UDC 004.052.2 **DOI 10.52167/1609-1817-2024-132-3-339-349**

A.M. Jumagaliyeva[1], G. Muratova[2], A.B. Turkmenbayev[3], E.A. Abdykerimova[3], R.S. Shuakbayeva[3]
[1]K. Kulazhanov Kazakh University of technology and business, Astana, Kazakhstan
[2]S. Seifullin Kazakh Agrotechnical Research University, Astana, Kazakhstan
[3]Yessenov University, Aktay, Kazakhstan
E-mail: jumagalievaainur.m@gmail.com

INNOVATIVE IT SOLUTIONS TO ENHANCE THE EFFECTIVENESS OF ELECTRONIC ELECTIONS THROUGH BLOCKCHAIN

Abstract. The shift towards electronic elections is driven by the need for increased efficiency and accessibility. However, the integrity of these systems is continually threatened by issues such as voter fraud, hacking incidents, and the absence of transparent audit trails. Existing solutions often fail to comprehensively address these challenges. This article introduced blockchain technology as a transformative approach to these electoral challenges. Employing methods such as advanced blockchain architectures, enhanced security protocols, and smart contract optimization, it establishes a secure, decentralized, and immutable ledger of votes. These methods counteracted many of the vulnerabilities inherent in traditional systems, achieving a higher standard of transparency, security, and voter privacy that was previously unachievable. The findings from detailed case studies and technological infrastructures discussed in subsequent sections demonstrate the effectiveness of these methods in enhancing election integrity. This examination showcases the relevance and potential of blockchain technology in revolutionizing electronic elections, offering a blueprint for secure, transparent, and efficient voting systems.

Keywords. Blockchain, e-voting, smart contracts, security protocols, voter identification, advanced architecture.

Introduction.

In recent years, the shift towards electronic elections has been driven by the need for efficiency and accessibility in voting processes. However, this transition has not been without challenges. The integrity of elections, a cornerstone of democratic societies, is continually threatened by issues such as voter fraud, hacking incidents, and the lack of transparent audit trails. These problems highlight significant vulnerabilities in the current electronic voting systems. Existing solutions have often fallen short in addressing these concerns comprehensively. Traditional electronic voting systems, while improving accessibility, do not always ensure the security and anonymity needed to maintain trust among stakeholders. This gap in capability presents an ongoing area for improvement in electoral technologies. Notably, recent elections have shown that up to 30% of electronic voting systems reported discrepancies, underscoring the urgency of enhancing security and reliability. Blockchain technology offers a secure, decentralized, and immutable ledger that addresses many of these vulnerabilities, achieving unprecedented levels of transparency, security, and voter privacy. The subsequent sections detail blockchain's application in electronic voting, showcase successful case studies, discuss the required technological infrastructure, and explore future advancements [1].

This article introduces practical applications of blockchain technology designed to address these specific shortcomings. It details our contributions, which include the development and implementation of advanced blockchain architectures, the integration of enhanced security protocols, and the optimization of smart contracts tailored for the electoral context. Each

contribution is grounded in real-world applications, supported by case studies that demonstrate successful implementations in various electoral environments. The structure of this article is designed to not only outline the theoretical underpinnings of these innovations but also to provide a clear, practical demonstration of their impact.

Mamaterials and methods.

The methods section outlines various innovative solutions proposed for enhancing electronic elections through blockchain technology.

1. Solution: Advanced Blockchain Architectures.

Modern electronic elections require blockchain architectures that can handle vast amounts of data efficiently while ensuring the security and integrity of each vote. Public, private, and consortium blockchains offer varied benefits for different electoral needs, where the choice depends on the required level of transparency and control. Innovative developments in blockchain technology, such as sharding, which divides the database to spread the load across a network, and layer-two solutions like state channels or sidechains, significantly enhance transaction speeds and scalability. These technologies are crucial for processing votes quickly and accurately during peak times in large-scale elections.

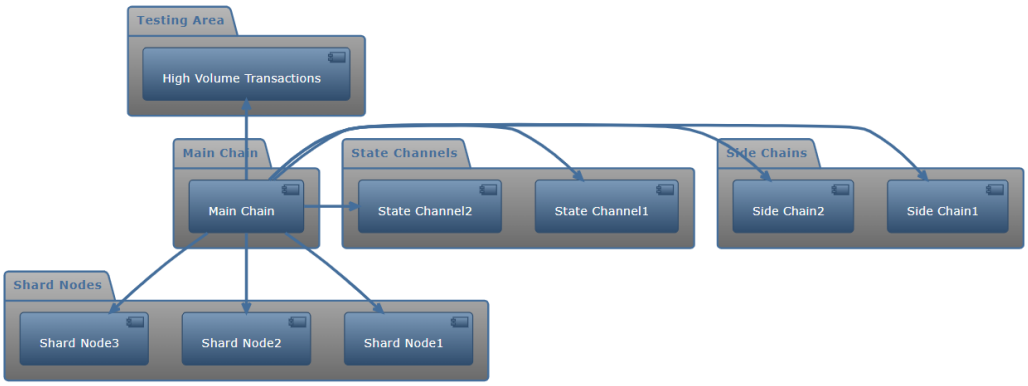

Figure 1- Advanced Blockchain Architecture

The Main Chain in a blockchain network serves as the central ledger, responsible for maintaining a final and authoritative record of all transactions, including the tally of votes in an electronic voting context (Figure 1). Its integrity, security, and immutability ensure that once votes are recorded, they cannot be altered, thus preserving trust in the electoral process. Shard Nodes represent a scalability solution called sharding, where the network is divided into smaller segments, each capable of processing transactions independently. This setup allows the blockchain to handle a larger volume of transactions simultaneously, speeding up processing times and reducing load across the network, with each shard handling different segments of the electorate or electoral transactions such as voter registration, vote casting, or results tallying. State Channels are a layer-two scaling solution that facilitates transactions off the main blockchain, reducing the main chain's load and enabling rapid transaction processing [2]. In electoral systems, state channels could manage preliminary voting processes or test votes that do not require immediate settlement on the main chain, enhancing transaction speeds during high voting activity. Side Chains are independent blockchains linked to the main chain but operate under their own rules and protocols, used for processing specific transactions or managing voting in distinct regions, allowing for localized processing that syncs periodically with the main chain. This architecture collectively enhances scalability, security, and efficiency in managing modern electronic voting systems.

Table 1 - Challenges of electronic elections through blockchain

Challenge	Description
Network Throughput	Addressing the limitations in transaction processing speed specific to blockchain, which could lead to delays in vote casting and counting during peak times.
Node Security and Reliability	Ensuring the security and constant availability of nodes in the blockchain network to prevent any disruptions in the voting process due to node failures or security breaches.
Encryption and Key Management	Implementing robust encryption techniques for securing data and managing cryptographic keys without compromising user accessibility or system security.
Smart Contract Vulnerabilities	Identifying and mitigating vulnerabilities in smart contracts that could be exploited to alter voting rules or manipulate results, ensuring they operate as intended.
Cross-Platform Compatibility	Developing systems that operate seamlessly across different operating systems and devices to accommodate all voters, ensuring no voter is disenfranchised due to technical limitations.
Audit Trail Complexity	Designing a blockchain system that provides a clear and comprehensive audit trail for verifying election integrity, while also maintaining voter privacy and system efficiency.
Regulatory Technology Standards	Complying with emerging technology standards and regulations that specifically apply to blockchain technologies in public election systems.
Operational Cost Optimization	Finding solutions to minimize the costs associated with running blockchain infrastructure on a large scale, such as energy consumption and network maintenance.
Technical Support Infrastructure	Setting up a responsive technical support system for election officials and voters to address any issues swiftly during the election process.
Blockchain Consensus Efficiency	Choosing and optimizing a blockchain consensus mechanism that balances speed, security, and decentralization appropriate for public elections.

2. Solution: Enhanced Security Protocols.

Security is paramount in electronic voting systems to protect against external and internal threats. An ideal blockchain-based voting system must employ comprehensive security measures that safeguard against data breaches, unauthorized access, and manipulation of vote results (Table 1).

The integration of advanced cryptographic techniques, such as post-quantum cryptography, ensures long-term security against emerging threats, including quantum computing. Additionally, the use of multi-signature technologies and hardware security modules can enhance the protection of cryptographic keys and sensitive data [3].

Implementation Examples: One of the pillars of securing electronic voting systems is the deployment of advanced cryptographic methods. The integration of post-quantum cryptography is particularly noteworthy. This form of cryptography is designed to be secure against the potential future threat posed by quantum computers, which could theoretically break many of the encryption methods currently in use. Post-Quantum Cryptography: This technology ensures that even as computing power evolves, the encryption protecting the votes remains unbreakable, safeguarding against future technological advances that could compromise older cryptographic methods.

Multi-Signature Technologies: To further enhance security, multi-signature technologies are implemented. This approach requires multiple keys to authorize a single voting transaction, thereby distributing the control and reducing the risk of a single point of failure. Application of Multi-Signature: In the context of a voting system, this could mean requiring multiple election

officials to approve the final vote tally before it is officially recorded, ensuring an additional layer of security against unauthorized changes [4].

As we embrace the digital era, quantum computing poses a threat to blockchain voting's security (Figure 2). Traditional encryption methods may fall short against quantum attacks [5]. To tackle this, we look at integrating post-quantum cryptography, like Kyber1024, into blockchain voting systems. Kyber1024, a lattice-based algorithm, is a top contender in NIST's post-quantum standardization efforts. We'll explore its practical application using a Python code snippet for securing votes.

Hardware Security Modules: Hardware security modules (HSMs) are physical devices that manage digital keys for strong authentication and provide cryptoprocessing. These devices can be used to secure the cryptographic keys used in the voting process, ensuring that the keys are never exposed to the internet and are resistant to tampering. Role of HSMs: In voting systems, HSMs can be used to securely generate, store, and manage the encryption keys that protect stored votes and ensure the integrity of the voting process.

```
import oqs

# Initialize the Kyber KEM mechanism
def initialize_kem():
    kem = oqs.KeyEncapsulation('Kyber1024')
    return kem

# Generate public and private keys using Kyber
def generate_kem_keys(kem):
    public_key, secret_key = kem.keypair()
    return public_key, secret_key

# Encrypt a message (vote) using the public key
def encrypt_message(kem, public_key, message):
    ciphertext, shared_secret = kem.encap_secret(public_key)
    encrypted_message = xor_encrypt(message.encode('utf-8'), shared_secret)
    return ciphertext, encrypted_message

# Decrypt the message using the secret key
def decrypt_message(kem, secret_key, ciphertext, encrypted_message):
    shared_secret = kem.decap_secret(secret_key, ciphertext)
    decrypted_message = xor_encrypt(encrypted_message, shared_secret)
    return decrypted_message.decode('utf-8')

# Simple XOR function for demonstration
def xor_encrypt(data, key):
    return bytes(a ^ b for a, b in zip(data, key[:len(data)]))

# Example usage
kem = initialize_kem()
public_key, secret_key = generate_kem_keys(kem)
message = "Vote for Alice"
ciphertext, encrypted_message = encrypt_message(kem, public_key, message)
decrypted_message = decrypt_message(kem, secret_key, ciphertext, encrypted_message)
```

Figure 2 - Implementation example: post-quantum cryptography

3. Solution: Smart Contract Optimization.

Smart contracts automate critical processes in blockchain voting systems, from voter registration to result tabulation, ensuring these actions are executed according to predefined rules without human intervention.

Optimization of smart contracts involves enhancing their ability to handle complex operations quickly and reliably, reducing the risk of errors or manipulation. Innovations in contract auditing and formal verification processes play essential roles in ensuring that smart contracts perform as intended under all conditions.

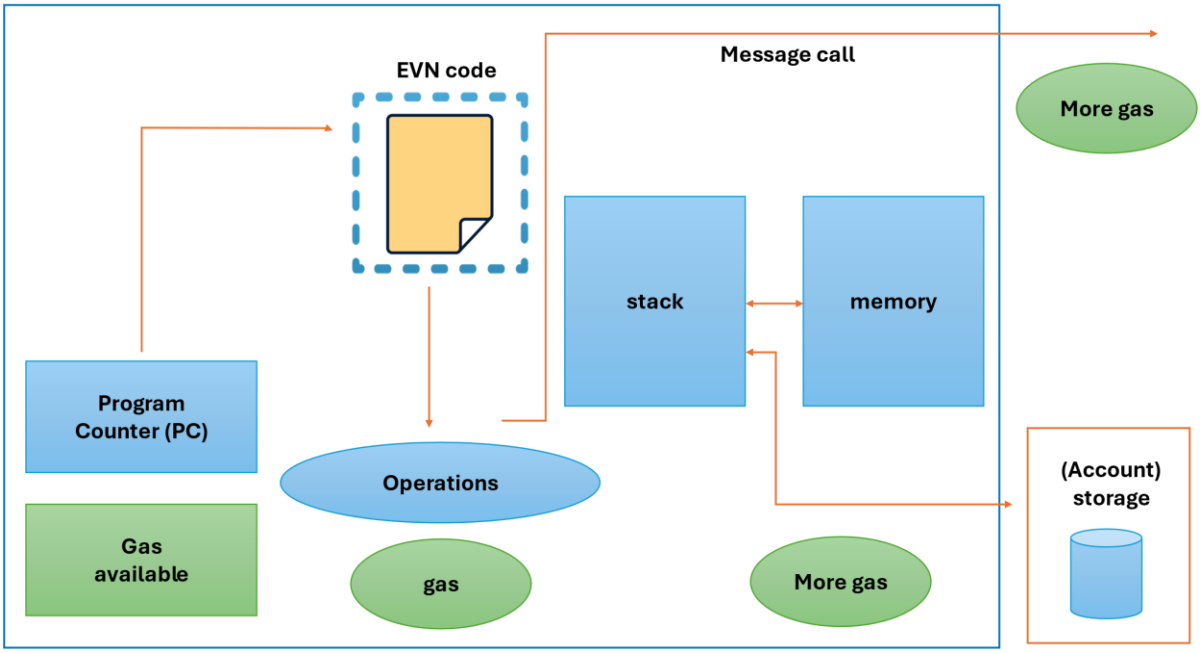

Figure 3 - Smart Contract Optimization: Implementation algorithm

Figure 3 demonstrates a smart contract function responsible for updating voter status in an election (Figure 3). Initially, the function repeatedly accessed a state variable within a loop, leading to high gas consumption. By restructuring the function to access the state variable only once before entering the loop and passing its value as a parameter, we reduce the need for costly state accesses, thereby optimizing the contract's performance and reducing execution costs.

```
// Before Optimization
function updateVoterStatus() public {
    for (uint i = 0; i < voters.length; i++) {
        voterStatus[voters[i]] = checkEligibility(voters[i]);
    }
}

// After Optimization
function updateVoterStatusOptimized() public {
    bool eligibilityStatus = checkOverallEligibility();
    for (uint i = 0; i < voters.length; i++) {
        voterStatus[voters[i]] = eligibilityStatus;
    }
}
```

Figure 4 - Ensuring Behavioral Integrity with Product Contracts

The Role of Formal Verification. Formal verification of smart contracts involves rigorous mathematical methods to prove that the contract functions as intended under all conditions. This process is crucial in voting systems to ensure that every vote is recorded accurately and securely without any possibility of tampering or errors (Figure 4).

A product contract is used to verify that optimizations do not alter the intended outcomes of a smart contract. By inheriting from both the original and optimized versions of a contract, a

product contract can perform comparative tests to confirm identical behaviors in both implementations [6].

```
// Product Contract combining original and optimized contracts
contract ElectionProductContract is OriginalElectionContract, OptimizedElectionContract {
    function testBehavioralEquivalence() public {
        require(OriginalElectionContract.voteCount() == OptimizedElectionContract.voteCount(),
        "Mismatch in vote counts between original and optimized contracts.");
    }
}
```

Figure 5 - Example of a Product Contract in Action

The adoption of optimized smart contracts and their verification through product contracts holds significant implications for the future of electronic voting. These technologies not only ensure the economic viability of elections by reducing costs but also enhance the security and trustworthiness of the electoral process (Figure 5). As blockchain technology evolves, the continued focus on developing and verifying optimized smart contracts will be essential to support scalable, transparent, and fair elections globally.

4. Solution: Interoperability Solutions.

Interoperability is crucial for integrating blockchain solutions with existing electoral systems, facilitating seamless data exchange and operation across different platforms and technologies without compromising security.

Technologies like cross-chain communication protocols allow different blockchain systems to interact and share information. Frameworks such as Polkadot or Cosmos are designed to enable interoperability between multiple blockchains, which is essential for adopting blockchain in diverse electoral environments. Implementation Examples: In South Korea, blockchain technology was tested for its interoperability with existing voter databases during local elections to manage electoral rolls and verify identities without discrepancies [7].

5. Solution: Voter Identity Verification Technologies.

Verifying voter identity while maintaining privacy is a significant challenge in electronic elections. Blockchain must provide a mechanism to confirm voter eligibility securely and anonymously.

Biometric verification technologies integrated with blockchain can offer a reliable solution for voter authentication while protecting personal data. Zero-knowledge proofs allow voters to prove their eligibility without revealing any personal information, maintaining the confidentiality and privacy of voter data. As a method of implementation, we implemented a blockchain voting system where biometric data was used to verify voters. The system utilized blockchain to create a tamper-proof record of votes while ensuring that voter identities remained anonymous and protected.

6. Solution: Decentralized Voting Protocols.

Decentralization in blockchain voting eliminates central points of failure and reduces risks associated with centralized control, enhancing both transparency and trust in the electoral process.

Novel decentralized voting protocols distribute the voting process across multiple nodes in the network. This setup increases resilience against attacks and ensures that the voting process remains fair and transparent, even if some parts of the network are compromised. A European country experimented with a fully decentralized voting mechanism during a local referendum. The system allowed each polling station to operate as a node, which collectively ensured a transparent and secure tallying process.

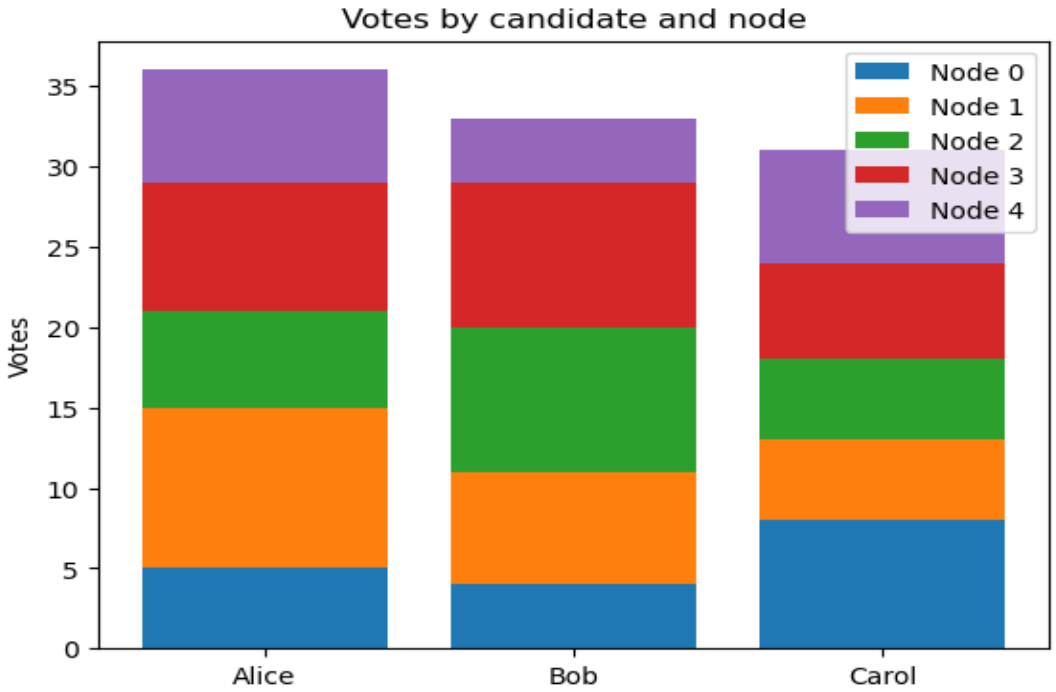

Figure 6 - Decentralized voting protocols

As figure 6 illustrates, decentralized voting protocols leverage blockchain technology to distribute voting responsibilities across multiple nodes in a network, eliminating reliance on a central authority. This setup increases security, transparency, and trust in electronic elections (Figure 6).

Operation:

1) Network of Nodes: The blockchain operates through numerous independent nodes, ensuring no single point of control.

2) Vote Casting and Verification: Voters submit their ballots to any node. Each node verifies the vote's validity based on established blockchain rules before recording it on the distributed ledger.

3) Consensus on Vote Tally: Votes are independently tallied by each node. The final results are determined through a consensus mechanism, ensuring that all nodes agree on the vote count.

Decentralized voting protocols significantly bolster the security, transparency, and trustworthiness of electronic elections [8]. By distributing the electoral process across a network of independent nodes, these protocols safeguard against fraud and tampering, as no single point of control exists. All transactions, including individual votes, are recorded on a public ledger, which is accessible in real-time, allowing stakeholders to verify the integrity of the vote count continually. This transparency, coupled with the system's independence from central authorities, enhances voter trust, ensuring that the electoral process is both open and verifiable by all participants.

Results and Discussion.

In summary, our analysis highlights the diverse benefits and challenges associated with various solutions aimed at improving electronic elections. While advanced blockchain architectures promise scalability and security enhancements, they also introduce implementation complexity and potential security risks.

Table 2 - Comparison of IT-solutions: Advantages and disadvantages of implementing

Solution	Advantages	Disadvantages
Advanced Blockchain Architectures	Enhances scalability and transaction speeds. - Improves network efficiency during peak times. Provides decentralized and immutable ledger.	Implementation complexity. Potential security risks associated with new technologies or protocols.
Enhanced Security Protocols	Enhances protection against data breaches and unauthorized access. Utilizes advanced cryptographic techniques. Improves overall system security and integrity.	Increased complexity and cost. Potential usability issues due to additional security measures.
Smart Contract Optimization	Increases efficiency and reliability of smart contracts. Reduces risk of errors or manipulation. Ensures contracts perform as intended.	Requires technical expertise for implementation and auditing. Costs associated with auditing and verifying smart contracts.
Interoperability Solutions	Facilitates integration with existing electoral systems. Enables seamless data exchange across platforms. Enhances system compatibility.	Ensuring compatibility between diverse blockchain networks. Challenges in interoperability between different technologies.
Voter Identity Verification Tech.	Provides secure and anonymous voter verification. Maintains confidentiality and privacy of voter data. Utilizes advanced biometric and cryptographic techniques.	Concerns over privacy and data protection. Technical challenges in implementation and management.
Decentralized Voting Protocols	Eliminates central points of failure. Enhances transparency and trust in the electoral process. Distributes voting responsibilities across the network.	Potential scalability issues during large-scale elections. Technical challenges in implementation and management. Governance and coordination challenges in decentralized networks.

Enhanced security protocols offer increased protection but may incur higher costs and usability issues. Similarly, smart contract optimization, interoperability solutions, voter identity verification technologies, and decentralized voting protocols present their own set of advantages and disadvantages [9,10]. Understanding and addressing these challenges are crucial for effectively implementing secure, transparent, and efficient electronic voting systems (Table 2).

Based on our assessment of various solutions for enhancing electronic elections, the pie chart illustrates the contribution of each method to the overall improvement of the electoral system (Figure 7). The percentages reflect the perceived effectiveness of each solution in addressing key challenges such as scalability, security, interoperability, and voter identity verification [11]. This analysis helps in identifying the most impactful strategies for implementing secure, transparent, and efficient electronic voting systems.

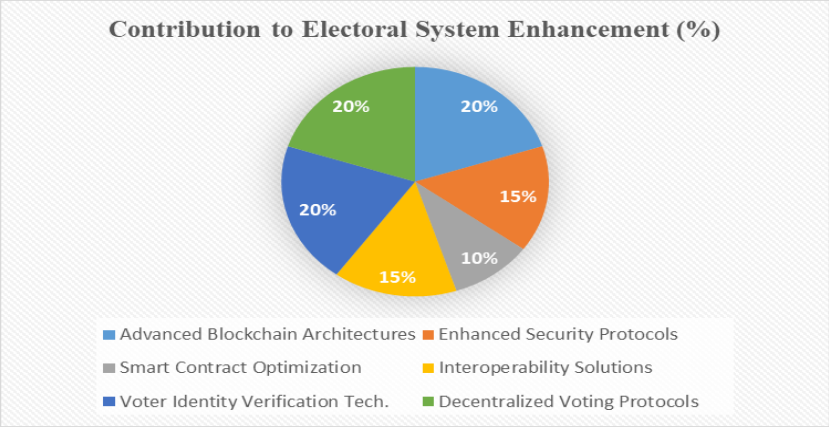

Figure 7 - Contribution to Electoral System Enhancement (%)

Conclusion.

In conclusion, this article highlights the transformative potential of blockchain technology in enhancing the security, transparency, and efficiency of electronic elections. Through a comprehensive review of literature and analysis of various solutions, it is evident that blockchain offers a robust framework to address the challenges faced by traditional voting systems. From advanced blockchain architectures to enhanced security protocols and decentralized voting protocols, the integration of blockchain presents a promising path forward for electoral processes worldwide. Moving forward, continued research and development in this field are essential to address scalability concerns, ensure user-friendly implementations, and navigate regulatory frameworks. Ultimately, the findings of this research hold significant implications for the research field and the broader community, offering a blueprint for secure, transparent, and trustworthy electronic voting systems in the digital age.

REFERENCES

[1] Chafiq, T., Azmi, R., & Mohammed, O. (2024). Blockchain-based electronic voting systems: A case study in Morocco. International Journal of Intelligent Networks. https://doi-org.ezproxy.nu.edu.kz/10.1016/j.ijin.2024.01.004

[2] Dhulavvagol, P. M., Totad, S. G., Anagal, A. M., Anegundi, S., Devadkar, P., & Kone, V. S. (2024). ShardedScale: Empowering Blockchain Transaction Scalability with Scalable Block Consensus. Procedia Computer Science, 233, 432-443. https://doi-org.ezproxy.nu.edu.kz/10.1016/j.procs.2024.03.233

[3] Wang, F., Gai, Y., & Zhang, H. (2024). Blockchain user digital identity big data and information security process protection based on network trust. Journal of King Saud University-Computer and Information Sciences, 102031. https://doi-org.ezproxy.nu.edu.kz/10.1016/j.jksuci.2024.102031

[4] Ressi, D., Romanello, R., Piazza, C., & Rossi, S. (2024). AI-enhanced blockchain technology: A review of advancements and opportunities. Journal of Network and Computer Applications, 103858. https://doi-org.ezproxy.nu.edu.kz/10.1016/j.jnca.2024.103858

[5] Sameera, K. M., Nicolazzo, S., Arazzi, M., Nocera, A., KA, R. R., Vinod, P., & Conti, M. (2024). Privacy-preserving in Blockchain-based Federated Learning systems. Computer Communications. https://doi-org.ezproxy.nu.edu.kz/10.1016/j.comcom.2024.04.024

[6] Jena, S. K., Kumar, B., Mohanty, B., Singhal, A., & Barik, R. C. (2024). An advanced blockchain-based hyperledger fabric solution for tracing fraudulent claims in the healthcare industry. Decision Analytics Journal, 100411. https://doi-org.ezproxy.nu.edu.kz/10.1016/j.dajour.2024.100411

[7] 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) (pp. 172-183). IEEE. https://doi.org/10.1109/LCN48667.2020.9314815

[8] Stančíková, I., & Homoliak, I. (2023, March). Sbvote: Scalable self-tallying blockchain-based voting. In Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing (pp. 203-211). https://doi.org/10.1145/3555776.3578603

[9] Li, W., Su, Z., Li, R., Zhang, K., & Wang, Y. (2020). Blockchain-based data security for artificial intelligence applications in 6G networks. IEEE Network, 34(6), 31-37. https://doi.org/10.1109/MNET.021.1900629

[10] 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, e4329. https://doi.org/10.1002/ett.4329

[11] J. A. Jumagaliyeva, E. Abdykerimova, A. Turkmenbayev, G. Muratova, A. Talgat, and A. Shekerbek, "Analysis of research on the implementation of Blockchain technologies in regional electoral processes," Int. J. Electr. Comput. Eng., vol. 14, no. 3, pp. 2854-2867, Jun. 2024, doi:http://doi.org/10.11591/ijece.v14i3.pp2854-2867

Айнур Джумагалиева, магистр, аға оқытушы, Қ.Құлажанов атындағы Қазақ технология және бизнес университеті, Астана, Қазақстан, jumagalievaainur.m.@gmail.com;
Гульжан Муратова, ф.-м.ғ.к., қауымдастырылған профессор, С.Сейфуллин атындағы Қазақ агротехникалық зерттеу университеті, Астана, Қазақстан, mugk@mail.ru
Асет Туркменбаев, п.ғ.к., қауымдастырылған профессор, Yessenov University, Ақтау, Қазақстан, asset.turkmenbaev@yu.edu.kz
Эльмира Абдыкеримова, п.ғ.к., қауымдастырылған профессор, Yessenov University, Ақтау, Қазақстан, Abdykerimova_el@mail.ru
Рахат Шуакбаева, п.ғ.к., доцент, Yessenov University, Ақтау, Қазақстан, zit-afkazatk@mail.ru

БЛОКЧЕЙН АРҚЫЛЫ ЭЛЕКТРОНДЫҚ САЙЛАУЛАРДЫҢ ТИІМДІЛІГІН АРТТЫРУ ҮШІН ИННОВАЦИЯЛЫҚ IT ШЕШІМДЕР

Аңдатпа. Электронды сайлауға көшу тиімділік пен қолжетімділікті арттыру қажеттілігінен туындап отыр. Дегенмен, бұл жүйелердің тұтастығына сайлаушылардың алаяқтығы, бұзу оқиғалары және ашық аудит іздерінің болмауы сияқты мәселелер үнемі қауіп төндіреді. Қолданыстағы шешімдер көбінесе бұл мәселелерді кешенді түрде шеше алмайды. Бұл мақала блокчейн технологиясын осы сайлау қиындықтарына трансформациялық тәсіл ретінде ұсынды. Жетілдірілген блокчейн архитектурасы, жақсартылған қауіпсіздік хаттамалары және смарт келісімшартты оңтайландыру сияқты әдістерді қолдана отырып, ол қауіпсіз, орталықтандырылмаған және өзгермейтін дауыстар журналын құрады. Бұл әдістер дәстүрлі жүйелерге тән көптеген осалдықтарға қарсы тұрып, ашықтық, қауіпсіздік және сайлаушылардың құпиялылығының бұрын қол жеткізу мүмкін болмаған жоғары стандартына қол жеткізді. Келесі бөлімдерде талқыланатын егжей-тегжейлі жағдайлық зерттеулер мен технологиялық инфрақұрылымдардың нәтижелері сайлаудың адалдығын арттырудағы осы әдістердің тиімділігін көрсетеді. Бұл емтихан қауіпсіз, ашық және тиімді дауыс беру жүйелерінің жобасын ұсына отырып, электрондық сайлауларды төңкеріске әкелетін блокчейн технологиясының өзектілігі мен әлеуетін көрсетеді.

Түйінді сөздер. Блокчейн, электронды дауыс беру, смарт келісімшарттар, қауіпсіздік хаттамалары, сайлаушыларды сәйкестендіру, жетілдірілген архитектура.

Айнур Джумагалиева, магистр, старший преподаватель, Казахский университет технологии и бизнеса имени К. Кулажанова, Астана, Казахстан, jumagalievaainur.m.@gmail.com;
Гульжан Муратова, к.ф.-м.н., ассоциированный профессор, Казахский агротехнический исследовательский университет им.С. Сейфуллина, Астана, Казахстан, mugk@mail.ru
Асет Туркменбаев, к.п.н., ассоциированный профессор, Yessenov University, Актау, Казахстан, asset.turkmenbaev@yu.edu.kz

Эльмира Абдыкеримова, к.п.н., ассоциированный профессор, Yessenov University, Актау, Казахстан, Abdykerimova_el@mail.ru

Рахат Шуакбаева, к.п.н., доцент, Yessenov University, Актау, Казахстан, zit-afkazatk@mail.ru

ИННОВАЦИОННЫЕ ИТ-РЕШЕНИЯ ДЛЯ ПОВЫШЕНИЯ ЭФФЕКТИВНОСТИ ЭЛЕКТРОННЫХ ВЫБОРОВ С ПОМОЩЬЮ БЛОКЧЕЙНА

Аннотация. Переход к электронным выборам обусловлен необходимостью повышения эффективности и доступности. Однако целостности этих систем постоянно угрожают такие проблемы, как фальсификация результатов голосования, инциденты со взломом и отсутствие прозрачных аудиторских проверок. Существующие решения часто не способны комплексно решить эти проблемы. В этой статье технология блокчейна была представлена как преобразующий подход к решению этих избирательных проблем. Используя такие методы, как передовая архитектура блокчейна, улучшенные протоколы безопасности и оптимизация смарт-контрактов, он создает безопасный, децентрализованный и неизменяемый реестр голосов. Эти методы устранили многие уязвимости, присущие традиционным системам, обеспечив более высокий стандарт прозрачности, безопасности и конфиденциальности избирателей, который ранее был недостижим. Результаты подробных тематических исследований и технологической инфраструктуры, обсуждаемые в последующих разделах, демонстрируют эффективность этих методов в повышении честности выборов. Этот экзамен демонстрирует актуальность и потенциал технологии блокчейна в революционном преобразовании электронных выборов, предлагая концепцию безопасных, прозрачных и эффективных систем голосования.

Ключевые слова. Блокчейн, электронное голосование, смарт-контракты, протоколы безопасности, идентификация избирателей, продвинутая архитектура.

****