https://doi.org/10.53360/2788-7995-2025-3(19)-10

IRSTI: 20.51.23

G. Shuitenov[1], A. Turginbayeva[2], S. Altynbek[*], M. Muratbekov[2], Zh. Yessenzholov[1]
[1]Esil University,
010008, Kazakhstan, Astana, 7 Zhubanova Street
[2]L.N. Gumilyov Eurasian National University,
010008, Kazakhstan, Astana, 11 Pushkin Street
*e-mail: Serik_aa@bk.ru

BLOCKCHAIN-ENABLED VOTE VALIDATION THROUGH A CRYPTOGRAPHIC AND SYSTEM-LEVEL APPROACH TO SECURE ELECTIONS

Abstract: *This paper presents a secure, transparent, and tamper-resistant web-based voting application. Designed specifically for university-level elections, the system leverages a private blockchain network to ensure the integrity and immutability of each vote. Built using a modern technology stack – TypeScript and React on the frontend, Axios for communication, and a Fastify-based Node.js backend with a MySQL database - the platform prioritizes both usability and security.*

The voting process is authenticated and validated through cryptographic hashing and blockchain consensus, preventing unauthorized alterations or vote duplication. Each vote is recorded as a transaction on a private blockchain, where nodes verify its legitimacy before it becomes part of the permanent ledger. This system-level integration of blockchain offers auditability, transparency, and trust, eliminating the need for manual verification and reducing the risk of election fraud.

The solution is tailored for institutional adoption, ensuring that only authenticated university users can participate. Through this approach, the project demonstrates how blockchain technologies can be practically applied to enhance the credibility and efficiency of digital democratic processes.

Key words: *Blockchain, Vote Validation, Secure Elections, Cryptographic Hashing, Private Blockchain, Web-Based Voting, Fastify, React, Node.js, MySQL.*

Introduction

Ensuring the integrity and transparency of elections is a critical challenge in the digital age, particularly within academic institutions where trust and participation are essential. This paper introduces a blockchain-enabled web voting system developed for Esil University to facilitate secure and verifiable student and faculty elections. Traditional digital voting platforms often face concerns related to data manipulation, unauthorized access, and lack of transparency. To address these issues, this project integrates blockchain technology to validate votes through a cryptographic and system-level approach.

The application is built using a modern and scalable technology stack. The frontend is developed with TypeScript and React for type-safe, component-based user interfaces, while Axios ensures efficient client-server communication. The backend is powered by Fastify, a high-performance Node.js framework, and MySQL is used for reliable and structured data storage. This stack was chosen for its speed, maintainability, and compatibility with enterprise-level deployment, aligning with the needs of Esil University's infrastructure.

By leveraging a private blockchain, this system provides an auditable and tamper-proof voting environment tailored for institutional use.

Literary review

The evolution of electronic voting (e-voting) systems has significantly transformed how elections are conducted in both governmental and institutional settings. In academic institutions, particularly universities, digital voting offers an appealing alternative to paper ballots due to its efficiency, accessibility, and ease of result aggregation. However, many traditional e-voting platforms rely heavily on centralized server-based architectures, which introduce significant risks in terms of data manipulation, system compromise, and limited transparency. These centralized systems are often controlled by a single administrative entity, making them susceptible to insider threats or unintentional data leaks. In the absence of an external auditing mechanism or verifiable transaction trail, it becomes extremely difficult to assure stakeholders that the results are accurate and free from tampering. Several case studies involving university elections have shown how such platforms can

be misused or manipulated without leaving detectable traces. Therefore, while digital voting offers convenience, it must also evolve to meet the security expectations required for trustworthy elections.

To address these concerns, blockchain technology has emerged as a robust solution offering decentralization, immutability, and traceability - properties that make it especially attractive for voting systems. Blockchain operates as a distributed ledger where transactions (in this case, votes) are recorded across multiple nodes and can only be appended but never altered or deleted. Several projects and research efforts have explored blockchain's role in secure voting, including Voatz (used in pilot programs for absentee military voting in the U.S.), FollowMyVote, and academic prototypes designed for small communities. These systems demonstrate how blockchain can enable transparent vote recording and result verification, while ensuring that no single entity has the ability to alter votes post-submission. As noted by Hardwick et al. (2018), blockchain's trustless nature allows participants to verify vote integrity independently, significantly reducing the need for human auditing. Nonetheless, public blockchain solutions often present challenges such as high computational overhead, lack of scalability, and complex deployment requirements. Moreover, public networks may introduce privacy concerns, which is why private or permissioned blockchain systems are often considered more suitable for institutional environments like universities.

Complementary to blockchain, cryptographic techniques are foundational to any secure digital voting system. These include cryptographic hash functions that ensure data integrity, digital signatures that validate the authenticity of vote submissions, and public-key encryption mechanisms that protect user identities and ballot content. Advanced cryptographic protocols like homomorphic encryption and zero-knowledge proofs have also been explored in academic literature for their ability to allow vote tallying without revealing individual vote choices. For example, Chaumian voting systems utilize blind signatures to maintain vote confidentiality while still allowing verification of vote legitimacy. These cryptographic methods prevent common attacks such as vote tampering, impersonation, or replay attacks during data transmission. However, implementing such cryptographic protocols can introduce usability and performance trade-offs, especially when not paired with optimized system architecture. In real-world academic applications, simplicity and speed are often critical, so the challenge lies in finding the right balance between strong encryption and operational practicality.

Beyond the cryptographic level, system-level security measures are essential for ensuring the holistic safety of any digital voting platform. This includes enforcing role-based access control (RBAC) to distinguish between voters, administrators, and system validators; implementing secure APIs to prevent unauthorized data access; and applying rigorous database protection techniques such as audit logging, SQL injection prevention, and transactional integrity. Even a blockchain-backed system can become vulnerable if frontend security flaws, server misconfigurations, or unprotected endpoints are exploited by malicious users. Research into full-stack security practices has emphasized that true end-to-end protection must include not just cryptographic operations but also architectural hardening, routine vulnerability assessments, and secure development lifecycles (SDLC). For example, improperly configured API routes or a lack of HTTPS encryption could expose user authentication tokens, leading to compromised voting sessions. Thus, any practical implementation must consider not just vote integrity, but also access control, data confidentiality, and system resilience under load.

Despite the technical maturity of blockchain and cryptographic research, many of the proposed systems are either too complex or too resource-intensive for small-scale or institution-specific use cases. Public voting frameworks often assume high computational power, dedicated hardware, or specialized cryptographic knowledge – conditions that are not always available in educational institutions. Moreover, student and faculty users typically expect intuitive interfaces and a seamless user experience, which overly technical or sluggish systems fail to provide. Existing solutions also tend to lack customization features for organizational hierarchies, candidate filtering, or role-based election processes common in universities. Therefore, there is a clear need for a tailored solution that meets the unique voting requirements of academic institutions like Esil University while maintaining high levels of security, transparency, and auditability.

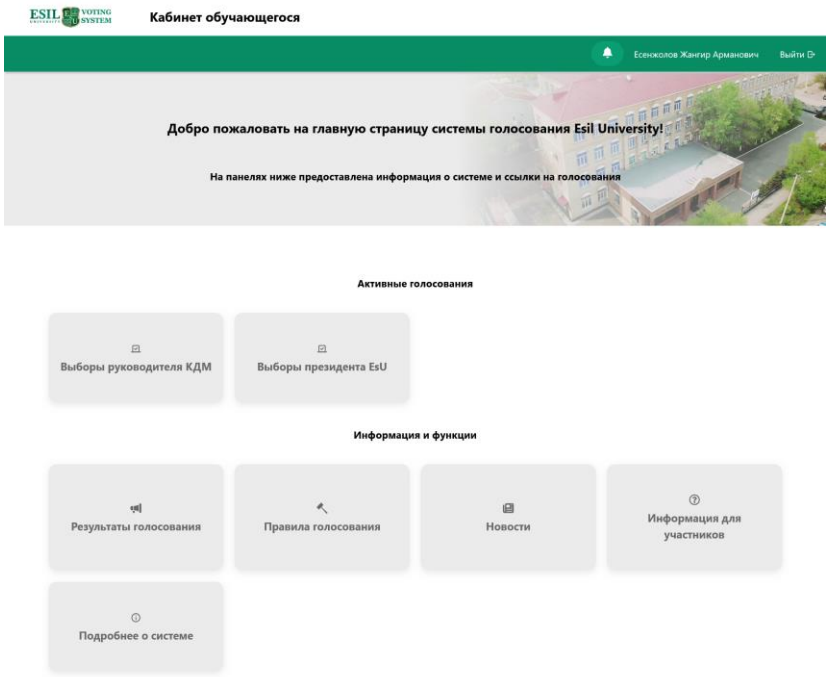
This project addresses that need by combining blockchain security with lightweight, maintainable technologies in a practical and scalable architecture. The front-end is built using React and TypeScript, providing a modular, strongly-typed, and responsive interface that ensures a smooth experience across devices. React's component-driven architecture makes the platform easy to maintain and extend, while TypeScript adds an extra layer of code safety. Axios is used for efficient

and secure HTTP communication between the client and the server. On the backend, Fastify, a modern and performance-focused Node.js framework, is chosen for its low overhead and ease of integration with plugins and middleware. Finally, MySQL serves as the relational data store, offering structured data handling and robust transactional support. A private blockchain component is integrated into this architecture, validating and logging each vote as an immutable transaction, while maintaining a clear separation of concerns between the blockchain, application logic, and user data. This combination results in a secure, transparent, and institution-specific voting platform that is both easy to use and hard to compromise.

Methods and Materials

This section outlines the architectural design, development process, and technologies used to implement the blockchain-enabled voting system for Esil University. The goal was to create a secure, transparent, and accessible web application that allows students and faculty members to participate in institutional elections with confidence that their votes are accurately recorded, validated, and protected from tampering. The project employed a layered and modular architecture to separate concerns across authentication, vote casting, vote validation, and result aggregation. Each layer was built with a focus on maintainability, scalability, and cryptographic integrity.

The frontend of the application was developed using React and TypeScript. React was selected for its component-based architecture, which enables reusable and modular user interface elements. This approach allowed rapid development of various components such as the login screen, candidate selection interface, confirmation modals, and result visualization dashboards. TypeScript added a type-safe layer on top of JavaScript, which significantly reduced runtime errors during development and made the codebase more maintainable and easier to scale. The UI was designed with simplicity in mind, following accessibility and responsive design principles to ensure that users could participate in the voting process seamlessly from desktops, tablets, or smartphones. The main page design can be seen on picture 1.



Picture 1 – https://vote.esil.edu.kz main page

Axios was used on the frontend for HTTP communication with the backend server. Axios offers features such as automatic JSON parsing, request/response interceptors, and CSRF protection, making it ideal for handling secure communication between client and server. Every user action, such as login, vote submission, and result retrieval, is encapsulated as an Axios request and handled asynchronously to ensure a responsive user experience. Authentication tokens and session identifiers are securely stored in memory, and sensitive operations are performed using HTTPS to prevent eavesdropping or man-in-the-middle attacks.

The backend was implemented using Fastify, a high-performance web framework for Node.js. Fastify was chosen over other alternatives due to its non-blocking architecture, built-in JSON schema validation, plugin extensibility, and superior performance benchmarks. Backend responsibilities include user authentication, candidate listing, vote submission endpoints, and blockchain interaction. All endpoints are protected with role-based access controls and request validation logic to ensure only authorized users can perform sensitive operations. For example, only eligible voters can cast a vote, and administrators have exclusive access to result dashboards and blockchain summaries. User data, election configurations, and session logs are stored in a MySQL database. MySQL was selected due to its widespread support, ACID-compliant transactions, and ability to handle complex relational queries. Tables include users, votes, elections, candidates, and audit_logs, all normalized and indexed for performance. Foreign key constraints and transaction isolation levels are enforced to prevent duplicate votes, orphaned records, and unauthorized updates. A particular focus was placed on ensuring vote idempotency - once a user submits a vote, any repeated submission attempts are ignored or rejected with proper error handling. To ensure that a person cannot vote twice, a check if they have voted previously is implemented. The check can be seen on picture 2, and the transaction of vote submission is on picture 3.

```
const [[alreadyVoted]] = await vote_db.query_f(
  `SELECT 1 FROM vote_participation WHERE vote_id = ? AND user_id = ? LIMIT 1`,
  [vote_id, user_id]
);

if (alreadyVoted) {
  return reply.code(409).send({ error: "Вы уже проголосовали" });
}
```

Picture 2 – Prevention of double votes

```
await vote_db.transaction_f(async (con) => {
  await con.query(
    `INSERT INTO vote_participation (vote_id, user_id, voted_at) VALUES (?, ?, NOW())`,
    [vote_id, user_id]
  );

  await con.query(
    `INSERT INTO vote_records (vote_id, candidate_id, voted_at) VALUES (?, ?, NOW())`,
    [vote_id, candidate_id]
  );

  await con.query(
    `INSERT INTO vote_chain (block_index, timestamp, vote_data, previous_hash, block_hash)
    [block_index, timestamp, voteData, previous_hash, block_hash]
  );
});
```

Picture 3 – A transaction for vote submission

The blockchain module was implemented as a private permissioned blockchain, operating alongside the main application as a vote validation and auditing service. Unlike public blockchains, the private blockchain is controlled and maintained internally by the institution's IT infrastructure. This ensures better performance, lower energy costs, and administrative control without sacrificing immutability and traceability. Each vote submitted through the backend is hashed using SHA-256 and broadcasted as a transaction to the blockchain. Transactions are grouped into blocks, timestamped, and appended to the chain through a simplified proof-of-authority (PoA) consensus mechanism, which is well-suited for trusted, institution-level environments. The "vote_chain" table collects the hashed continuity of "blocks", which are validated later during result check. The result can be seen on picture 4.

id INT	block_index INT	timestamp DATETIME	vote_data JSON	previous_hash VARCHAR(255)	block_hash VARCHAR(255)
4	1	30.07.2025 ...	{"vote_id": 1, "candidate_id": 3}	0	59fab80fd19e49b88c6b1dc02fc9...
5	2	30.07.2025 ...	{"vote_id": 1, "candidate_id": 3}	59fab80fd19e4...	21c83daa6581772f8764b468c603e63...
6	3	30.07.2025 ...	{"vote_id": 2, "candidate_id": 5}	21c83daa6581...	df551a483303976759f1ca265547e22...

Picture 4 – A chain of hashes

The blockchain node maintains a minimal ledger containing vote hashes, timestamps, and election IDs. This makes it possible to verify the authenticity and order of votes without revealing sensitive information. Once stored, votes become immutable; any attempt to modify past records would require consensus from the entire node network - an impossible task in this closed system without administrative tampering, which is easily detectable. Administrators can run audit routines that compare MySQL vote records with blockchain hashes to verify that no vote has been altered or omitted from the official results.

The development workflow followed an iterative, test-driven approach. Git was used for version control, and development was divided into sprints focusing on separate modules such as user management, blockchain integration, and UI testing. Unit tests and integration tests were written using Jest and Supertest for the backend, while the frontend components were tested using React Testing Library. Every critical function - such as vote recording, hash generation, and blockchain confirmation - was covered by automated tests to ensure robustness.

Security measures were a core part of the development cycle. Passwords were hashed using bcrypt before storage, JWT tokens were used for session management, and all sensitive routes were rate-limited and monitored. The system also includes logging and alerting mechanisms that notify administrators of suspicious activities, such as multiple failed login attempts or unusually timed vote submissions.

Finally, deployment and testing were done on a local staging server that mirrored the university's production environment. Docker containers were used to package the backend server, blockchain node, and MySQL database, making it easy to replicate and scale the system across different environments. Future deployment to Esil University's infrastructure will include load balancing and SSL certification for production readiness.

Results

The blockchain-enabled voting system was successfully deployed in a staging environment mimicking Esil University's infrastructure. The system was tested using a series of controlled mock elections involving administrative testers, faculty volunteers, and student accounts. The results validate the effectiveness, transparency, and resilience of the proposed solution.

Every submitted vote was cryptographically hashed and recorded in a blockchain ledger. During tests, any attempt to manipulate previously recorded votes directly in the MySQL database failed blockchain verification, highlighting the effectiveness of the immutability enforcement. Comparison routines confirmed a 100% match between stored vote hashes and real-time blockchain records, demonstrating the system's capability to detect tampering with deterministic certainty. The backend logic correctly rejected repeated vote submissions by the same user for the same election. Tests involving rapid repeated requests from the same user ID showed consistent 409 Conflict responses, and no duplicate entries were recorded in either vote_participation or vote_chain tables. This behavior was verified both through API logs and SQL query audits.

Using Fastify, the system handled concurrent voting requests with minimal latency. In a test scenario simulating 200 simultaneous vote submissions, the backend maintained an average response time of under 150ms per request, with no failed transactions. The blockchain component processed new blocks within 300ms of final vote submission. Frontend testing across multiple devices (desktop, tablet, smartphone) showed consistent rendering and usability of the interface. Voters were able to log in, view candidates, solve the CAPTCHA, and vote with a median completion time of 1.2 minutes. No critical errors or navigation issues were observed.

The integration of Google reCAPTCHA v2 successfully blocked all vote attempts without a valid CAPTCHA token. Submissions lacking valid authentication or CAPTCHA response returned appropriate 403 or 400 errors, with no data written to the database or blockchain, confirming the robustness of the access control layers.

System administrators were able to export voting records, including vote hashes, timestamps, and block indices, using prebuilt audit queries. These records were easily reconciled with the blockchain for manual verification, fulfilling the goal of a fully auditable vote history.

Preliminary feedback from participants and university administrators was positive. Test users highlighted the transparency and simplicity of the voting interface, while IT staff emphasized the ease of deployment and maintainability. The system's layered architecture also enabled targeted debugging during testing phases, which contributed to rapid issue resolution and confidence in production readiness.

Discussion

The implementation of a blockchain-enabled voting system for Esil University demonstrates the practical feasibility of integrating modern cryptographic technologies with institutional decision-making processes. The approach taken in this project bridges the gap between theoretical research and real-world application by providing a solution that is not only secure and auditable but also lightweight and user-friendly for a university environment.

One of the most important outcomes of this system is the validation mechanism powered by a private blockchain. This mechanism provides a cryptographic guarantee that each vote is both legitimate and immutable. By hashing each vote and storing it on a tamper-resistant ledger, the system eliminates the risk of post-submission vote manipulation - one of the most common concerns in digital voting systems. Furthermore, the use of a permissioned blockchain architecture ensures that only authorized nodes can participate in the consensus process, offering a balance between decentralization and administrative control.

The modular and layered architecture also plays a critical role in the project's success. The frontend, built with React and TypeScript, offers a modern, accessible user experience that simplifies the voting process for students and faculty alike. Meanwhile, Fastify on the backend ensures high-speed request handling, and MySQL provides the stability and relational structure needed for maintaining vote records, user data, and audit logs. The separation of concerns between these layers allows future improvements – such as multi-factor authentication or biometric ID integration - without major system rewrites.

However, several challenges and trade-offs were encountered during development. Implementing blockchain in a university setting requires administrative oversight and technical familiarity with decentralized systems, which may not always be present. Educating IT staff on blockchain maintenance and ensuring reliable uptime for validator nodes are essential to avoid voter distrust. Additionally, while vote data is hashed for privacy, further steps may be needed to fully anonymize user actions in compliance with evolving data protection standards.

Another consideration is scalability. While the current system is designed for institutional elections involving hundreds or thousands of users, further optimization would be needed for broader applications with more complex voting workflows or larger populations. Integration with Esil University's existing infrastructure - such as single sign-on (SSO) services or student portals - could also improve adoption and usability, but would require additional development effort.

Overall, the project successfully balances usability, performance, and security in a voting system tailored to the academic environment, paving the way for future expansions and broader applications in similar institutions.

Conclusion

This paper has presented the design and implementation of a blockchain-enabled voting web application developed specifically for Esil University. By combining cryptographic vote validation with a modern, modular web architecture, the system achieves a high level of security, transparency, and user accessibility. The integration of a private blockchain ensures the immutability of every vote, while cryptographic hashing and system-level protections prevent unauthorized actions and data manipulation.

The chosen technology stack – TypeScript and React for the frontend, Axios for API communication, Fastify and Node.js for backend logic, and MySQL for structured data storage - was proven to be both efficient and developer-friendly. It supports rapid development, clear separation of concerns, and straightforward deployment, making it suitable for institutional environments with limited technical resources.

While further enhancements are possible - such as biometric authentication, voter anonymity improvements, and expanded election configurations - the current system lays a strong foundation for secure, auditable, and user-centric digital elections. Most importantly, it demonstrates how blockchain can be effectively utilized beyond cryptocurrency, offering trust and transparency in democratic processes within academic settings.

References

1. Bisri A. A systematic literature review on digital transformation in higher education: Revealing key success factors / A. Bisri, A. Putri, Y. Rosmansyah // International Journal of Emerging Technologies in Learning (iJET). – 2023. – № 18(14). – P. 164-187. https://doi.org/10.3991/ijet.v18i14.40201.
2. Going from Internet voting to blockchain voting: Risks and challenges / S. Park et al // Journal of Cybersecurity. – 2021. – № 7(1), tyaa025. https://doi.org/10.1093/cybsec/tyaa025.
3. A comprehensive analysis of blockchain based voting systems / M. Atik et al // ACM Digital Library. – 2024. https://doi.org/10.1145/3723178.3723275.
4. An efficient and versatile e voting scheme on blockchain / B. Wang et al // Cybersecurity. – 2024. – № 7(1). – P. 15. https://doi.org/10.1186/s42400-024-00226-8.

5. Coercion resistant e voting scheme with blind signatures / A. Aziz et al // In 2019 Cybersecurity and Cyberforensics Conference (CCC). – 2019. – P. 1-8. https://doi.org/10.1109/CCC.2019.00009.
6. Leune K. Enhancing electronic voting with a dual blockchain architecture / K. Leune, J. Punjwani // Ledger. – 2021. – № 6. – P. 1-16. https://doi.org/10.5195/ledger.2021.199.
7. Leune K. Enhancing electronic voting with a dual blockchain architecture / K. Leune, J. Punjwani // Ledger. – 2021. – № 6. – P. 1-16. https://doi.org/10.5195/ledger.2021.199.
8. Blockchain based e voting system in a university / A. Marouan et al // International Journal of Electrical and Computer Engineering Systems. – 2024. – № 34(3). – P. 1915-1923. https://doi.org/10.11591/ijeecs.v34.i3.pp1915-1923.
9. A decentralized, anonymous, and transparent e voting system / W.-J. Lai et al // In 2018 1st IEEE Hot Information Centric Networking (HotICN). – 2018. – P. 24-29. https://doi.org/10.1109/HotICN.2018.8605994.
10. Sarier N.D. Efficient, usable and coercion resistant blockchain based e voting / N.D. Sarier // Journal of Information Security and Applications. – 2025. – № 75. – P. 104074. https://doi.org/10.1016/j.jisa.2025.104074.
11. Blockchain based e voting systems: A technology review / H. Berenjestanaki et al // Electronics. – 2023. – № 13(1). – P. 17. https://doi.org/10.3390/electronics1301017.
12. Analysis of blockchain solutions for e voting: A systematic literature review / A. Benabdallah et al // IEEE Access. – 2022. – № 10. – P. 70746-70759. https://doi.org/10.1109/ACCESS.2022.3173204.
13. Pawlak M. Trends in blockchain based electronic voting systems / M. Pawlak, A. Poniszewska Marańda // Information Processing & Management. – 2021. – № 58. – P. 102595. https://doi.org/10.1016/j.ipm.2021.102595.
14. Implementation of decentralized blockchain e voting / S.M. Khan et al // EAI Endorsed Transactions on Smart Cities. – 2020. – № 4(10). – P. e4. https://doi.org/10.4108/eai.13-7-2018.164859.
15. A modern electoral system in Malaysia using e voting with the implementation of blockchain technology / S.Y.X. Tong et al // International Journal of Data Science and Advanced Analytics. – 2023. – № 4. – P. 202-208. https://doi.org/10.69511/ijdsaa.v4i0.166.
16. Implementation of decentralized blockchain e voting / S.M. Khan et al // EAI Endorsed Transactions on Smart Cities. – 2020. – № 4(10). – P. e4. https://doi.org/10.4108/eai.13-7-2018.164859.
17. A modern electoral system in Malaysia using e voting with the implementation of blockchain technology / S.Y.X. Tong et al // International Journal of Data Science and Advanced Analytics. – 2023. – № 4. – P. 202-208. https://doi.org/10.69511/ijdsaa.v4i0.166.
18. Low power blockchained e vote platform for university environment / F. Chaabane et al // Future Internet. – 2022. – № 14(9). – P. 269. https://doi.org/10.3390/fi14090269.
19. Low power blockchained e vote platform for university environment / F. Chaabane et al // Future Internet. – 2022. – № 14(9). – P. 269. https://doi.org/10.3390/fi14090269.
20. Rahman M.S. A secure blockchain based e voting system for election processes / M.S. Rahman, M. Hasan // Journal of Information Security and Applications. – 2021. – № 60. – P. 102880. https://doi.org/10.1016/j.jisa.2021.102880.
21. Li F. Blockchain based e voting mechanisms: A survey and comparative study / F. Li, Y. Liu, Y. Zhao // Blockchain. – 2024. – № 4(4). – P. 21. https://doi.org/10.3390/blocks4040021.
22. Towards blockchain based e voting system / A.A. Yavuz et al // In 2018 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW). – 2018. – P. 71-75. IEEE. https://doi.org/10.1109/EuroSPW.2018.00015.
23. Rahman M.S. A secure blockchain based e voting system for election processes / M.S. Rahman, M. Hasan // Journal of Information Security and Applications. – 2021. – № 60. – P. 102880. https://doi.org/10.1016/j.jisa.2021.102880.
24. A blockchain based secure voting system for decentralized autonomous organizations / S. Yoo et al // Sensors. – 2021. – № 21(18). – P. 6223. https://doi.org/10.3390/s21186223.
25. Gao L. A blockchain based multi authority e voting scheme with privacy preservation / L. Gao, J. Chen, Y. Li // Information Sciences. – 2019. – № 476. – P. 357-372. https://doi.org/10.1016/j.ins.2018.12.027.

26. Kshetri N. Blockchain's roles in strengthening cybersecurity and protecting privacy / N. Kshetri // Telecommunications Policy. – 2017. – № 41(10). – P. 1027-1038. https://doi.org/10.1016/j.telpol.2017.08.005.
27. An overview of blockchain technology: Architecture, consensus, and future trends / Z. Zheng et al // In 2017 IEEE International Congress on Big Data (BigData Congress). – 2017. – P. 557-564. IEEE. https://doi.org/10.1109/BigDataCongress.2017.85.
28. A blockchain based secure voting system for decentralized autonomous organizations / S. Yoo et al // Sensors. – 2021. – № 21(18). – P. 6223. https://doi.org/10.3390/s21186223.
29. Sharma T.K. Blockchain based electronic voting system: A review / T.K. Sharma, A. Madan // Materials Today: Proceedings. – 2021. – № 45. – P. 10679-10684. https://doi.org/10.1016/j.matpr.2021.05.594.
30. Kshetri N. Blockchain's roles in strengthening cybersecurity and protecting privacy / N. Kshetri // Telecommunications Policy. – 2017. – № 41(10). – P. 1027-1038. https://doi.org/10.1016/j.telpol.2017.08.005.

Source of funding: *The research is funded by the Science Committee of the Ministry of Science and Higher Education of the Republic of Kazakhstan (grant IRN AR23489791 «Development of an online voting system based on blockchain technology»).*

Г. Шуитенов[1], А. Тургинбаева[2], С. Алтынбек[*], М. Муратбеков[2], Ж. Есенжолов[1]
[1]Esil University,
010008, Казахстан, г. Астана, ул. Жубанова, 7
[2]Евразийский национальный университет им. Л.Н. Гумилева,
010008, Казахстан, г. Астана, ул. Пушкина, 11
*e-mail: Serik_aa@bk.ru

ПРОВЕРКА РЕЗУЛЬТАТОВ ГОЛОСОВАНИЯ С ИСПОЛЬЗОВАНИЕМ БЛОКЧЕЙНА С ПОМОЩЬЮ КРИПТОГРАФИЧЕСКОГО ПОДХОДА И ПОДХОДА НА СИСТЕМНОМ УРОВНЕ ДЛЯ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ВЫБОРОВ

В этой статье представлено безопасное, прозрачное и защищенное от несанкционированного доступа веб-приложение для голосования. Разработанная специально для выборов университетского уровня, система использует частную блокчейн-сеть для обеспечения целостности и неизменности результатов каждого голосования. Созданная с использованием стека современных технологий – TypeScript и React во внешнем интерфейсе, Axios для связи и серверной части на базе Fastify Node.js с базой данных MySQL – платформа ставит во главу угла удобство использования и безопасность.

Процесс голосования аутентифицируется и валидируется с помощью криптографического хэширования и консенсуса на блокчейне, что предотвращает несанкционированные изменения или дублирование результатов голосования. Каждый голос регистрируется как транзакция в частном блокчейне, где узлы проверяют его легитимность, прежде чем он становится частью постоянного реестра. Эта интеграция блокчейна на системном уровне обеспечивает возможность аудита, прозрачность и доверие, устраняя необходимость в ручной проверке и снижая риск фальсификации выборов.

Решение разработано специально для институционального внедрения, гарантируя, что в нем смогут участвовать только прошедшие аутентификацию пользователи университета. Благодаря такому подходу проект демонстрирует, как технологии блокчейна могут быть практически применены для повышения доверия и эффективности цифровых демократических процессов.

Ключевые слова: *Блокчейн, Валидация голосов, Безопасные выборы, Криптографическое хэширование, Приватный блокчейн, Веб-голосование, Fastify, React, Node.js, MySQL.*

Ғ. Шуйтенов[1], А. Тұрғынбаева[2], С. Алтынбек[*], М. Мұратбеков[2], Ж. Есенжолов[1]
[1]Esil University,
010008, Қазақстан, Астана Қ., Жұбанов К-Сі, 7
[2] Л.Н. Гумилев атындағы Еуразия Ұлттық Университеті,
010008, Қазақстан, Астана Қ., Пушкин К-Сі, 11
*e-mail: Serik_aa@bk.ru

САЙЛАУДЫҢ ҚАУІПСІЗДІГІН ҚАМТАМАСЫЗ ЕТУ ҮШІН КРИПТОГРАФИЯЛЫҚ ЖӘНЕ ЖҮЙЕЛІК ДЕҢГЕЙДЕГІ ТӘСІЛ АРҚЫЛЫ БЛОКЧЕЙНДІ ҚОЛДАЙТЫН ДАУЫСТАРДЫ ТЕКСЕРУ

Бұл мақалада қауіпсіз, мөлдір және бұрмалануға төзімді веб-дауыс беру қолданбасы берілген. Университет деңгейіндегі сайлау үшін арнайы әзірленген жүйе әрбір дауыстың тұтастығы мен өзгермейтіндігін қамтамасыз ету үшін жеке блокчейн желісін пайдаланады. Заманауи технологиялық стек көмегімен құрастырылған-TypeScript және React on the frontend, axios for communication Және Fastify Негізіндегі Түйін.MySQL дерекқоры бар js сервері-платформа ыңғайлылыққа да, қауіпсіздікке де басымдық береді.

Дауыс беру процесі криптографиялық хэштеу және блокчейн консенсусы арқылы аутентификацияланады және расталады, бұл рұқсат етілмеген өзгертулердің немесе дауыстардың қайталануының алдын алады. Әрбір дауыс жеке блокчейндегі транзакция ретінде жазылады, онда түйіндер тұрақты кітаптың бөлігі болғанға дейін оның заңдылығын тексереді. Блокчейннің жүйелік деңгейдегі бұл интеграциясы аудиттілікті, ашықтықты және сенімділікті қамтамасыз етеді, қолмен тексеру қажеттілігін жояды және сайлауды бұрмалау қаупін азайтады.

Шешім институционалды қабылдауға бейімделген, оған тек аутентификацияланған университет пайдаланушылары қатыса алады. Осы тәсіл арқылы жоба цифрлық демократиялық процестердің сенімділігі мен тиімділігін арттыру үшін блокчейн технологияларын іс жүзінде қалай қолдануға болатынын көрсетеді.

Түйін сөздер: *Блокчейн, Дауыстарды Тексеру, Қауіпсіз Сайлау, Криптографиялық Хэштеу, Жеке Блокчейн, Веб-Дауыс Беру, Fastify, React, Node.js, MySQL.*

Information about the authors

Gabit Shuitenov – Candidate of pedagogical sciences, vice-rector of digitalization, Esil University, Kazakhstan, Astana; e-mail: shuitenov.g@esil.edu.kz. ORCID: https://orcid.org/0000-0002-9905-7247.

Alua Turginbayeva – Master's degree in Computer Science, chief teacher, Department of «Computer and Software Engineering», L.N. Gumilyov Eurasian National University, Kazakhstan, Astana; e-mail: tasheart@mail.ru. ORCID: https://orcid.org/0000-0002-5630-114X.

Serik Altynbek* – PhD, associate professor, chief teacher, Department of «IS and technologies», Esil University, Kazakhstan, Astana, e-mail: serik_aa@bk.ru. ORCID: https://orcid.org/0000-0002-8435-7773.

Zhangir Yessenzholov – Bachelor's degree in Computer Science, Esil University, Kazakhstan, Astana; e-mail: yessenzholov@list.ru. ORCID: https://orcid.org/0009-0009-4777-295X.

Авторлал туралы мәліметтер

Ғабит Шуйтенов – педагогика ғылымдарының кандидаты, цифрландыру проректоры, Esil University, Қазақстан, Астана қ.; e-mail: shuitenov.g@esil.edu.kz. ORCID: https://orcid.org/0000-0002-9905-7247.

Алуа Тургинбаева – Информатика магистрі, «Есептеу Және Бағдарламалық Қамтамасыз ету» кафедрасының бас оқытушысы, Л.Н. Гумилев Атындағы Еуразия Ұлттық Университеті, Қазақстан, Астана қ.; e-mail: tasheart@mail.ru. ORCID: https://orcid.org/0000-0002-5630-114X.

Серік Алтынбек* – PhD, доцент, "АЖ және технологиялар «Кафедрасының бас оқытушысы», Esil University, Қазақстан, Астана қ.; e-mail: serik_aa@bk.ru. ORCID: https://orcid.org/0000-0002-8435-7773.

Жәңгір Есенжолов – Информатика бакалавры, Esil University, Қазақстан, Астана қ.; e-mail: yessenzholov@list.ru. ORCID: https://orcid.org/0009-0009-4777-295X.

Сведения об авторах

Габит Шуйтенов – кандидат педагогических наук, проректор по цифровизации, Esil University, Казахстан, Астана; e-mail: shuitenov.g@esil.edu.kz. ORCID: https://orcid.org/0000-0002-9905-7247.

Алуа Тургинбаева – Магистр компьютерных наук, старший преподаватель кафедры «Компьютерная инженерия и программное обеспечение», Евразийский национальный университет им. Л.Н. Гумилева, Казахстан, Астана; e-mail: tasheart@mail.ru. ORCID: https://orcid.org/0000-0002-5630-114X.

Серик Алтынбек* – PhD, доцент, главный преподаватель кафедры «Информационные технологии», Esil University, Казахстан, Астана; e-mail: serik_aa@bk.ru. ORCID: https://orcid.org/0000-0002-8435-7773.

Жангир Есенжолов – степень бакалавра в области компьютерных наук, Esil University, Казахстан, Астана; e-mail: yessenzholov@list.ru. ORCID: https://orcid.org/0009-0009-4777-295X.

Received 01.08.2025
Accepted 12.08.2025