., & Homoliak, I. (2023). Always on voting: A framework for repetitive voting on the blockchain // IEEE Transactions on Emerging Topics in Computing. – 2023. https://doi.org/10.1109/TETC.2023.3315748
6. Hussain, A.A., & Al-Turjman, F. (2021). Artificial intelligence and blockchain: A review // Transactions on Emerging Telecommunications Technologies. – 2021. – No. 32 (9). – e4268. https://doi.org/10.1002/ett.4266
7. Agate, V., De Paola, A., Ferraro, P., Re, G.L., & Morana, M. (2021). SecureBallot: A secure open-source e-Voting system // Journal of Network and Computer Applications. – 2021. – No. 191. – Pp. 103165. https://doi.org/10.1016/j.jnca.2021.103165
8. Widayanti, R., Aini, Q., Haryani, H., Lutfiani, N., & Apriliasari, D. (2021, September). Decentralized electronic vote based on blockchain p2p // In 2021 9th International Conference on Cyber and IT Service Management (CITSM). – 2021. – Pp. 1-7. IEEE. https://doi.org/10.1109/CITSM52892.2021.9588851
9. Jumagalieva, A., Abdykerimova, E., Turkmenbayev, A., Muratova, G., Amangul, T., & Shekerbek, A. (2024). Analysis of research on the implementation of Blockchain technologies in regional electoral processes // International Journal of Electrical and Computer Engineering (IJECE). – 2024. – No. 14 (3). – Pp. 2854-2867. https://doi.org/10.11591/ijece.v14i3.pp2854-2867