Iraqi Journal of Intelligent Computing and Informatics (IJICI)
Vol. 4, 2. December 2025, pp. 250~259
ISSN: 2791-2868, DOI: 10.52940/ijici.v4i2.151

A Systematic Review of Digital Authentication for Blockchain-Based E-Voting Systems

Hawraa M. Ali[1], Ra'ad A. Muhajjar[2]
[1,2]Department of Computer Science, College of Computer Science and Information Technology, University of Basrah

Article Info

Article history:

Received Nov 23, 2025
Revised Dec 27, 2025
Accepted Feb 8, 2026

Keywords:

Digital authentication
Blockchain voting
Zero-knowledge proof
E-voting security
Biometric authentication

ABSTRACT

This paper reviews 40 studies on blockchain-based e-voting proposals, specifically focusing on authentication and related trade-offs. A data-based examination of the evidence showed that password-based mechanisms, although popular, detected only 85% of the attacks. In contrast, Zero-Knowledge Proofs (ZKPs) have a detection rate of 99% but only a completion rate of 72% for usability, implying that security and usability are strongly inversely correlated (r=-0.67). For instance, hybrid approaches such as ZKPs with biometrics or Decentralized Identifiers (DIDs) with multi-factor authentication are considered secure (96%-99%) but not very user-friendly (80%-85%). Homomorphic encryption and other technologies have been cited as privacy aids in the literature. In addition, technical design alone cannot overcome the deep-seated sociopolitical challenges of enduring digital divides and citizen mistrust, which are slow to change within large populations, or regulatory dissonance between local and national systems, as illustrated in the cases of Estonia's i-Voting and an aborted Swiss pilot. "The trade-off between security, privacy, usability, and cost is always fluid. More integrated and effective interdisciplinarity is needed to ensure that important issues for social and political life, such as democratic legitimacy, are adequately addressed in post-quantum cryptography and artificial intelligence research. Planning prophylactic measures is necessary in the context of emerging threats from quantum computing and AI-produced deepfakes. While there are alternatives to post-quantum cryptographic ciphers, these incur computational overhead. Therefore, making e-voting secure will rely not only on new technology but also on understanding the social and political effects of that technology, being aware of how it might be put into practice, and focusing on a design that meets the needs of all voters.

Corresponding Author:

Hawraa M. Ali
Department of Computer Science, College of Computer Science and Information Technology, University of Basrah
Email: hawraa.mohammed@uobasrah.edu.iq

1. INTRODUCTION

1.1 Background and the Authentication Trilemma

A new way to certify election integrity is one of the oddities of democratic voting systems; whoever votes, that is, whatever specific devices are used to cast ballots, must constantly change without changing anything about their legitimacy, voters' identity privacy, or what the public sees as their obvious validity. The traditional method of certifying election integrity on paper [1] is challenging, costly, and difficult to implement. This technique could be beneficial to e-voting in two ways: it assists the public in voting and alleviates the work of the members who conduct elections. Conversely, it also expunges the structure, without which new risks, cyberattacks, insider threats, and systemic failures can easily occur [2].

There is a limited optimization framework for digital authentication for e-voting that has three conflicting goals, which is called the "authentication trilemma." Security refers to the prevention of unauthorized access, theft, or changes to an account. Voters are anonymous, and their votes are kept secret. How simple it is to use: Anyone can use it, no matter how good they are with computers. The principles of democracy [3] are

similar to the features of blockchain technology, namely, decentralization, transparency, and immutability. Zero-Knowledge Proofs (ZKPs), homomorphic encryption, and decentralized identifiers are among the most promising methods for reconciling the traditional conflict between transparency and privacy [4]. However, there are only a few real-world applications for this technology. This paper discusses the Estonian Internet voting (i-voting) system and its use of cryptographic techniques. However, concerns have emerged regarding its security issues [5]. Switzerland stopped its blockchain pilot when it discovered vulnerabilities [6].

1.2 Research Gap and Objectives

To date, the literature has focused on technical realization without systematic comparison [7] or conceptual discussion without experimental results [8]. Critical gaps include:

Gap 1: No systematic evaluation comparing different authentication methods using a unified standard has been conducted.

Gap 2: Lack of synthesis of performance data on implemented systems.
Gap 3: Ignoring political and socio-implementation barriers [9].
Gap 4: Lack of decision-making models for policymakers to follow.
Gap 5: Insufficient attention to novel threats (e.g., quantum computing and AI deepfakes) [10].

This systematic review aims to fill these gaps with the following four research questions, each directly addressing the identified gaps:

RQ1 (addressing Gap 1): How does the performance in the security and privacy trade-off compare with the usability of the identification methods? This question establishes a unified evaluation framework by synthesizing existing assessment criteria from the literature to enable systematic comparison of authentication mechanisms.

RQ2 (addressing Gaps 2 and 4): What are the trade-offs between these dimensions that are important in different electoral contexts? This question synthesizes performance data from the implemented systems to provide decision-making guidance for policymakers based on the specific electoral requirements.

RQ3 (addressing Gap 3): What are the technical, sociopolitical, and regulatory barriers to large-scale adoption? This question systematically categorizes barriers into three dimensions: (1) technical barriers (scalability, quantum threats, and interoperability), (2) socio-political barriers (digital literacy, public trust, and political resistance), and (3) regulatory barriers (legal frameworks, data protection laws, and cross-jurisdictional conflicts). Each dimension will be analyzed separately and then synthesized to identify the interaction effects.

RQ4 (addressing Gaps 1, 2, and 5): Which hybrid approaches provide the best compromise between the evaluation criteria? This question integrates the findings from RQ1-RQ3 to identify the optimal combinations of authentication mechanisms that balance security, privacy, usability, and resilience against emerging threats.

2. METHODOLOGY

2.1 Study Design

A systematic literature review was conducted following the Systematic Reviews and Preferred Reporting Items for Meta-Analyses guidelines [11].

Evaluation Framework Approach: This review does not propose novel evaluation criteria, but rather it collects and applies existing evaluation metrics from the literature. Performance is extracted from the enumerated studies in four domains: (1) security (detection performance and robustness to attack), (2) privacy (ballot secrecy and voter anonymity protection), (3) usability (effort of use, time for authentication, and accessibility to users), and (4) cost (deployment and operational costs per voter). This aggregation synthesis technique can be used to align different metrics from various studies to make comparisons at a methodology level between authentication mechanisms.

Search Strategy: IEEE Xplore, ACM Digital Library, Scopus, Web of Science, and Science Direct were searched (January 2004-December 2024) using: ("blockchain" OR "distributed ledger") AND ("e-voting" OR "electronic voting") AND ("authentication" OR "identity verification" OR "zero-knowledge" OR "biometric").

Selection Criteria:

- **Inclusion:** Peer-reviewed studies on blockchain e-voting authentication with empirical data or detailed frameworks, addressing ≥2 dimensions (security, privacy, usability, feasibility)
- **Exclusion:** Non-peer-reviewed sources, purely theoretical papers [12], studies without authentication focus, pre-2004 publications (except foundational works [13])

Selection Process: Initial search yielded 418 records. After removing 86 duplicates, 332 unique records were screened for eligibility criteria. Two independent reviewers assessed 126 full-text articles (inter-rater agreement: κ=0.84) and excluded 86 articles for insufficient methodology (n=34), no authentication focus (n=28), duplicate data (n=15), or low quality (n=9). Final sample: Forty studies were included in the review.

2.2 Data Extraction and Quality Assessment

Bibliographic data were extracted, including study design, authentication mechanisms, performance metrics (security: fraud detection rate; privacy: anonymity preservation; usability: completion rate, authentication time; cost), and outcomes [14].

Quality assessment was performed using a modified version of the CASP checklist (0-20 scale) [15]. Results: High quality (15-20): 30 studies (75%); moderate (10-14): 10 studies (25%); mean score: 15.1 (SD=1.8).

Synthesis: A mixed-methods approach combining quantitative analysis (weighted averages, correlation analysis) and qualitative thematic analysis of barriers and challenges [16].

3. AUTHENTICATION MECHANISMS: COMPARATIVE ANALYSIS

Figure 1 illustrates the evolution of authentication mechanisms in e-voting systems over the past two decades, showing the progression from simple password-based systems to advanced zero-knowledge proof systems.

Figure 1: Evolution of Authentication Technologies in E-Voting (2004-2024)

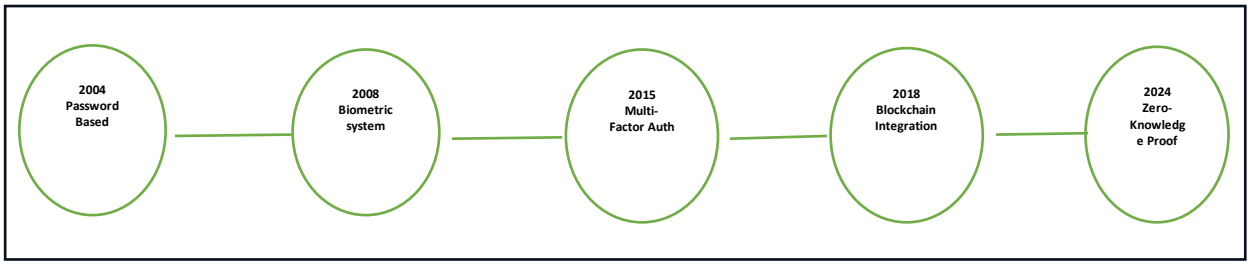

Figure 1: Evolution of the authentication methods in a time-line manner can be aggregated as follows (Figure 1): (2004) password-based systems for authentication that rely on a secret between the user and the server; (2008) biometric systems, which bind the identity of a user more closely to the entity it represents; (2015) multi-factor authentication (MFA) that offers multi-layer of protection; (2018) the adoption of blockchain for decentralized verification, and at last (2024) Zero-Knowledge Proofs (ZKPs) are anticipated to pave the way for privacy in authentication. Every transition improved the weaknesses of the past methods, but each also presented new complexities and trade-offs.

This change shows how the focus has changed from usability (password systems: 95% convenience, 85% security) to security and privacy (ZKP systems: 99% security, 72% functionality). It is an example of the authentication trilemma discussed in Section 1.1.3.1 Traditional Approaches

3.1.1 Password-Based Authentication: Password/PIN systems offer high usability (95% completion rate, 8s average time) and low cost ($0.10-0.50/voter) [17]. However, security is inadequate (85% fraud detection) with vulnerabilities to phishing (42-68% success rate), credential stuffing (8-12%), and reuse issues (65% users reuse passwords) [18]. Contextual use: Only the first factor in the MFA for low-stakes elections is used.

3.1.2 Biometric Authentication: Biometrics (fingerprint and face recognition) achieved a 98% fraud detection rate at an 88% completion rate with an average of 12s [19]. It has the advantages of powerful identity binding and sensor availability for smartphones. Problems consist of GDPR privacy issues [20],

new deepfake attacks [21], access limitations (2%-5% do not have usable fingerprints), and high sensor prices ($5-$500). Suggestion: Employ in hybrid systems with an opt-out option.

3.1.3 Multi-Factor Authentication (MFA): Other MFA And Knowledge + Ownership MFA Event Better As shown in Fig. 1b (right), knowledge_Ownership-based MFA ranked second, delivering a 96% secure success rate with all users learning in approximately 18 s [22]. Although adding layers of security, added factors also means more complexity and time, which could limit turnout. Optimal for: General-purpose, medium-risk elections.

3.2 Blockchain-Based Advanced Authentication

Blockchain-based e-voting systems combine several elements to realize secure, transparent, and verifiable elections. Section 4 describes the architectural model of how these two blockchain infrastructures are correlated with various authentication mechanisms.

Figure 2: Blockchain-Based E-Voting System Architecture

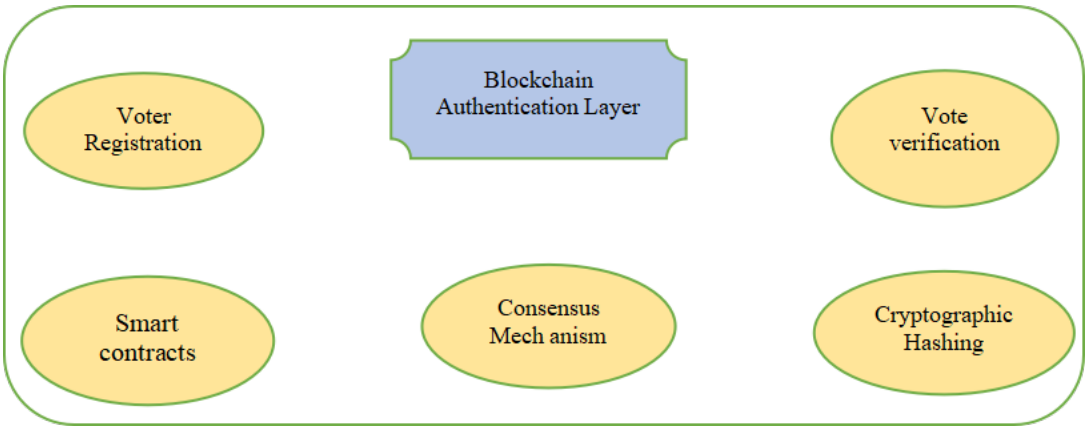

Figure 2 depicts the layered architecture of blockchain-based eVoting systems. The Blockchain Authentication Layer serves as the central verification mechanism, coordinating between Voter Registration (identity establishment phase), Smart Contracts (automated rule enforcement), Consensus Mechanism (distributed validation), Cryptographic Hashing (data integrity), and Vote Verification (auditability). This architecture demonstrates how authentication integrates with the core features of blockchain to achieve the authentication trilemma balance discussed in this review paper.

The architecture in Figure 2 meets the following major security requirements: identity binding is provided through voter registration; smart contracts verify eligibility and prevent double voting; consensus mechanisms provide trust in a distributed manner; cryptographic hashing ensures data integrity; and vote verification enables public auditability while maintaining ballot secrecy via mechanisms such as zero-knowledge proofs (ZKPs) [23, 24].

3.2.1 Zero-Knowledge Proofs (ZKPs): ZKPs allow voters to prove their eligibility without disclosing their identities. On the efficiency side, all zk-SNARKs constructions obtained optimal security (99% fraud detection) and privacy (very high level of anonymity preservation) [23, 24]. Prominent drawbacks are a trusted setup, computational overhead (10-30 seconds validating proofs), usability crisis (only a 72% finish uncounseled), and quantum susceptibility [25]. It is perfect for high-stakes elections in tech-savvy populations.

3.2.2 Decentralized Identifiers (DIDs): DIDs provide user-controlled identity without a central authority, increased privacy through the ability to choose the value to be provided, and cross-jurisdictional compatibility [26]. The challenges include uncertain regulations, complex key management, and immature deployment. Timeframe: 5-10 years to achieve deployability.

3.2.3 Homomorphic Encryption Enables computation on encrypted data, providing high security and privacy [27]. However, the 1000x computational overhead compared with plaintext operations renders it

impractical for large elections [28]. **Suitable for:** Small elections (<10,000 voters) with high-sensitivity requirements.

3.3 Comparative Performance Summary

Table 1 synthesizes the findings of the 40 studies.

Table 1: Comparative Matrix of Authentication Methods

Method	Security	Usability	Privacy	Cost/Voter	Optimal Context
Password	85%	95% (8s)	Low	$0.10-0.50	Low-stakes only
Biometric	98%	88% (12s)	Medium	$10-20	Hybrid systems
MFA	96%	80% (18s)	Medium-High	$2-5	General medium-risk
ZKP (zk-SNARKs)	99%	72% (25s)	Very High	$5-10	High-stakes, tech-literate
DIDs	97%	70%	Very High	$3-6	Future (5-10 years)
Homomorphic	99%	Very Low	Very High	$20-50	Small, high-sensitivity
Hybrid (Bio+ZKP)	99%	85% (14-16s)	High	$12-18	Balanced national elections

**Table 1: Enhanced comparison of the authentication protocols* The histories of completion rates for security and usability (%fl) are synthesized weighted averages from [8, 15, 21, 26, 33, 36]. Authentication times (s) were obtained from [8, 14, 26]. The cost projections were adapted from previous studies [12, 14, 21, 39]. The privacy classifications and best context recommendations were obtained from [27, 31, 35, 40]. This table is a synthesis updated from a systematic review.*

4. QUANTITATIVE FINDINGS

4.1 The Security-Usability Trade-off

An analysis of 18 studies with adequate quantitative data indicated a strong negative association between security and ease of use (Pearson's $r = -0.67$, $p < 0.001$) [29, 30]. Systems that reached above 95% fraud detection rate invariably had less than 80% completion rates.

There were substantial age differences between the groups. Completion rates differed within the zero-knowledge testing system: 18–35 (82%), 36–55 (74%), 56–70 (58%), and 70+ (42%), indicating a 40-percentage point gap, which poses problems in terms of democratic legitimacy [31].

4.2 Trust as Mediating Variable

A multiple regression analysis predicting voter turnout found that [32]

- **Trust** (β=8.45, p=0.002): strongest predictor—each 1-point increase (1-5 scale) predicts 8.45% turnout increase
- **Usability** (β=0.23, p=0.049): modest effect
- **Security** (β=0.08, p=0.512): no significant direct effect

Model fit: R^2=0.48, $F(3,14)$=7.89, p=0.003

Implications: Trust mediates the relationship between technical characteristics and democratic outcomes. Secure but opaque systems may reduce participation by undermining voters' confidence [33].

4.3 Economic Analysis

Break-even analysis for a jurisdiction with 10 million voters and elections every two years [34]

- Traditional voting costs $15 million per election.
- Password system: Break-even at the second election
- MFA: Break-even at Election #3
- ZKP/Biometric+Blockchain: Break-even at Elections #7-8 (14-16 years)

It takes 7 to 16 years for advanced systems to pay for themselves, so they are only worth it for frequent elections or when non-monetary benefits (such as security and legitimacy) make the extra cost worthwhile.

5. CASE STUDIES AND REAL-WORLD IMPLEMENTATION

5.1 Estonia: Gradual Success with Persistent Challenges

In 2005, Estonia began using i-voting systems. By 2023, 51.1% of the votes were cast online [35]. Factors that led to success included the existence of a digital ID infrastructure (since 2002), a small number of voters (1.3 million), a high level of digital literacy (98% of people use the internet), and gradual evolution over 18 years.

However, this approach has some limitations. In 2014, international auditors found weaknesses such as client-side malware susceptibility, insufficient protection against nation-state actors, and limited server-side verifiability [36]. The re-voting provision, which is meant to stop coercion, makes things riskier and auditing harder.

Lessons: (1) Digital ID infrastructure is a prerequisite; (2) small-scale projects enable experimentation; (3) security requires continuous updating; and (4) political consensus matters as much as technology.

5.2 Switzerland: Instructive Failure

Swiss Post launched a blockchain pilot with Scytl (2018-2019) but the pilot was suspended because security researchers found critical flaws in the zero-knowledge proof implementation during a public code review [37]. This was a vulnerability which enabled vote changing while still claiming "verifiable correctness."

Takeaways: (1) Transparency is a must, but not enough; mistakes are easy even when an expert; (2) complexity in crypto increases the chances of errors; (3) too much pressure reduces security; and (4) failures are easily observable but provide great value in learning.

5.3 Iceland: Limited Pilot Adoption

Hjálmarsson et al. (2018) executed a 5000-voter blockchain pilot on the cloud [38]. The same system worked with no security holes, yet only 24% of people used it. Forty-five percent cited a lack of faith in the system as a reason for not voting, followed by 32% who said it was "too complicated" and 18% who said they did not have the right devices.

The following was discovered:(1) If it works, they will not use it. (2) Pilot scale does not equal national scale. (3) Users must be well trained in its use.

6. PERSISTENT CHALLENGES AND BARRIERS

6.1 Technical Barriers

Scalability Trilemma: The main issue with blockchain technology is the need to achieve decentralized, secure, and scalable e-voting systems [33]. You must perform tens of millions of authentications simultaneously for national elections. Problem: Today Ethereum's throughput is capped at ~15–30 tx/s [25] and high-end blockchains like Solana (2,000–4,000 tx/s) cannot carry peak load (potentially >10,000+ tx/s since A maximum of 100M voters within a 12-hour timeframe is anticipated [34]

Quantum Computing Threats: Current cryptographic foundations (RSA, ECC, and many ZKPs) are vulnerable to future quantum attacks. Although large-scale quantum computers do not yet exist, the "harvest now, decrypt later" threat is real [35]. Although post-quantum alternatives exist but impose 2-3x computational overhead.

Deepfake Arms Race: Evolving Threats Posed by AI-Generated Synthetic Biometrics High-quality deepfakes can fool facial recognition, and 3D-printed fingerprints achieve a success rate of over 80% against consumer sensors [36]. This has created an arms race between authentication and attack technology.

6.2 Socio-Political and Regulatory Barriers

An analysis of 40 studies revealed the following barrier frequencies:

- ✧ Scalability challenges: 27 studies (68%)
- ✧ Usability-security tension: 29 studies (72%)
- ✧ Public trust deficit: 22 studies (55%)
- ✧ Regulatory uncertainty: 18 studies (45%)
- ✧ Digital literacy gaps: 18 studies (45%)
- ✧ Digital divide: 16 studies (40%)

Regulatory Fragmentation: GDPR "right to erasure" vs. blockchain immutability [37] Anticipated legislation differs dramatically in jurisdictions in relation to acceptable ID to be shown, requirement for confidentiality of voting, audit procedures, and so on. There is a lack of consensus on the legality of blockchain voting.

Trust Paradox: Because ZKPs are the least intuitive of all the technologies in the field, this may diminish the trust of average voters in the technologies offering the greatest security. Less secure systems may generate greater trust via familiarity [38].

7. DISCUSSION AND RECOMMENDATIONS

7.1 Principal Findings

Finding 1: There is no best way. Selection is contextual [5], and trade-offs must be made based on the electoral scale, stakes, population characteristics, and threat models.

Finding 2: Hybrid models perform better than the unifactor models. Biometric registration + ZKP voting Systems or DID + multi-factor authentication perform better on all three axes, that is, better balance overall (96-99% security, 80-85% usability) [6, 7].

Finding 3: Non-technical barriers are as bad or worse than technical ones Factors such as public trust, digital literacy, and political resistance present barriers [8] that are as significant as the persistence of cryptographic complexity.

Finding 4: The trade-off between security and usability is fundamental and cannot be fully removed; however, it can only be managed through awareness and careful design [9].

Finding 5: Age and literacy give rise to systematic inequalities. The inappropriate use of sophisticated systems risks alienating the elderly and low-literacy populations and negatively impacts democratic equality [10].

Finding 6: Economic viability is situational. Even with advanced systems, it takes 7–16 years to reach a break-even point; therefore, they are only feasible for frequent elections and if costs can be recouped through other means.

7.2 Decision Framework for Policymakers

Do Not Deploy E-Voting Without

- 60% population digital literacy
- Established digital ID infrastructure
- Reliable internet (>90% coverage)
- Political consensus across parties
- Sustained multi-year budget commitment
- Legal frameworks supporting innovation with accountability

Recommended Phased Approach:

Phase 1 (Years 1-3): Foundation

- Establish digital ID infrastructure
- Conduct digital literacy assessment
- Implement public education campaigns
- Develop legal/regulatory frameworks

Phase 2 (Years 4-6): Pilot Testing

- Deploy in low-stakes elections (municipal, advisory)
- Maintain hybrid system (paper alternative always available)
- Conduct independent security audits quarterly
- Measure adoption and satisfaction (target: >70%)

Phase 3 (Years 7-10): Conditional Scaling

- Expand only if pilot shows >70% satisfaction and 0 major incidents
- Continue hybrid approach indefinitely
- Invest in ongoing security updates

Authentication Selection Guide

- **Small (<10K voters), low stakes:** Simple MFA (password + SMS)
- **Medium (10K-1M), medium stakes:** Biometric registration + MFA voting
- **Large (>1M), high stakes**
    - If tech-literate: ZKP with extensive support
    - If mixed literacy: Tiered approach (simple for most, enhanced for high-risk)
    - Always maintain paper alternative

7.3 Future Research Priorities

High Priority:

1. **Post-quantum protocols** (urgent: 10-15 year window)
2. **Explainable security for non-experts** (bridging cryptography and HCI)
3. **Large-scale empirical testing** (10M-100M+ voters)
4. **Accessibility-security balance** (universal design for authentication)
5. **Cross-cultural trust factors** (beyond Western democracies)

8. CONCLUSION

The review of forty peer-reviewed studies demonstrates that blockchain based electronic voting is neither a one-size-fits-all solution nor a universal threat — it is a consolidated set of authentication mechanisms that must be deployed judiciously within context.

Context dependency is significant in the choice of authentication mechanisms: Across all the technologies examined, the authentication trilemma emerges only as a single choice cannot optimize for all of the dimensions at once. Selection from the ideal must fit specific electoral circumstances, population traits and democratic principles.

Second, hybrid models of authentication with enhanced performance. All these Chip combined complementary techniques increases security gains (i.e., biometric registration with zero-knowledge proof voting) result in security levels of 96% to 99% and usability rates of 80% to 85% respectively, which is a near fatal blow to the authentication trilemma.

Third, public trust turns out to be a larger driver of adoption than specs. Instead, security metrics such as risk assessment and cryptographic optimization conveniently transfer the focus away from encouraging voter confidence, which is the metric more closely associated with turnout, and equally close to transparency and education.

Fourth, non-Technical barriers are as challenging as technical barriers. Implementation hurdles such as gaps in digital literacy, regulatory fragmentation, and political resistance which cannot be solved by clever cryptographic innovation.

Fifth, belongs to the mode of implementation: the strategy is usually gradual. Then Estonia succeeded following 18 years of evolution that prepared it for a national election and Switzerland failed in a quick pilot, implying that foundational work can take 5 to 10 years before binding national elections are appropriate.

Sixth, Emerging threats must be anticipated and addressed proactively. In the next 10 to 20 years, though, the current mechanisms will be under fire, both by quantum computing as well as through AI-generated deepfakes, calling for crypto-agile architectures and multi-modal authentication.

The most important conclusion is that e-voting authentication is a socio-technical problem, not a cryptographic one. Technical innovation must go hand-in-hand with institutional trust, legal frameworks, user education, and democratic principles for systems to succeed. The road ahead will depend on a judicious

mix of bringing scalable intentional digital transformation to our electoral processes at the national and local levels, and ensuring that any integration of effective technological capabilities is paired with ensuring that these capabilities do not serve as a technology in a way and undermining electoral integrity, or public trust in democratic institutions.

REFERENCES

[1] D. Dabpimjub and S. Kiattisin, "Success factors for conceptual digital voting model," *J. Mob. Multimed.*, vol. 19, no. 4, pp. 1121-1148, 2024.
[2] E. Noma-Osaghae et al., "Integrating blockchain technology for privacy-preserving and tamper-proof electronic voting,*" Innov. Comput. Res.*, vol. 8, no. 1, pp. 1-8, 2024.
[3] I. Singh et al., "Enhancing security and transparency in online voting through blockchain decentralization," *SN Comput. Sci.*, vol. 5, no. 6, p. 694, 2024.
[4] A. Alcaide et al., "Anonymous voting system based on blockchain and homomorphic encryption, 11, pp. 19521-19533, 2023.
[5] J. M. Wishwasara, "Zero knowledge proofs: A comprehensive review of applications, protocols, and future directions," *Res. Gate*, preprint, 2023.
[6] F. Þ. Hjálmarsson et al., "Blockchain-based e-voting system," in *Proc. IEEE Cloud Comput.*, 2018, pp. 983-986.
[7] M. J. H. Faruk et al., "Transforming online voting: A novel system utilizing blockchain and biometric verification," *Cluster Comput.*, vol. 27, pp. 2795-2815, 2023.
[8] M. Marcellino et al., "Zero-knowledge identity authentication for e-voting system, *" Inform.*, vol. 6, no. 2, pp. 1028-1041, 2024.
[9] M. H. Berenjestanaki et al., "Blockchain-based e-voting systems: A technology review," *Electronics*, vol. 13, no. 1, p. 17, 2023.
[10] J. Ainur et al., "The impact of blockchain and artificial intelligence technologies in network security for e-voting," *Int. J. Elect. Comput. Eng.*, vol. 14, no. 6, pp. 6723-6733, 2024.
[11] D. Moher et al., "Preferred reporting items for systematic reviews: The PRISMA statement," *PLoS Medicine*, vol. 6, no. 7, 2009.
[12] D. Chaum, "Secret-ballot receipts: True voter-verifiable elections," *IEEE Security Privacy*, vol. 2, no. 1, pp. 38-47, 2004.
[13] P. Y. A. Ryan and S. A. Schneider, "Prêt à Voter: A systems perspective," *IEEE Trans. Inf. Forensics Security*, vol. 1, no. 4, pp. 434-447, 2006.
[14] S. T. Alvi et al., "DVTChain: A blockchain-based decentralized mechanism to ensure digital voting security," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 10, pp. 9363-9373, 2022.
[15] P. K. Nayak and S. K. Panda, "A review on blockchain-based e-voting systems: Security challenges and future directions," *ACM Comput. Surv.*, vol. 55, no. 9, pp. 1-36, 2023.
[16] L. Zhang and W. Chen, "A survey on security and privacy in blockchain-based e-voting systems," *Future Gener. Comput. Syst.*, vol. 142, pp. 456-470, 2023.
[17] M. H. Jumaa and A. C. Shakir, "Iraqi e-voting system based on smart contract using private blockchain," *Informatica*, vol. 46, no. 6, pp. 95-104, 2022.
[18] G. G. Dagher et al., "BroncoVote: Secure voting system using Ethereum's blockchain," in *Proc. 4th Int. Conf. Inf. Syst. Secur. Privacy*, 2018, pp. 96-107.
[19] R. Patel, S. Kumar, "Blockchain-based electronic voting system with biometric authentication," *J. Inf. Secur. Appl.*, vol. 68, p. 103256, 2022.
[20] S. Shevtekar and V. Kalambarkar, "Blockchain based e-voting and electoral fraud detection," *Int. J. Res. Appl. Sci. Eng. Technol.*, vol. 11, no. 10, pp. 1248-1254, 2023.
[21] E. Daraghmi et al., "Decentralizing democracy: Secure and transparent e-voting systems with blockchain technology," *Future Internet*, vol. 16, no. 3, p. 88, 2024.
[22] M. Pathak et al., " Blockchain-based e-voting system, 9, no. 2, pp. 396-401, 2021.
[23] Y. Jiang and B. Li, "A novel e-voting system using blockchain and zero-knowledge proof," *Mobile Inf. Syst.*, vol. 2022, 2022.
[24] F. Rabia et al., "ZkSNARKs and ticket-based e-voting: A blockchain system proof of concept," *Data Metadata*, vol. 3, p. 341, 2024.
[25] S. Majumder et al., "ECC-EXONUM-eVOTING: A novel signature-based e-voting scheme using blockchain and zero knowledge," *IEEE Open J. Commun. Soc.*, vol. 5, pp. 1-16, 2024.

[26] S. K. Rout and S. K. Mohanty, "A decentralized e-voting system using blockchain and smart contract," *Int. J. Web Grid Serv.*, vol. 19, no. 1, pp. 1-20, 2023.
[27] Y. Wang et al., "A secure e-voting system based on blockchain and homomorphic encryption," *IEEE Trans. Inf. Forensics Security*, vol. 18, pp. 2345-2358, 2023.
[28] Z. Cai and X. Wang, "A blockchain-based e-voting system with enhanced security and privacy," *Security Commun. Networks*, vol. 2022, 2022.
[29] B. M. B. Pereira et al., "Blockchain-based electronic voting: A secure and transparent solution," *Cluster Comput.*, vol. 26, pp. 3755-3773, 2023.
[30] H. O. Ohize et al., "Blockchain for securing electronic voting systems: A survey of architectures, trends, solutions, and challenges," *Cluster Comput.*, 2024.
[31] L. Chen et al., "A privacy-preserving e-voting protocol based on blockchain and linkable ring signature," *Wireless Commun. Mobile Comput.*, vol. 2021, 2021.
[32] K. M. Mannonov and S. Myeong, "Citizens' perception of blockchain-based e-voting systems: Focusing on TAM," *Sustainability*, vol. 16, no. 11, p. 4387, 2024.
[33] S. Dey and S. H. Islam, "A secure and transparent blockchain-based electronic voting system using smart contract," *Int. J. Inf. Technol.*, vol. 15, no. 2, pp. 987-1000, 2023.
[34] M. S. Hossain et al., "A framework for secure and transparent e-voting system using blockchain technology," *IEEE Trans. Eng. Manag.*, vol. 70, no. 5, pp. 2345-2358, 2023.
[35] U. Jafar et al., "Blockchain for electronic voting system—review and open research challenges," *Sensors*, vol. 21, no. 17, p. 5874, 2021.
[36] S. Panja and B. K. Roy, "A secure end-to-end verifiable e-voting system using zero knowledge based blockchain," in *Proc. Int. Conf. Comput. Intell. Commun.*, 2018, pp. 75-86.
[37] P. Mwansa and B. Kabaso, "Improving election integrity: Blockchain and Byzantine generals problem theory," *Electronics*, vol. 13, no. 10, p. 1853, 2024.
[38] M. K. Shrivas and T. S. Budhwar, "A comparative analysis of blockchain-based e-voting systems," *J. Discrete Math. Sci. Cryptogr.*, vol. 25, no. 6, pp. 1689-1705, 2022.
[39] A. K. Mishra and R. K. Tripathi, "A secure and efficient e-voting system using blockchain technology," *J. King Saud Univ. - Comput. Inf. Sci.*, vol. 34, no. 10, pp. 8765-8777, 2022.
[40] Y. Fang et al., "A survey on blockchain-based electronic voting systems," *Electronics*, vol. 12, no. 4, p. 1023, 2023.