Rethinking the Ballot Box

Building a Secure, ISO 37301-Aligned Blockchain Voting System

Kenneth William Mayle | ken.mayle@gmail.com | https://kwm59.io

Rev 0 | March 22, 2025

Title:

Rethinking the Ballot Box: Building a Secure, ISO 37301-Aligned Blockchain Voting System

Abstract:

This white paper introduces a new model for secure, anonymous, and verifiable digital voting that aligns with ISO 37301 standards for compliance and governance. The proposed system leverages privacy-preserving cryptography and blockchain immutability to ensure that votes are tamper-proof, untraceable, and individually auditable by each voterwithout relying on centralized trust.

1. Introduction

Modern democracy faces a paradox: we demand transparency and verifiability in elections while also requiring absolute voter anonymity. Traditional systemsboth paper-based and digitalstruggle to provide both. Meanwhile, public trust erodes, and the threat of manipulation, coercion, or disenfranchisement grows. This paper outlines a blockchain-based voting system that addresses these challenges head-on.

2. The Problem Space

- Centralized databases are vulnerable to tampering and surveillance.
- Digital systems often require identifying users, compromising voter anonymity.

- Vote coercion is possible when systems allow vote-tracking or receipts.

- Most systems trade off either verifiability, anonymity, or immutabilityrarely all three.

3. Guiding Principles

- Anonymity: Votes are unlinkable to identities.

- Verifiability: Each voter can confirm their vote was counted.

- Immutability: Once cast, votes cannot be changed or deleted.

- Coercion Resistance: Voters cannot prove how they votedeven if pressured.

- ISO 37301 Alignment: Designed in the spirit of ethical compliance, auditability, and integrity.

4. System Architecture (High-Level)

- Ballot Interface: Touch-based digital interface to select candidates.

- Cryptographic Shield: Vote is anonymized via ring signatures and stealth addressing.

- Immutable Ledger: Vote is recorded in a transparent blockchain ledger.

- Self-Audit Portal: Voter can recognize their own vote via obfuscated metadataonly known to them.

5. Compliance & Governance Alignment

This voting model is structured in alignment with ISO 37301s principles of:

- Ethical governance

- Transparency and accountability

- Traceability of process (not identity)

- Risk-based controls

The system is also philosophically consistent with ISO 19600 (now withdrawn), which emphasized a principles-based compliance model adaptable to emerging technologies.

6. Coercion Resistance by Design

Unlike traditional receipts or vote confirmation codes, this system offers no externally verifiable proof. Only the voter, using personal cryptographic context, can recognize their voterendering vote-buying or intimidation impossible.

7. Privacy & Transparency: Not Opposed

- Public Ledger: Every vote can be seen.
- Private Recognition: Only the voter knows which is theirs.
- Enables independent, crowd-sourced audits without endangering personal privacy.

8. Business Opportunity

This system addresses growing global demand for secure, trusted, and scalable digital voting solutions. Key opportunities include:

- Government pilots in election modernization initiatives
- Licensing for civic platforms and e-democracy apps
- Public-private partnerships with NGOs, oversight bodies, and watchdog groups
- Integration into university and shareholder voting systems
- R&D grants and public sector funding for civic infrastructure and digital trust

9. Implementation Roadmap

- Phase 1: Prototype development and closed simulations
- Phase 2: Testnet launch with real-time vote simulation and feedback collection
- Phase 3: Formal audit and peer review of code and cryptographic processes
- Phase 4: Institutional pilot programs with voting organizations or cooperatives
- Phase 5: Global release as open-source infrastructure and supported SaaS model

10. Environmental & Civic Impact

- Digital Equity: Designed for accessibility and offline-compatible vote casting
- Transparency Without Exposure: Builds trust in institutions without revealing voter identities
- Energy Awareness: Uses lightweight cryptographic techniques, optimized for minimal blockchain bloat and energy use
- Civic Engagement: Encourages participation by making auditing intuitive and verifiable to the individual

11. Future Outlook & Testnet Plans

We plan to release a public demo environment allowing:

- Voters to simulate casting and auditing votes
- Observers to verify tallies on-chain
- Researchers to test system behavior under attack scenarios

12. Call to Collaboration

We invite civic technologists, cryptographers, standards bodies, and ethics scholars to help refine and validate this approach before full deployment.

Appendix: ISO 37301 At a Glance

- Focus: Compliance Management Systems
- Certifiable: Yes
- Relevant Values: Integrity, anti-fraud, auditability
- Link to Voting System: System enforces ethical design through code, not just policy