International Journal of Emerging Technology in Computer Science & Electronics (IJETCSE)
ISSN: 0976-1353 Volume 32 Issue 02 – FEBRUARY 2026.

A Critical Review of Blockchain-Based Electronic Voting Systems: Scalability, Security, and Infrastructure Constraints in Developing Democracies

Yakubu Atomsa[#1], Gregory Maksha Wajiga[*2], Etemi Joshua Garba [*2], and Yusuf Musa Malgwi[*2]

[#] *Department of Computer Science, Faculty of Science, Federal University of Kashere, Gombe State, Nigeria*

[*] *Department of Computer Science, Faculty of Computing, Modibbo Adama University, Yola, Adamawa State Nigeria*

Abstract – **Blockchain technology is widely proposed as a foundation for secure and transparent electronic voting systems. However, large-scale electoral deployment remains constrained by unresolved challenges relating to scalability, governance, and infrastructural readiness. This paper presents a structured critical review of blockchain-based electronic voting systems with emphasis on deployment feasibility in developing democracies. Drawing on systematically selected literature, the review synthesizes findings across architectural models, consensus mechanisms, cryptographic techniques, and scalability strategies including sharding, off-chain processing, and parallel validation. The analysis shows that while blockchain enhances auditability and tamper resistance, practical viability depends on the interaction between system design, performance engineering, and infrastructure capacity. Across reviewed studies, throughput limitations, consensus overhead, and connectivity dependence consistently emerge as major barriers to national-scale implementation. Evidence further indicates that hybrid architectures combining high-performance validation with public auditability are the most frequently proposed pathway toward large-scale feasibility, though empirical validation remains limited. By integrating architecture, scalability, and infrastructure constraints within a unified evaluation framework, this study provides a research roadmap for infrastructure-aware blockchain voting systems in emerging democracies.**

Index Terms— **Blockchain, electronic voting, scalability, sharding, consensus mechanisms, wireless mesh networks, developing countries.**

I. Introduction

Electoral integrity remains central to democratic legitimacy, motivating continued interest in secure electronic voting systems. Conventional e-voting platforms are typically centralized, creating single points of failure and limiting public verifiability [28], [49]. Blockchain technology has therefore been proposed as an alternative trust model enabling distributed record maintenance and cryptographically verifiable audit trails [31] [66].

Despite rapid growth in proposed blockchain voting systems, national-scale deployment remains contested. Public blockchain infrastructures exhibit throughput and latency constraints that conflict with time-bounded electoral workloads [19], [26]. Permissioned and hybrid architectures improve performance but introduce governance and trust trade-offs [23], [57]. Evidence across reviewed studies suggests hybrid models combining controlled consensus with public auditability are the most frequently proposed pathway toward national-scale feasibility, although real-world deployment remains limited.

Beyond performance considerations, infrastructural readiness represents a critical determinant of feasibility. Reliable connectivity, stable power supply, and digital accessibility directly influence system availability and participation equity in emerging democracies [13]. However, existing reviews typically evaluate security, architecture, or consensus mechanisms independently, with limited integration of scalability engineering and infrastructural constraints [16], [25].

This paper addresses this gap through a structured critical review integrating architectural analysis, scalability mechanisms, and infrastructure readiness within a unified deployment-oriented framework. The study synthesizes design trade-offs, evaluates feasibility conditions, and identifies research priorities for scalable and infrastructure-aware blockchain-based voting systems.

II. Related Work

A growing body of review literature examines blockchain-based electronic voting systems from security, architectural, and implementation perspectives. Broad syntheses report that blockchain architectures enhance transparency and tamper resistance while facing persistent challenges related to scalability, governance complexity, and deployment maturity [58], [38].

Security-focused reviews emphasize cryptographic mechanisms enabling privacy-preserving and verifiable elections. Homomorphic encryption, zero-knowledge proofs, and distributed verification protocols are widely identified as foundational techniques for ballot secrecy and end-to-end verifiability, though their computational overhead constrains system scalability [38], [22].

Comparative analyses of blockchain voting frameworks reveal substantial architectural diversity and limited empirical validation at scale. Reported limitations include identity management risks, smart contract vulnerabilities, consensus overhead, and digital divide challenges [15], [61]. Scalability-oriented reviews consistently identify throughput limits, network synchronization cost, and latency constraints as major barriers to national deployment [39] [16].

Methodologically, prior reviews vary in analytical design. Narrative and taxonomy-oriented studies provide conceptual classification but limited deployment insight. Security-focused analyses emphasize cryptographic guarantees while abstracting from performance constraints. Scalability-centered reviews evaluate optimization mechanisms but frequently assume stable infrastructure conditions. These differences produce fragmented findings that do not fully capture interactions among architecture, performance engineering, and deployment environment constraints.

Accordingly, the literature lacks a deployment-oriented synthesis integrating architecture, scalability mechanisms, and infrastructural readiness within a unified evaluation model. This study addresses this gap through a structured comparative framework focused on feasibility in developing democracies. The methodological approach is described in the next section.

Table 2.1: Comparative Positioning of Blockchain Voting Review Studies

Study	Scope Focus	Scalability Analysis	Infrastructure Constraints	Empirical/System Comparison	Deployment Context
[58] Taş & Tanrıöver (2020)	General blockchain voting landscape	Limited	Not addressed	Conceptual classification	General
[38] Jafar et al. (2021a)	Architecture and feasibility	Moderate	Minimal	Conceptual framework	General
[34] Huang et al. (2021)	Security and taxonomy	Limited	Not addressed	Survey analysis	General
[22] Devi & Bansal (2022)	Security threats and cryptography	Not central	Not addressed	Security-focused review	General
[15] Benabdallah et al. (2022)	Comparative system analysis	Moderate	Limited mention	Implementation comparison	General
[61] Vladucu et al. (2023)	Systems overview and terminology	Limited	Limited	Survey of proposals	General
[39] Jafar et al. (2021b)	Scalability techniques	Strong	Not addressed	Performance comparison	General
[16] Berenjestanaki et al. (2024)	Challenges and trends	Moderate	Limited	Conceptual review	General
This Study	Architecture + scalability + infrastructure integration	Comprehensive	Central focus	Analytical synthesis	Developing democracies

III. REVIEW METHODOLOGY AND ANALYTICAL FRAMEWORK

This study adopts a structured literature review methodology to synthesize research on blockchain-based electronic voting systems with emphasis on scalability, security, and deployment feasibility. The review follows a transparent search–screening–selection protocol to reduce selection bias and enable systematic comparison across heterogeneous proposals.

3.1 Data Sources and Search Strategy

Relevant literature was retrieved from IEEE Xplore, Scopus, Web of Science, and SpringerLink, with supplementary identification through Google Scholar. Searches employed controlled keywords and Boolean combinations including *blockchain voting*, *scalable blockchain voting*, *smart contract voting*, and *decentralized voting systems*. Reference chaining was applied to identify additional influential studies.

3.2 Eligibility Criteria

Studies were included if they (i) were peer-reviewed journal or conference publications, (ii) proposed or evaluated blockchain-based voting architectures or scalability mechanisms, (iii) were published between 2015 and 2024, and (iv) presented technical, security, or performance analysis. Non-academic sources and cryptocurrency-only studies were excluded.

3.3 Study Selection

The initial search produced approximately 130 publications. After duplicate removal and abstract screening, 78 studies were retained for full-text evaluation. Application of eligibility criteria yielded 60 primary studies forming the analytical basis of this review [39] [16].

3.4 Analytical Framework

To enable cross-study comparison, selected works were evaluated across five integrated dimensions:

1. ***Architecture*****:** public, permissioned, or hybrid governance structure
2. ***Security Properties*****:** anonymity, verifiability, coercion resistance
3. ***Scalability Strategy*****:** sharding, off-chain processing, consensus optimization
4. ***Infrastructure Dependency*****:** connectivity, energy stability, device capability
5. ***Deployment Feasibility*****:** suitability for national-scale elections

This framework extends prior reviews that examine security or consensus mechanisms independently by jointly evaluating system design and environmental constraints [34], [15].

The analytical model provides the basis for the architectural synthesis presented in the next section.

IV. BLOCKCHAIN-BASED ELECTRONIC VOTING ARCHITECTURES

Blockchain-based electronic voting systems aim to provide tamper-resistant record keeping, verifiable tally processes, and transparent auditability through distributed ledger mechanisms [31], [66]. Existing proposals differ primarily in governance structure, consensus design, and privacy implementation, resulting in distinct architectural categories with varying deployment implications.

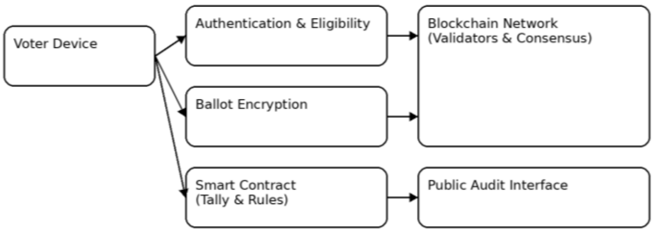

Fig. 4.1: Functional Architecture of Blockchain-Based Electronic Voting

4.1 Public Blockchain Voting Architectures

Public blockchain voting systems operate on open networks where any participant may validate transactions. These architectures maximize transparency and auditability by enabling universal verification of election records [48]. However, consensus mechanisms such as Proof-of-Work introduce latency and throughput constraints incompatible with time-bounded electoral processes [26], [19]. Energy consumption and unpredictable confirmation time further limit suitability for national-scale elections.

4.2 Permissioned Blockchain Voting Architectures

Permissioned architectures restrict validator participation to authorized entities, enabling deterministic consensus and predictable performance [18]. Protocols such as Practical Byzantine Fault Tolerance provide fast finality and controlled governance structures appropriate for institutional settings [2]. However, validator centralization introduces trust concentration and governance dependency risks, potentially weakening perceived neutrality of the electoral infrastructure [23].

4.3 Hybrid and Consortium Models

Hybrid architectures combine controlled validation with public auditability by separating transaction validation from transparency mechanisms [57]. Consortium-based governance distributes trust across multiple institutions while maintaining operational efficiency. Across reviewed studies, hybrid models are the most frequently proposed approach for large-scale electoral deployment due to their balance between performance and transparency [39], [16]. Nevertheless, empirical validation under real electoral workloads remains limited.

Table 4.1: Comparison of Blockchain Voting Architectural Models

Architecture	**Transparency**	**Performance**	**Governance**	**Typical Limitations**
Public Blockchain	High	Low–Moderate	Open participation	Latency, throughput constraints, energy cost
Permissioned Blockchain	Moderate–High	High	Validator set controlled	Collusion risk, trust assumptions
Hybrid Architecture	High (public audit)	High	Mixed governance	Design complexity, coordination overhead

4.4 Cryptographic Mechanisms for Voting Integrity

Blockchain voting frameworks employ specialized cryptographic techniques to ensure ballot secrecy and verifiability. Homomorphic encryption enables encrypted tally computation without revealing individual votes, while zero-knowledge proofs allow verification of ballot correctness without disclosing voter choices [34], [22]. These mechanisms enhance trust but introduce computational overhead that affects system scalability.

4.5 Architectural Trade-Off Synthesis

Architectural design reflects a balance among transparency, performance, and governance control. Public systems prioritize auditability but face scalability limitations. Permissioned systems improve performance at the cost of decentralization. Hybrid models attempt to reconcile these tensions but require careful coordination between consensus efficiency and verification transparency. Consequently, architectural choice alone does not determine deployment feasibility; performance engineering and infrastructure capacity remain critical determinants.

Table 4.2: Comparison of Consensus Mechanisms for Blockchain-Based Electronic Voting

Consensus Mechanism	Core Principle	Finality Type	Throughput	Latency	Energy Demand	Suitability for National Elections	Key Advantages	Key Limitations
Proof of Work (PoW)	Nodes solve cryptographic puzzles to append blocks	Probabilistic	Low	High	Very High	Low	Strong security, censorship resistance	Slow confirmation, high energy consumption, poor scalability
Proof of Stake (PoS)	Validators selected based on stake ownership	Probabilistic / Deterministic (variant-dependent)	Medium	Medium	Low	Moderate	Energy efficient, better scalability than PoW	Stake concentration risks, governance complexity
Practical Byzantine Fault Tolerance (PBFT)	Known validators reach agreement through message exchange rounds	Deterministic	High	Low	Low	High (permissioned systems)	Fast finality, high throughput, strong consistency	Limited scalability with large validator sets
Proof of Authority (PoA)	Pre-approved authorities validate transactions	Deterministic	High	Very Low	Very Low	High (controlled environments)	Predictable performance, minimal resource overhead	Centralization risk, trust in authorities required
Hybrid Consensus (PoS + BFT)	Combines stake-based selection with BFT validation	Deterministic	High	Low	Low	Very High	Balances scalability, security, and efficiency	Increased design complexity, governance challenges

Table 4.3: Security Properties vs Cryptographic Techniques in Blockchain-Based E-Voting

Security Property	Homomorphic Encryption	Zero-Knowledge Proofs	Mix-Nets	Secret Sharing / Threshold Cryptography	Blockchain Ledger	Smart Contracts
Ballot Secrecy	✓ Encrypts votes while enabling computation	✓ Proves correctness without revealing vote	✓ Anonymizes vote paths	✓ Distributes decryption authority	✕ Public record (encrypted only)	✕ Depends on external crypto
Voter Anonymity	✓ Hides vote content	✓ Prevents identity disclosure	✓ Breaks link between voter and ballot	✓ Prevents single-party exposure	✕ Requires pseudonymous identities	✕ Not inherent
End-to-End Verifiability	✓ Enables verifiable tally	✓ Public correctness proofs	✓ Verifiable mixing steps	✓ Collective verification	✓ Immutable audit trail	✓ Deterministic execution
Integrity / Tamper Resistance	✓ Prevents vote alteration	✓ Detects invalid operations	✓ Ensures valid permutation	✓ Prevents unilateral decryption	✓ Append-only ledger	✓ Enforces election rules
Coercion Resistance	◑ Limited	✓ Supports receipt-free protocols	✓ Removes traceability	◑ Depends on implementation	✕ Public auditability may expose patterns	✕ Not inherent
Transparency / Auditability	◑ Requires proof layer	✓ Public verification possible	✓ Verifiable mixing	✓ Distributed trust	✓ Full transaction traceability	✓ Public logic verification
Fault Tolerance	◑ Depends on key management	◑ Protocol dependent	◑ Depends on mix servers	✓ Robust against node compromise	✓ Distributed consensus	✓ Automated recovery logic
Scalability Impact	✕ High computational overhead	✕ Proof generation cost	✕ Communication overhead	◑ Moderate overhead	◑ Depends on consensus	◑ Execution cost

Legend: ✓ Strong support ◑ Conditional / partial support ✕ Not provided inherently

V. SCALABILITY MECHANISMS AND PERFORMANCE CONSTRAINTS

National-scale elections impose bursty transaction loads, strict time windows, and requirements for deterministic, publicly auditable outcomes. Blockchain-based voting systems must therefore balance throughput, latency, security, and governance control under peak participation conditions [30].

5.1 Sharding-Based Processing

Sharding partitions the network into parallel processing groups, distributing transaction validation across multiple subsets of nodes to increase throughput [47], [65]. In electoral deployments, shards may correspond to administrative regions, enabling localized validation and reduced congestion. However, cross-shard communication and global state aggregation introduce synchronization overhead and potential security vulnerabilities [20].

5.2 Off-Chain and Layer-Two Mechanisms

Off-chain processing reduces ledger load by executing operations outside the primary blockchain while preserving verifiability through cryptographic commitments [57]. These approaches lower latency and storage demands but require reliable dispute resolution and verification protocols to maintain electoral integrity.

5.3 Parallel Transaction Validation

Parallel execution frameworks allow independent vote transactions to be processed simultaneously, improving responsiveness during peak voting periods [64]. Ensuring deterministic execution order and preventing race conditions remains a central design challenge for secure vote recording.

5.4 Consensus Optimization

Permissioned consensus protocols such as Practical Byzantine Fault Tolerance and Proof-of-Authority provide deterministic finality and predictable confirmation times suited to time-bounded electoral processes [18], [2], [9]. Performance gains, however, may introduce governance centralization risks and reduced fault tolerance under adversarial conditions.

5.5 Scalability Trade-Off Synthesis

Scalability mechanisms improve performance but introduce trade-offs among decentralization, complexity, and security assurance. Evidence across reviewed studies indicates that performance optimization alone does not ensure deployment feasibility; system effectiveness remains contingent on infrastructural capacity, network stability, and governance design [30], [39], [26], [17].

VI. INFRASTRUCTURAL CONSTRAINTS AND DEPLOYMENT FEASIBILITY

Large-scale deployment of blockchain-based electronic voting systems depends not only on architectural design and scalability mechanisms but also on underlying infrastructural capacity. Across reviewed studies, connectivity reliability, energy stability, digital accessibility, and institutional governance emerge as decisive determinants of operational feasibility.

6.1 Connectivity and Network Reliability

Blockchain voting systems require stable communication networks for transaction propagation, consensus participation, and ledger synchronization. In infrastructure-constrained environments, intermittent connectivity can delay confirmation, increase fork probability, and disrupt consensus finality [30], [61]. Empirical indicators from the International Telecommunication Union and the World Bank document persistent disparities in broadband availability across developing regions, directly affecting the feasibility of fully online voting infrastructures.

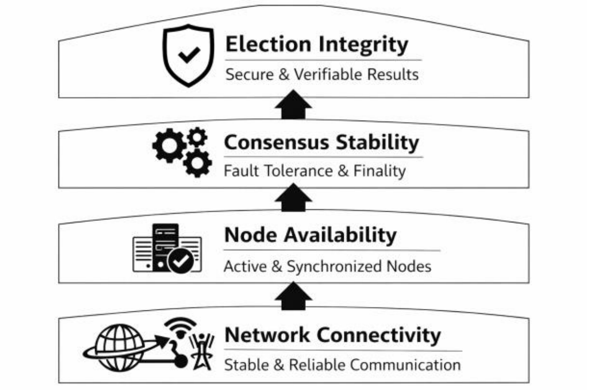
Election Integrity
Secure & Verifiable Results
Consensus Stability
Fault Tolerance & Finality
Node Availability
Active & Synchronized Nodes
Network Connectivity
Stable & Reliable Communication

Fig. 6.1: Infrastructure Dependency Model of Blockchain-Based E-Voting

6.2 Energy Infrastructure and System Availability

Reliable electrical power is essential for continuous node operation, storage persistence, and validator participation. Power instability can reduce fault tolerance and disrupt consensus processes, particularly in permissioned and Byzantine Fault Tolerant systems requiring minimum validator participation thresholds [2], [30]. Development indicators reported by the United Nations Development Programme highlight persistent electricity reliability challenges in emerging economies, reinforcing energy stability as a core component of system resilience.

6.3 Digital Divide and Accessibility

Deployment feasibility is further influenced by disparities in digital literacy, device ownership, and secure system usability [60]. Blockchain voting interfaces that require complex cryptographic interaction may introduce usability barriers that reduce participation or increase operational error [15], [25]. Consequently, infrastructure readiness encompasses both technical capacity and user accessibility conditions.

6.4 Governance and Institutional Capacity

Permissioned and hybrid blockchain voting systems introduce governance responsibilities including validator management, protocol maintenance, and incident response coordination [44], [61]. Institutional capability therefore directly influences system trustworthiness and operational security, particularly in national electoral contexts.

6.5 Infrastructure-Aware Architectural Adaptation

Recent research proposes infrastructure-resilient design strategies such as lightweight clients, intermittent synchronization models, and decentralized communication frameworks to accommodate heterogeneous deployment environments [29], [55], [57]. Hybrid architectures integrating performance optimization with environmental adaptation are frequently identified as the most viable pathway toward deployment feasibility in emerging democracies [39], [16].

6.6 Deployment Feasibility Synthesis

Across the literature, system viability emerges from the interaction between architectural design, scalability mechanisms, and infrastructural capacity rather than from any single technical innovation. Accordingly, blockchain-based voting is increasingly conceptualized as a socio-technical infrastructure system requiring coordinated optimization of performance, governance, and environmental resilience [36], [59].

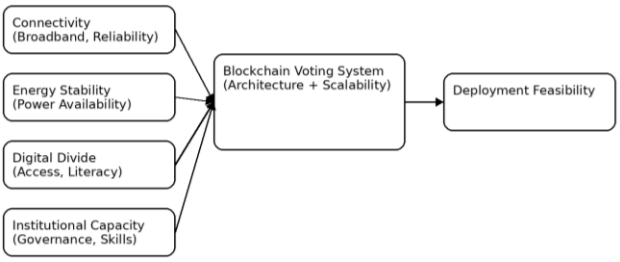
Connectivity (Broadband, Reliability)
Energy Stability (Power Availability)
Digital Divide (Access, Literacy)
Institutional Capacity (Governance, Skills)
Blockchain Voting System (Architecture + Scalability)
Deployment Feasibility

Fig. 6.3: Infrastructural Constraints and Deployment Feasibility

VII. SECTION VII: RESEARCH GAPS AND EMERGING DIRECTIONS

Despite extensive research on blockchain-based electronic voting, several critical limitations persist across the literature.

First, most proposed systems remain conceptual or experimentally validated at limited scale. Empirical evidence evaluating system behavior under national electoral workloads, heterogeneous infrastructure conditions, and institutional governance constraints remains scarce [15], [61]. The field therefore lacks deployment-validated architectural models.

Second, a persistent scalability-security tension remains unresolved. Privacy-preserving cryptographic mechanisms such as homomorphic encryption and zero-knowledge proofs introduce computational overhead that constrains throughput and latency, while high-performance consensus protocols often require governance centralization [18], [42], [25]. Integrated optimization of privacy, verifiability, and performance remains an open research problem.

Third, infrastructural conditions are frequently treated as external assumptions rather than system design parameters. Most architectures presume stable connectivity, continuous power availability, and homogeneous user capabilities, assumptions inconsistent with deployment realities in emerging democracies [8], [63], [57]. Infrastructure-aware architectural design remains underdeveloped.

Fourth, governance and institutional capacity receive limited analytical attention despite their central role in trust formation, validator management, and system oversight [56], [7], [44]. Technical security guarantees alone do not ensure operational legitimacy.

Finally, evaluation methodologies remain fragmented across studies, limiting comparability and cumulative knowledge development [58], [34].

Collectively, the literature indicates a shift toward deployment-oriented research emphasizing hybrid architectures, performance-aware privacy mechanisms, infrastructure-resilient communication models, and governance-integrated system design. Advancing blockchain-based electronic voting requires unified evaluation frameworks and empirical studies conducted under realistic electoral and infrastructural conditions.

VIII. CONCLUSION

This paper presented a structured critical review of blockchain-based electronic voting systems with emphasis on scalability, security, and infrastructural deployment constraints in emerging democracies. The synthesis shows that while blockchain enhances auditability, transparency, and tamper resistance, these properties alone do not ensure practical deployability at national scale.

Across the literature, system feasibility is shaped by the interaction between architectural design, consensus performance, governance structure, and infrastructural readiness. Persistent throughput limitations, consensus overhead, and privacy-related computational costs constrain large-scale implementation, while connectivity instability, energy reliability, and digital access disparities introduce operational risks. Consequently, deployment viability cannot be assessed solely through cryptographic or protocol-level analysis.

Evidence across reviewed studies indicates that hybrid architectures combining controlled high-performance validation with publicly verifiable audit mechanisms represent the most frequently proposed pathway toward scalable deployment, though empirical validation remains limited. The literature further highlights the need for infrastructure-aware system design and governance-integrated evaluation models.

Future progress depends on deployment-oriented research integrating performance engineering, privacy preservation, infrastructural resilience, and institutional capacity. By framing blockchain voting as a socio-technical infrastructure challenge rather than a purely cryptographic system, this review provides a consolidated foundation for developing scalable and context-appropriate electronic voting systems.

REFERENCES

[1] Abayomi-Zannu, T. P., Odun-Ayo, I. A., & Barka, T. F. (2019). A proposed mobile voting framework utilizing blockchain technology and multi-factor authentication. *Journal of Physics: Conference Series, 1378*(3), 032104.

[2] Abuidris, Y., Kumar, R., Yang, T., & Onginjo, J. (2021). Secure large-scale e-voting system based on blockchain contract using a hybrid consensus model combined with sharding. *ETRI Journal, 43*(2), 357–370.

[3] Adeleke, R. (2021). Digital divide in Nigeria: The role of regional differentials. *African Journal of Science, Technology, Innovation and Development, 13*(3), 333–346.

[4] Aker, J. C., & Mbiti, I. M. (2010). Mobile phones and economic development in Africa. *Journal of Economic Perspectives, 24*(3), 207–232.

[5] Akyildiz, I. F., Wang, X., & Wang, W. (2005). Wireless mesh networks: A survey. *Computer Networks, 47*(4), 445–487.

[6] Al-Madani, A. M., Gaikwad, A. T., Mahale, V., & Ahmed, Z. A. (2020). Decentralized e-voting system based on smart contract using blockchain technology. In *Proceedings of ICSIDEMPC 2020* (pp. 176–180).

[7] Alvarez, R. M., Hall, T. E., & Llewellyn, M. H. (2008). Are Americans confident their ballots are counted?. The Journal of Politics, 70(3), 754-766.

[8] Alvarez, R. M., Hall, T. E., & Trechsel, A. H. (2009). Internet voting in comparative perspective: the case of Estonia. *PS: Political Science & Politics*, *42*(3), 497-505.

[9] Androulaki, E., Barger, A., Bortnikov, V., Cachin, C., Christidis, K., De Caro, A., ... & Yellick, J. (2018, April). Hyperledger fabric: a

distributed operating system for permissioned blockchains. In Proceedings of the thirteenth EuroSys conference (pp. 1-15).

[10] Antal, C., Cioara, T., Anghel, I., Antal, M., & Salomie, I. (2021). Distributed ledger technology review and decentralized applications development guidelines. *Future Internet*, *13*(3), 62.

[11] Anwar ul Hassan, C., Hammad, M., Iqbal, J., Hussain, S., Ullah, S. S., AlSalman, H., & Arif, M. (2022). A liquid democracy enabled blockchain-based electronic voting system. *Scientific Programming, 2022*, 1–10.

[12] Apeh, A. J., Ayo, C. K., & Adebiyi, A. (2021). A scalable blockchain implementation model for nationwide electronic voting system. In *Computational Science and Its Applications* (pp. 84–100). Springer.

[13] Asongu, S. A., & Le Roux, S. (2017). Enhancing ICT for inclusive human development in Sub-Saharan Africa. *Technological Forecasting and Social Change, 118*, 44–54.

[14] Bartolucci, S., Lenzini, G., & Petrocchi, M. (2018). SHARVOT: Secret share-based voting on the blockchain. In *IEEE IoTSMS 2018* (pp. 218–225).

[15] Benabdallah, A., Audras, A., Coudert, L., El Madhoun, N., & Badra, M. (2022). Analysis of blockchain solutions for E-voting: a systematic literature review. IEEE Access, 10, 70746-70759.

[16] Berenjestanaki, S. M., Daneshgar, F., & Bagheri, A. (2024). Blockchain-based e-voting systems: A technology review. *Computers & Security, 138*, 103583.

[17] Brewer, E. (2012). CAP twelve years later: How the" rules" have changed. Computer, 45(2), 23-29.

[18] Cachin, C., & Vukolić, M. (2017). Blockchain consensus protocols in the wild. *arXiv preprint arXiv:1707.01873*.

[19] Croman, K., Decker, C., Eyal, I., et al. (2016). On scaling decentralized blockchains. In *Financial Cryptography and Data Security* (pp. 106–125). Springer.

[20] Dang, H., Dinh, T. T. A., Loghin, D., Chang, E. C., Lin, Q., & Ooi, B. C. (2019). Towards scaling blockchain systems via sharding. In *Proceedings of the ACM SIGMOD Conference* (pp. 123–140).

[21] Darmawan, I. (2021). E-voting adoption in many countries: A literature review. *Asian Journal of Comparative Politics, 6*(4), 482–504.

[22] Devi, U., & Bansal, S. (2022, December). Secure e-Voting System—A Review. In International Conference on Hybrid Intelligent Systems (pp. 1209-1224). Cham: Springer Nature Switzerland.

[23] Dhulavvagol, B., Patil, P., Naik, N., & Patil, V. (2020). Blockchain Ethereum clients performance analysis considering e-voting application. In *ESCI 2020* (pp. 285–289).

[24] Donepudi, S., & Reddy, K. T. (2021). Hyperledger-based performance-driven framework for mass e-voting. *Intelligent Decision Technologies, 15*(4), 579–589.

[25] Gandhi, S. K., Kumar, S., Kaur, G., Kaur, H., & Gupta, S. (2022). Security requirement analysis of blockchain-based e-voting systems. In *ICICCS 2022* (pp. 1553–1560).

[26] Gervais, A., Karame, G. O., Wüst, K., et al. (2016). On the security and performance of proof-of-work blockchains. In *ACM CCS 2016* (pp. 3–16).

[27] Gibson, J. P., Krimmer, R., Teague, V., & Pomares, J. (2016). A review of e-voting: The past, present and future. *Annals of Telecommunications, 71*, 279–286.

[28] Goulet, J., & Zitelli, J. (2017). Surveying and improving electronic voting schemes. CSE400_20042005/senior_design_projects_04_05.htm.

[29] Gupta, S., Gupta, K. K., Shukla, P. K., & Shrivas, M. K. (2022, March). Blockchain-based voting system powered by post-quantum cryptography (BBVSP-PQC). In 2022 Second International Conference on Power, Control and Computing Technologies (ICPC2T) (pp. 1-8). IEEE.

[30] Hafid, A., Hafid, A. S., & Samih, M. (2020). Scaling blockchains: A comprehensive survey. *IEEE Access, 8*, 125244–125262.

[31] Hardwick, F. S., Gioulis, A., Akram, R. N., & Markantonakis, K. (2018). E-voting with blockchain: An e-voting protocol with decentralisation and voter privacy. In *IEEE iThings 2018* (pp. 1561–1567).

[32] Hevner, A. R., March, S. T., Park, J., & Ram, S. (2004). Design science in information systems research. *MIS Quarterly, 28*(1), 75–105.

[33] Hjálmarsson, F. Þ., Hreiðarsson, G. K., Hamdaqa, M., & Hjálmtýsson, G. (2018). Blockchain-based e-voting system. In *IEEE CLOUD 2018* (pp. 983–986).

[34] Huang, H., Kong, W., Zhou, S., Zheng, Z., & Guo, S. (2021). A survey of state-of-the-art on blockchains: Theories, modelings, and tools. ACM Computing Surveys (CSUR), 54(2), 1-42.

[35] International Telecommunication Union. (2023). Measuring digital development: Facts and figures 2023.

[36] ITU (2022). *Measuring Digital Development: Facts and Figures*. International Telecommunication Union.

[37] Jafar, U., Ab Aziz, M. J., Shukur, Z., & Hussain, H. A. (2022). A systematic literature review and meta-analysis on scalable blockchain-based electronic voting systems. *Sensors, 22*(19), 7585.

[38] Jafar, U., Aziz, M. J. A., & Shukur, Z. (2021a). Blockchain for electronic voting system - review and open research challenges. Sensors, 21(17), 5874.

[39] Jafar, U., & Aziz, M. J. A. (2021b). A state of the art survey and research directions on blockchain based electronic voting system. In Advances in Cyber Security: Second International Conference, ACeS 2020, Penang, Malaysia, December 8-9, 2020, Revised Selected Papers 2 (pp. 248-266). Springer Singapore.

[40] Khan, K. M., Arshad, J., & Khan, M. M. (2020). Investigating performance constraints for blockchain-based secure e-voting system. *Future Generation Computer Systems, 105*, 13–26.

[41] Kho, Y. X., Heng, S. H., & Chin, J. J. (2022). A review of cryptographic electronic voting. *Symmetry*, *14*(5), 858.

[42] Kim, M., Lee, W., & Kim, H. K. (2021). E-voting system using homomorphic encryption and blockchain technology. *Electronics, 10*(23), 3030.

[43] Kokoris-Kogias, E., Jovanovic, P., Gasser, L., Gailly, N., Syta, E., & Ford, B. (2018). Omniledger: A secure, scale-out decentralized ledger via sharding. In *IEEE Symposium on Security and Privacy* (pp. 583–598).

[44] Kshetri, N., & Voas, J. (2018). Blockchain-enabled e-voting. *IEEE Software, 35*(4), 95–99.

[45] Lai, R., Zhao, G., He, Y., & Hou, Z. (2023). A robust sharding-enabled blockchain for MANETs. *Applied Sciences, 13*(15), 8726.

[46] Liu, Y., Liu, J., Salles, M. A. V., Zhang, Z., Li, T., Hu, B., & Lu, R. (2022). Building blocks of sharding blockchain systems. *Computer Science Review, 46*, 100513.

[47] Luu, L., Narayanan, V., Zheng, C., Baweja, K., Gilbert, S., & Saxena, P. (2016). A secure sharding protocol for open blockchains. In *ACM CCS 2016* (pp. 17–30).

[48] McCorry, P., Shahandashti, S. F., & Hao, F. (2017, April). A smart contract for boardroom voting with maximum voter privacy. In International conference on financial cryptography and data security (pp. 357-375). Cham: Springer International Publishing.

[49] Mpekoa, N., & van Greunen, D. (2017, May). E-voting experiences: A case of Namibia and Estonia. In 2017 IST-Africa Week Conference (IST-Africa) (pp. 1-8). IEEE.

[50] Nasir, M. H., Arshad, J., Khan, M. M., Fatima, M., Salah, K., & Jayaraman, R. (2022). Scalable blockchains: A systematic review. *Future Generation Computer Systems, 126*, 136–162.

[51] National Academies of Sciences, Engineering, and Medicine. (2018). *Securing the vote: Protecting American democracy*. National Academies Press.

[52] Noizat, P. (2015). Blockchain electronic vote. In *Handbook of Digital Currency* (pp. 453–461). Academic Press.

[53] Odusanya, K., & Adetutu, M. (2020). Determinants of Internet usage in Nigeria. In *Responsible Design and Implementation of ICT* (pp. 307–318). Springer.

[54] Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology. *Journal of Management Information Systems, 24*(3), 45–77.

[55] Russo, A., Anta, A. F., Vasco, M. I. G., & Romano, S. P. (2021). Chirotonia: A scalable and secure e-voting framework. In *IEEE Blockchain Conference* (pp. 417–424).

[56] Saltman, R. (2006). The History and Politics of Voting Technology. Palgrave.

[57] Sanka, A. I., & Cheung, R. C. C. (2021). A systematic review of blockchain scalability. *Journal of Network and Computer Applications, 195*, 103232.

[58] Taş, R., & Tanrıöver, Ö. Ö. (2020). A systematic review of blockchain for e-voting. *Symmetry, 12*(8), 1328.

[59] Truby, J. (2018). Decarbonizing Bitcoin: Law and policy choices for reducing the energy consumption of Blockchain technologies and digital currencies. Energy research & social science, 44, 399-410.

[60] van Dijk, J. (2020). *The digital divide*. Polity Press.

[61] Vladucu, M. V., Dong, Z., Medina, J., & Rojas-Cessa, R. (2023). E-voting meets blockchain: A survey. *IEEE Access, 11*, 23293–23308.

[62] Wang, G., Shi, Z. J., Nixon, M., & Han, S. (2019). Sok: Sharding on blockchain. In *ACM Advances in Financial Technologies* (pp. 41–61).

[63] World Bank. (2022). World development report 2022: Finance for an equitable recovery.

[64] Xie, J., Tang, H., Huang, T., Yu, F. R., Xie, R., Liu, J., & Liu, Y. (2019). Blockchain technology applied to smart cities. *IEEE Communications Surveys & Tutorials, 21*(3), 2794–2830.

[65] Zamani, M., Movahedi, M., & Raykova, M. (2018). RapidChain: Scaling blockchain via full sharding. In *ACM CCS 2018* (pp. 931–948).

[66] Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology. In *IEEE International Congress on Big Data* (pp. 557–564).

[67] Zhou, Q., Huang, H., Zheng, Z., & Bian, J. (2020). Solutions to scalability of blockchain. *IEEE Access*, *8*, 16440–16455.