Blockchain-based governance for universities

Teodora NONCHEVA, Andrian MINCHEV

Trakia University, Department of Computer Science and Mathematics,
Stara Zagora, Bulgaria

teodora.noncheva@trakia-uni.bg, andrian.minchev@trakia-uni.bg

Abstract: *Many universities still employ a centralised or a manual method of academic governance that limits both participation and transparency; the implementation of a blockchain-based architecture creates a method of communication and participation through the separation of identity verification and vote casting, thus creating privacy and trust. This system allows for the implementation of weighted voting, quorum enforcement, and role-based eligibility using zero-knowledge proofs, blind signatures, and homomorphic encryption. Simulations demonstrate that the architecture is scalable, resilient against insider threats, and produces accurate results. Governance is conceptualized as an intrinsic functional layer of Virtual Learning Environments (VLEs), extending their role beyond content delivery toward participatory, transparent, and verifiable academic decision-making. This positioning aligns the proposed architecture directly with contemporary research on digital education ecosystems and virtual learning infrastructures*.

Keywords: Blockchain, Academic governance, Universities, Virtual learning Environments.

1. Introduction

The higher education's shift to digital platforms has altered how educational institutions teach and assess learning by creating a new way in which students and staff engage with one another through digital methods of communication (e.g., virtual classrooms), as well as the widespread growth of Learning Management System (LMS) platforms. As educational institutions become increasingly complex, operating in an environment that involves not only the instructor-student relationship but also the administration-staff-student relationship, the importance of governance in the academic environment cannot be understate. The methods by which academic institutions choose their leaders (rectors, academic councils, etc.) and control student activities are at the heart of this new system of governance (Ohize et al., 2025).

The methods of governance employed by higher educational institutions to elect and govern their staff and students have not yet fully evolved to accommodate the rapid growth of digital platforms in the same way that many of the institutions' learning and assessment processes have already shifted (Ohize et al., 2025). Most organisations continue to utilise paper ballots and manually manage electronic election and governance processes, both of which add significant logistical

https://doi.org/10.58503/icvl-v21y202609

impediments to participation by the entire academic community (Hajian Berenjestanaki et al., 2024). In addition, there are often concerns about the reliance on a small group of individuals with special access to the electronic systems used to govern, as it can detract from the perceived legitimacy of the election and governance processes (OECD, 2024). The absence of transparent and verifiable election and governance mechanisms in institutions has resulted in a fundamental inconsistency between the manner in which digital learning environments are structured and administered, and the manner in which elections and governance mechanisms have traditionally been conducted (Chen, 2024).

This paper proposes a blockchain-based governance architecture designed specifically for university ecosystems. The proposed model treats academic governance as an integral component of the digital learning environment rather than as a separate administrative process. By conceptualising governance mechanisms as part of the virtual learning infrastructure, the proposed approach directly aligns with contemporary research on participatory digital education ecosystems and extends the scope of VLEs beyond content delivery toward transparent and verifiable institutional decision-making.

In addition to designing for security, an academic study has found that secure digital governance systems also have educational implications. Transparent and verifiable digital governance systems foster a relationship of trust between institutions and those they serve, promote student and staff participation, and contribute to the development of digital citizenship competence within a virtual learning environment (OECD, 2024).

In contrast to existing approaches that treat governance as an external administrative process, this study frames academic governance as a native component of the virtual learning ecosystem. From this perspective, voting mechanisms are not merely institutional tools, but socio-technical instruments embedded within VLEs that support participation, transparency, and the development of digital citizenship competencies. This framing establishes a direct conceptual link between blockchain-based governance and the research scope of virtual learning environments.

2. Related work

Research on electronic voting systems has evolved significantly over the past decade, expanding from centralized automation-oriented solutions toward decentralized and cryptographically verifiable architectures. Contemporary studies increasingly leverage Distributed Ledger Technology (DLT) to enhance transparency, integrity, and auditability in both civic and organizational voting contexts. This evolution reflects a broader shift toward digital governance infrastructures that support participation and trust in distributed institutional environments.

Recent blockchain-based voting research emphasizes architectural robustness, privacy preservation, and procedural correctness. Studies published

between 2021 and 2025 explore permissioned and hybrid blockchain models, end-to-end verifiability, and formal governance constraints, demonstrating the growing maturity of blockchain voting systems beyond proof-of-concept implementations.

Platforms such as Polys employ blind signature schemes to cryptographically separate voter authentication from vote casting. The underlying blind signature protocol, originally formalized by Chaum (1983), remains a foundational cryptographic primitive and continues to underpin modern privacy-preserving voting architectures, including contemporary blockchain-based systems. While the blind signature scheme originates from foundational cryptographic research, it remains a canonical mechanism upon which modern privacy-preserving voting systems are constructed, including contemporary blockchain-based architectures. Systems such as Voatz adopt permissioned blockchain infrastructures, including Hyperledger Fabric (Androulaki et al., 2018), to balance throughput and governance control. Recent studies emphasize that permissioned consensus models are particularly suited for institutional elections, where regulatory compliance and controlled participation are critical.

Despite these developments, existing platforms often do not support dynamic quorum requirements and role-based representation specific to the academic environment. Early conceptualizations of Virtual Learning Environments primarily emphasized content delivery and instructional support, with limited consideration for institutional governance functions (Chen, 2024). Recent research, however, increasingly explores the expansion of VLEs toward integrated digital governance and participatory infrastructures.

This research delineates the evolution of e-voting systems from centralized administrative tools toward decentralized trustless architectures utilizing Distributed Ledger Technology (DLT). While legacy systems prioritize automation, contemporary DLT-based frameworks such as Exonum and Voatz attempt to reconcile the tension between performance (throughput) and integrity (auditability) through permissioned consensus models.

Table 1. Comparative taxonomy of E-voting architectures

Architectural Paradigm	**Implementation / Framework**	**Primary Objective**	**Governance Model**	**Critical Limitations**
Monolithic Centralized	Legacy Civic/Org Systems	Operational Automation	**Centralized:** High reliance on a single Trusted Third Party (TTP).	Single Point of Failure (SPOF); lack of independent verifiability.
Permissionless DLT	Initial *Polys* Infrastructure	Censorship Resistance	**Decentralized:** Publicly verifiable via global consensus.	Scalability bottlenecks (latency); high resource intensity.

Permissioned / Consortium DLT	*Exonum*, *Voatz* (Hyperledger Fabric)	Throughput Optimization	**Federated:** Pre-approved validators manage consensus.	Diminished decentralization; potential for validator collusion.
Hybrid / Skipchain	Privatized/Public Hybrid	Temporal Integrity	**Anchored:** Private state periodically timestamped to public chain.	Architectural complexity; dependency on public chain persistence.
Integrated VLE Governance	Digital Citizenship Frameworks	Participatory Pedagogy	**Ecosystemic:** Governance as a core pedagogical function.	Categorical exclusion from current LMS/VLE design.
Privacy-Preserving Cryptography	ZKP, Homomorphic Encryption	Anonymity & Integrity	**Algorithmic:** Mathematical proof of vote validity.	Complexity in mapping to weighted, role-based academic hierarchies.

A significant techno-pedagogical gap was identified in early VLE research, where governance was treated as an external administrative layer (Dillenbourd, 2000) rather than an integral component of the learning ecosystem (Kaleci, Devkan, 2025). In this study, this observation is used to contextualize the historical evolution of VLE design, rather than to characterize the current state of learning management systems. This observation reflects the state of VLE design at the time and is used in this study to illustrate the historical separation between learning environments and governance processes, rather than to characterize current LMS capabilities. Furthermore, while cryptographic primitives like Zero-Knowledge Proofs (ZKP) ensure voter anonymity, their application remains under-prototyped in the nuanced context of academic governance, where weighted voting and role-based eligibility are mandatory.

Recent studies have significantly advanced the field of blockchain-based electronic voting by addressing transparency, security, and architectural scalability in both civic and organizational contexts (e.g., 2021–2025). Contemporary research explores permissioned blockchain governance models, end-to-end verifiability, and integration with digital platforms, providing an up-to-date foundation upon which this study builds. Unlike prior work, the present research explicitly focuses on university governance and its embedding within virtual learning environments (Jain, A. K., Gupta, N., & Gupta, B. B., 2025).

3. Regulatory and institutional constraints

The proposed architecture divides the process into three domains: institutional services (Off-chain), privacy gateway, and blockchain layer (On-chain).

3.1. Mathematical model of blind signatures

To break the link between identity and voice, an RSA blind signature scheme is used. The process is formalized as follows (Ye, J., et al., 2024):

- **Blinding**: The voter generates a message m (voting token) and masks it with a random number r: $m' \equiv m.r^{and}\ (towards\ N)$, where **(**and**,** N) is the university's public key.
- **Signing**: The university signs the masked message: $s' \equiv m'^{d}\ (towards\ N)$
- **Unblinding**: The voter removes the masking to obtain a valid signature s: $s \equiv s'.r^{-1} \equiv m^{d}\ (mod\ N)$

This mechanism allows the student to vote anonymously, proving to the blockchain that they own an authorized token, without the university knowing its contents.

3.2. Homomorphic encryption and vote summation

To protect the intermediate results, the cryptosystem is applied, which has an additive homomorphic property (Morar, C. D., et al. (2024). If two votes v1 and v2 are encrypted as E(v1) and E(v2), then their sum in encrypted form is calculated as the product of the ciphertexts:

$E(v1 + v2) = E(v1).E(v2)$

This allows the smart contract to perform tallying without decrypting individual ballots until the end of election day.

4. Experimental setup and evaluation

The experimental scenarios are designed to reflect governance processes typically conducted within digitally mediated university environments, where participation is distributed and asynchronous, similarly to interactions within virtual learning platforms.

This section evaluates the feasibility and correctness of the proposed blockchain-based e-voting architecture through scenario-based simulations reflecting realistic university governance elections. The evaluation focuses on procedural enforcement, eligibility control, and resilience against invalid and double-voting attempts, rather than cryptographic performance benchmarking.

4.1. Experimental Setup

Number of eligible voters (E): 300
Number of candidates (C): 4
Quorum requirement (Q): 70% of eligible voters
$Q = [0.7 \times E] = 210$
Voters are assumed to be authenticated off-chain via institutional identity

systems and issued one-time anonymous voting credentials. The blockchain layer processes only anonymized ballots and credential identifiers.

To evaluate procedural robustness, four turnout scenarios were simulated:

Table 2. Results of the quantitative analysis

Role	Eligible	Weight	Valid voters	Role turnout	Weighted valid
Faculty	80	2	55	68.8%	110
Students	200	1	145	72.5%	145
Staff	20	1	15	75.0%	15
Total	**300**		**215**	**71.7%**	**270**

Headcount quorum check (70%): 215≥210 ⇒ Valid
Weighted quorum check (70%): 270≥266 ⇒ Valid

To reflect typical university governance structures, we simulated a role-based electorate with weighted voting. The results show that both headcount-based quorum (215/300 = 71.7%) and weighted quorum (270/380 = 71.1%) can be enforced deterministically as explicit governance policies. This strengthens the positioning of the proposed model as a governance layer for Virtual Learning Environments, where participation is distributed and institutional roles must be represented transparently.

4.2. Evaluation Metrics

Evaluation uses the following metrics:

- Turnout ratio
  $\text{Turnout} = \frac{V}{E}$, where V is the number of accepted (valid) ballots.
- Quorum satisfaction
  $\text{Quorum\_met} = \begin{cases} \text{true}, V \geq Q \\ \text{false}, V < Q \end{cases}$
- Invalid ballot rate
  $\text{Invalid\_rate} = \frac{I}{V + I}$, where I is the number of rejected ballots.
- Double-voting detection rate
  $\text{DV\_caught} = \frac{\text{Rejected}_{\text{used\_token}}}{\text{Attempted}_{\text{double}}}$

These metrics reflect both governance correctness and security-related properties of the system.

5. Discussion and Impact on virtual learning

The implementation of the proposed architecture redefines academic governance as an integral pedagogical and participatory component of Virtual

Learning Environments rather than a separate administrative function.

Digital trust: Algorithmic transparency increases student engagement in online communities.

Governance Literacy: Participants gain practical knowledge about decentralized systems and cryptographic data protection.

Digital Citizenship: The system prepares students for responsible participation in the democratic processes of the digital society.

The experimental results demonstrate that the proposed architecture can reliably enforce quorum requirements, prevent double voting, and maintain procedural correctness under realistic university election conditions. In this sense, governance is not treated as a parallel administrative workflow, but as an integral socio-technical process embedded within digitally mediated academic participation.

While the evaluation does not benchmark cryptographic proof generation or network-level throughput, it validates the system's logical correctness and governance suitability. These results provide strong evidence that the architecture is viable for pilot deployments in academic environments.

6. Legal and ethical considerations

The architecture is designed according to the Privacy-by-Design principle to ensure compliance with GDPR and the Law on Higher Education (GDPR, EU 2016/679).

Right to deletion: Personal data remains Off-chain. When the identifier is deleted from the university database, the corresponding cryptographic hash in the blockchain becomes unusable (Hash-and-Delete).

Ethics: The system prevents student profiling through the use of anonymous one-time tokens.

7. Conclusion and future work

The proposed blockchain architecture provides a reliable infrastructure for managing universities. References to early LMS research are employed strictly to contextualize the historical evolution of virtual learning environments and do not constitute the technological basis of the proposed future developments. It combines mathematical security with educational goals, supporting the vision of the European Digital Education Area (EDEA). The present study delivers a validated architectural and procedural model for blockchain-based academic governance, positioned explicitly within the context of Virtual Learning Environments. The contribution of this work lies in its conceptualization and experimental validation of governance as an intrinsic component of digital learning ecosystems, rather than in the development of a specific software implementation.

Future work will extend this validated model toward applied implementations in contemporary LMS platforms such as Moodle and Canvas,

with the objective of empirically studying usability, scalability, and stakeholder acceptance within authentic virtual learning environments.

The paper presented a blockchain-based e-voting architecture specifically designed for university governance elections. The proposed system employs a constraint-driven design approach, which translates regulatory, institutional and privacy requirements into concrete architectural and procedural mechanisms. The architecture separates identity verification from the casting of votes, enforces quorum and eligibility rules through smart contracts, and leverages permissioned blockchain governance to balance institutional control with distributed trust.

The experimental evaluation of the proposed approach was conducted through the use of scenario-based experimentation. This evaluation demonstrated that the approach can reliably enforce quorum requirements, detect invalid and double-voting attempts, and determine election outcomes without processing personal data on-chain. The findings of this study demonstrate the viability of blockchain-based e-voting systems within academic environments and underscore their capacity to augment transparency and trust in university decision-making processes.

The evaluation focused on governance correctness instead of cryptographic or network performance, yet the findings provide a resilient foundation for future research. It is evident that a number of directions merit further investigation. Firstly, the integration of advanced cryptographic techniques, such as homomorphic encryption and zero-knowledge proofs, has the potential to facilitate fully encrypted tallying and enhance the integrity of end-to-end verification. Secondly, it is necessary to assess operational scalability by performing performance benchmarking under realistic network conditions and mobile device constraints. Thirdly, extending the architecture to support weighted voting and multi-round election procedures would address additional governance scenarios common in higher education.

It is recommended that subsequent research endeavors involve the implementation of pilot projects within authentic academic institutions. This will facilitate the evaluation of usability, stakeholder acceptance, and organizational impact. Such empirical studies are expected to further illuminate the socio-technical role of governance within virtual learning environments and to support the responsible evolution of participatory digital education infrastructures.

REFERENCES

Androulaki et al. (2018) Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains. *EuroSys*. ACM, 2018.

Chaum, D. (1083) Blind Signatures for Untraceable Payments. *Advances in Cryptology – CRYPTO*. 1983

Chen, X., He, S., Sun, L., Zheng, Y. & Wu, C. Q. (2024) A survey of consortium blockchain and its applications. Cryptography. 8(2), 12. https://doi.org/10.3390/cryptography8020012.

Dillenbourg, P. (2000) Virtual Learning Environments. *EUN Conference Proceedings*.

Hajian Berenjestanaki, M., Barzegar, H. R., El Ioini, N., Pahl, C. (2024) Blockchain-Based E-Voting Systems: A Technology Review. *Electronics*. 13, 17. https://doi.org/10.3390/electronics13010017.

Jain, A. K., Gupta, N. & Gupta, B. B. (2025) A survey on scalable consensus algorithms for blockchain technology. *Cyber Security and Applications*. 3, 100065. https://doi.org/10.1016/j.csa.2024.100065.

Kaleci, Devkan (2025) Integration and application of artificial intelligence tools in the Moodle platform: A theoretical exploration. *Journal of Educational Technology and Online Learning*. 8. 100-111. https://doi.org/10.31681/jetol.1595079.

Komljenovic, J., Birch, K., Sellar, S., et al. (2025) Digitalised higher education: Key developments, questions, and concerns. *Discourse*. 46(2), 276–292. https://doi.org/10.1080/01596306.2024.2408397.

Morar, C. D. et al. (2024) A survey of blockchain applicability, challenges, and key threats. *Computers*. 13(9), 223. https://doi.org/10.3390/computers13090223.

Ohize, H. O., Onumanyi, A. J., Umar, B. U. et al. (2025) Blockchain for securing electronic voting systems: A survey of architectures, trends, solutions, and challenges. *Cluster Computing*. https://doi.org/10.1007/s10586-024-04709-8

Regulation (EU) 2016/679 (GDPR).

Ye, J. et al. (2024) An electronic voting scheme with privacy protection. *Procedia Computer Science*. 246, 1050–1057. https://doi.org/10.1016/j.procs.2024.09.147.