iJRASET
International Journal For Research in
Applied Science and Engineering Technology

INTERNATIONAL JOURNAL
FOR RESEARCH
IN APPLIED SCIENCE & ENGINEERING TECHNOLOGY

Volume: 13 Issue: I Month of publication: January 2025

DOI: https://doi.org/10.22214/ijraset.2025.66154

Voter Verification in an Election Using Merkle Tree

Utkarsh Srivastava[1], Dr. Suresh Wati[2], Nishant Singh[3], Mr. Suresh Kumar Tiwari[4], Mayank Chaudhary[5]
Department of Design, Data Science & Cyber Security, Greater Noida Institute of Technology (Engg. Institute), Greater Noida, India

Abstract: This paper explores a blockchain-based e-voting system aimed at addressing traditional voting challenges, such as vote tampering, delayed results, and privacy issues. The proposed framework leverages Merkle tree structures for secure, efficient data verification and blockchain's distributed ledger to ensure immutability and transparency.

I. INTRODUCTION

The integrity and transparency of election systems are vital to the democratic process, yet traditional voting mechanisms often face significant challenges. These include vote tampering, delayed results, and the inability to verify individual votes without compromising voter anonymity. Electronic voting machines (EVMs), while a step forward, are not entirely immune to these vulnerabilities. Instances of EVM manipulation, technical malfunctions, and concerns over centralized control have undermined trust in their reliability.

A. Challenges in Traditional Voting Systems

Traditional voting systems, both manual and EVM-based, have exhibited several shortcomings:

1) Vote Tampering: Paper ballots and EVMs are susceptible to tampering, altering election outcomes and eroding public trust.
2) Delayed Results: Manual vote counting is time-intensive and prone to human error, leading to delays in declaring results.
3) Lack of Transparency: In centralized systems, it is challenging for voters to verify that their votes have been accurately counted.
4) High Resource Consumption: Elections often require substantial manpower, infrastructure, and resources, which can be wasteful and inefficient.

B. Need for a Modern Solution

With advancements in technology, blockchain has emerged as a promising tool to address the limitations of traditional voting systems. Blockchain's decentralized nature ensures that no single entity has control over the data, while its immutability guarantees that once votes are recorded, they

cannot be altered. Furthermore, the integration of cryptographic techniques like Merkle trees allows for efficient and secure verification of data.

C. Merkle Trees in Blockchain Voting

The Merkle tree is a fundamental component of blockchain technology, providing a hierarchical structure for data verification. Each "leaf" node in the Merkle tree represents the hash of a voter's transaction (vote), and the non-leaf

nodes store the hash of their child nodes. The root of the tree, known as the **Merkle root**, summarizes the entire dataset. If any data in the tree changes (e.g., a vote is tampered with), the hash at the affected node and its ancestors will also change, immediately signaling an inconsistency.

D. Objectives of the Proposed System

This paper proposes a blockchain-based e-voting system using Merkle trees, with the following objectives:

1) Ensure vote immutability through blockchain's append-only ledger.
2) Provide real-time results while maintaining voter anonymity.
3) Simplify the verification process using Merkle root hashes.
4) Enhance voter confidence by enabling individuals to verify their votes independently.

By leveraging blockchain's decentralized and secure framework, alongside the efficient data verification capabilities of Merkle trees, the proposed system aims to revolutionize the voting process, making it more secure, transparent, and efficient.

II. BACKGROUND

The foundation of the proposed voter verification system relies on two core technologies: blockchain and Merkle trees. This section explains their key concepts, structure, and relevance to secure e-voting systems.

A. Blockchain Technology

1) Definition and Structure

Blockchain is a decentralized, immutable ledger that records transactions across multiple computers. Unlike traditional databases that are centrally controlled, blockchain ensures transparency and security through a distributed framework. The key features of blockchain include:

- Decentralization: No single entity controls the data; it is stored and maintained by a network of nodes.
- Immutability: Once a transaction is recorded in a block, it cannot be altered or deleted.
- Transparency: Each participant in the network can verify and audit the data.

2) Block Structure

Each block in the blockchain contains:

- Transaction Data: In the context of voting, this represents votes cast by individuals.
- Previous Block Hash: A cryptographic link to the preceding block, ensuring chronological order and tamper resistance.
- Merkle Root: A unique hash summarizing all transactions within the block, enabling efficient data verification.
- Nonce and Timestamp: Elements used in validating the block and recording when it was created.

3) Relevance to E-Voting

Blockchain’s properties make it an ideal solution for e-voting. Votes recorded as blockchain transactions are immutable, ensuring the integrity of election results. The decentralized nature eliminates the risk of manipulation by a single authority, while the transparent ledger fosters trust among voters.

B. Merkle Trees

1) Definition and Structure

A Merkle tree is a data structure that uses cryptographic hashes to efficiently summarize and verify a large dataset. It organizes data into a binary tree where:

- Leaf Nodes: Represent the hashed data of individual transactions (e.g., votes).
- Non-Leaf Nodes: Contain hashes derived from their child nodes.
- Root Node (Merkle Root): Represents the unique hash of the entire dataset.

2) Advantages of Merkle Trees

- Efficient Verification: Instead of checking every transaction, only the path from a specific leaf to the root needs to be validated.
- Tamper Detection: If any transaction is altered, the corresponding hash in the tree changes, triggering a mismatch at the root.
- Scalability: Merkle trees handle large datasets efficiently, making them suitable for elections with many voters.

3) Relevance to E-Voting

In the proposed system, each voter’s transaction is hashed and stored in the Merkle tree. The root hash is added to the blockchain, ensuring:

- Votes are tamper-proof.
- Verification is quick and computationally efficient.
- Scalability for elections with millions of voters.

C. Synergy Between Blockchain and Merkle Trees

The integration of Merkle trees into blockchain technology enhances the efficiency and security of data management. In the context of e-voting:

1) Immutable Storage: Blockchain ensures that recorded votes cannot be modified.
2) Efficient Verification: Merkle trees allow quick validation of votes without requiring access to the full dataset.
3) Enhanced Privacy: Voter details are hashed, protecting sensitive information while maintaining transparency.

D. The Need for Blockchain and Merkle Trees in Voting

Traditional voting systems rely heavily on centralized processes, which are vulnerable to:

1) Tampering and Fraud: Centralized systems can be exploited to alter results.
2) Verification Challenges: Ensuring that votes are counted accurately is resource-intensive and often lacks transparency.
3) Lack of Anonymity: Voters' choices may be exposed.

By using blockchain and Merkle trees, the proposed system overcomes these challenges:

- Ensures end-to-end encryption and anonymized data storage.
- Facilitates real-time, transparent results.
- Empowers voters to independently verify their votes.

This synergy between blockchain and Merkle trees forms the backbone of a secure, scalable, and trustworthy e-voting system.

III. METHODOLOGY

The methodology outlines the design and functionality of the proposed blockchain-based e-voting system. It combines cryptographic principles, decentralized processes, and efficient data verification mechanisms using Merkle trees.

A. System Architecture

The system is designed to handle the end-to-end election process, ensuring security, transparency, and efficiency. It includes key roles, components, and processes:

B. Roles

1) Election Administrator

- Responsible for setting up and managing elections.
- Creates and deploys smart contracts for ballot management.
- Oversees voter registration and assigns nodes for blockchain interaction.

2) Voters

- Authenticate themselves using credentials (e.g., Voter ID, OTP).
- Cast votes securely via the decentralized voting app.
- Verify their votes through blockchain records.

3) District Nodes

- Decentralized nodes representing different voting districts.
- Validate transactions and store votes in the blockchain.
- Ensure the integrity of data through consensus mechanisms.

4) Bootnodes

- Help district nodes locate peers and establish network communication.
- Do not store blockchain data, ensuring lightweight operations.

C. Key Processes

1) Voter Registration

- Identity Verification: Voters are authenticated using government-issued IDs (e.g., Aadhar) and mobile OTP verification.

- Wallet Creation: A unique blockchain wallet is created for each voter, containing cryptographic keys used to verify and cast votes.
- Privacy Assurance: Voter identities are hashed to ensure anonymity in the blockchain.

2) Voting Process

a) Accessing the Ballot

- Voters log into the system using their credentials and OTP verification.
- They are redirected to a dashboard displaying the ballot options.

b) Casting a Vote

- Voters select a candidate or party of choice.
- A unique private key is generated and sent to the voter, who uses it to cast their vote.
- Votes are recorded as blockchain transactions and appended to a block after validation by district nodes.

c) Data Validation and Storage

- Votes are hashed and added to a Merkle tree.
- The Merkle root is stored in the blockchain, ensuring tamper-proof storage.

D. Real-Time Results and Verification

1) Votes are tallied in real-time using smart contracts deployed for each district

2) Voters can verify their votes using a transaction ID, which links their vote to the blockchain record without revealing their identity.

E. Merkle Tree Integration

The Merkle tree is used to organize and verify voter transactions efficiently:

1) Hash Computation: Each vote is hashed and stored as a leaf node.

2) Tree Construction: Hashes of leaf nodes are combined to form non-leaf nodes, culminating in a Merkle root.

3) Verification: To validate a vote, only the path from the leaf node (voter's transaction) to the Merkle root is checked, ensuring quick and secure verification.

F. Smart Contracts

Smart contracts automate and enforce the election process:

1) Ballot Management: Create and manage digital ballots for each district.

2) Vote Recording: Validate and store votes on the blockchain.

3) Result Declaration: Count and publish results instantly after the election concludes.

G. Security Features

1) Immutability: Blockchain ensures that once a vote is recorded, it cannot be altered.

2) Anonymity: Voter identities are hashed, and private keys ensure secure transactions.

3) Consensus Mechanisms: District nodes validate transactions collaboratively, preventing unauthorized changes.

4) Tamper Detection: Merkle tree structure allows efficient identification of altered votes by comparing hashes.

H. Workflow Summary

1) Election Setup

- Administrators define election parameters and deploy smart contracts
- Ballots and district nodes are configured.

2) Voter Participation

- Voters authenticate themselves, receive unique credentials, and cast their votes.

3) Blockchain Integration

- Votes are hashed and stored in blocks.
- Merkle roots validate the integrity of each block.

4) Real-Time Results

- Votes are tallied using smart contracts.
- Results are made available immediately after the election.

I. Advantages of the Methodology

1) Real-time results and tamper-proof voting.
2) Scalable for national elections with millions of voters.
3) Secure, transparent, and anonymous.

IV. PROPOSED SYSTEM

The proposed blockchain-based e-voting system introduces a secure and efficient framework for conducting elections. By leveraging blockchain's decentralized structure and Merkle trees for data integrity, the system ensures transparency, privacy, and real-time results.

A. System Design Features

The proposed system incorporates several key features aimed at addressing the limitations of traditional voting methods:

1) Voter Authentication:

- Utilizes government-issued voter IDs and mobile OTP verification for initial authentication.
- Generates a unique private key for each voter, required for casting votes.

2) Blockchain Ledger:

- Stores votes as immutable transactions.
- Records details such as the previous block hash, current block data, and the Merkle root for efficient data verification.

3) Dashboard Interface:

- Provides voters with options to:
- Cast their vote.
- View blockchain transactions.
- Access their profile and update mobile numbers.
- Check real-time election results.

4) Real-Time Tallying:

- Employs smart contracts to automatically count votes as they are recorded.
- Eliminates delays associated with manual counting processes.

5) Transparency and Auditability:

- Voters receive a transaction ID to verify their vote in the blockchain.
- Public access to the blockchain ensures accountability without compromising voter anonymity.

B. Security Mechanisms

The system integrates advanced security measures to protect the integrity and privacy of the voting process:

1) Data Integrity with Merkle Trees:

- Hashes each vote and organizes them into a Merkle tree.
- The Merkle root is stored in the blockchain, enabling efficient tamper detection.

2) Encryption:

- Uses cryptographic techniques to secure voter data and transactions.
- Ensures that only authorized votes are recorded.

3) Immutability:

- Blockchain's append-only nature prevents alteration or deletion of recorded votes.

4) *Consensus Mechanisms:*

- District nodes validate transactions collaboratively, ensuring the integrity of the blockchain.

5) *Voter Anonymity:*

- Hashing voter identities maintains privacy while linking votes to verified user.

C. *Workflow of the Proposed System*

1) *Voter Authentication*

- Voter logs in with a government-issued ID and receives an OTP on their registered mobile number.
- After verification, a unique private key is generated and sent to the voter.

2) *Casting a Vote:*

- Voter selects their candidate/party via the dashboard.
- The vote is hashed and stored as a transaction in the blockchain.
- The Merkle root of the transactions in the block validates the vote.

3) *Data Validation and Storage:*

- District nodes validate transactions and append them to the blockchain.
- Any tampering with votes is detected by comparing Merkle root hashes.

4) *Result Generation:*

- Smart contracts tally votes in real-time, storing the results on the blockchain.
- Results are immediately available to voters and administrators.

5) *Verification:*

- Voters use their transaction ID to confirm that their vote has been accurately recorded.

D. *Benefits of the Proposed System*

1) *Enhanced Security:*

- Protects against tampering and unauthorized access.
- Ensures votes are stored securely and immutably.

2) *Transparency:*

- Allows voters and administrators to verify the integrity of the process.
- Public ledger ensures accountability.

3) *Efficiency:*

- Reduces delays with real-time result generation.
- Scales effectively for large elections.

4) *Cost Savings:*

- Minimizes reliance on physical resources like paper ballots and manual labor.
- Reduces administrative overhead.

E. *Potential Challenges*

1) *Infrastructure Dependency:*

- Requires reliable internet and computational resources.
- May face challenges in regions with limited digital access.

2) *Adoption Barriers:*

- Voter education and trust in digital systems need to be established.
- Resistance to change from traditional voting methods.

3) *Scalability for Large Elections:*

- High network traffic may require optimized node and block management.

The proposed system combines modern cryptographic techniques and decentralized technologies to address the core issues of voting systems. It is designed to enhance trust, security, and efficiency in elections, ensuring fair representation for all voters.

V. RESULTS AND DISCUSSION

results demonstrate the effectiveness and efficiency of the proposed blockchain-based e-voting system in addressing traditional voting challenges. This section evaluates the system's performance, highlights its advantages, and discusses its limitations based on theoretical analysis and practical implementation scenarios.

A. Results

The system provides the following measurable outcomes:

1) Real-Time Vote Tallying:

- Votes are counted automatically as they are recorded in the blockchain.
- Results are generated in real-time, eliminating the delays associated with manual vote counting.

2) *Tamper-Proof Voting:*

- The integration of Merkle trees ensures that any attempt to tamper with vote data triggers a mismatch in the Merkle root hash, instantly detecting anomalies.
- Immutability of blockchain prevents any changes to recorded votes.

3) Efficient Voter Verification:

- The use of OTP and private key authentication ensures only eligible voters can cast votes.
- Voter details are securely hashed to maintain anonymity.

4) Transparency:

- Voters receive transaction IDs, enabling them to verify their votes on the blockchain without compromising privacy.
- Public access to the blockchain allows independent audits of the election process.

5) User-Friendly Interface:

- A dashboard simplifies voter interaction, offering options to cast votes, view blockchain transactions, and check election results.

B. Advantages

1) Security:

- Strong cryptographic techniques protect voter data and transaction integrity.
- Merkle tree and blockchain integration ensure end-to-end security.

2) Anonymity and Privacy:

- Voter identities are hashed, separating voter information from their votes.
- The use of private keys ensures vote secrecy.

3) Scalability:

- The system can handle millions of votes due to the efficiency of Merkle tree verification and distributed blockchain storage.

4) Cost-Effectiveness:

- Reduces reliance on physical infrastructure and manual labor.
- Eliminates the need for extensive security measures required in traditional systems.

5) Transparency and Trust:

- Open access to the blockchain builds public trust in the election process.
- Independent verification of results ensures fairness and accountability.

C. Limitations

1) Infrastructure Requirements:

- Dependence on robust digital infrastructure and reliable internet connectivity may exclude regions with limited resources.
- Computational requirements for blockchain and Merkle tree operations can strain hardware in large-scale elections.

2) User Adoption:

- Voter education is necessary to ensure understanding and trust in the system.
- Resistance from stakeholders accustomed to traditional voting systems may hinder adoption.

3) Potential Attacks:

- While the system is designed to be secure, sophisticated attacks targeting blockchain nodes or voter devices remain a concern.

4) Legal and Regulatory Challenges:

- Implementing a blockchain-based voting system requires legal and regulatory adaptations in election processes.

D. Discussion

The results indicate that the proposed system is well-suited for addressing the core challenges of traditional and electronic voting methods. By combining the immutable and decentralized nature of blockchain with the efficiency of Merkle trees, the system ensures a transparent, secure, and user-friendly election process. However, the success of real-world implementation depends on overcoming challenges like infrastructure development, user education, and legal approvals.

The adoption of this system has the potential to transform voting processes, offering a scalable and trustworthy alternative to traditional methods while building voter confidence in democratic systems.

VI. FUTURE SCOPE

The proposed blockchain-based e-voting system, while robust and innovative, has immense potential for future enhancements. This section discusses areas where the system can be extended and refined to meet evolving technological, societal, and electoral needs.

A. Enhanced Security Measures

1) Biometric Authentication:

- Integrating biometric verification, such as fingerprints or facial recognition, can add an additional layer of security to voter authentication.
- It ensures that votes are cast only by the registered voter and eliminates the risk of identity fraud.

2) Multi-Factor Authentication (MFA):

- Introducing dual-factor authentication (e.g., OTP + biometric or hardware token) can further secure the system against unauthorized access.
- MFA also reduces the risk of coercion, as voters must verify their identity twice before casting their vote.

3) Post-Vote Confirmation:

- Implementing a confirmation prompt after the vote is cast can reduce accidental votes or voter error.
- Voters could receive a secondary alert or notification prompting them to confirm their choice before it is finalized.

B. Scalability for National Elections

1) Load Balancing:

- Deploying advanced load-balancing mechanisms to handle increased traffic during peak voting hours ensures system reliability.
- Scalable node architecture can adapt to the needs of large-scale elections.

2) Optimized Blockchain Architecture:

- Implementing sharding techniques or sidechains can reduce the computational load on the primary blockchain, ensuring smooth performance during elections with millions of voters.

3) Offline Voting Support:

- Developing mechanisms for offline voting using hardware devices that sync with the blockchain post-election could increase accessibility in areas with limited internet connectivity.

C. Enhanced Voter Accessibility

1) Mobile Voting Platforms:

- Expanding the system to include user-friendly mobile applications can increase voter turnout by making voting more convenient.
- Multi-language support in the interface can ensure inclusivity across diverse demographics.

2) Special Accessibility Features:

- Designing interfaces for people with disabilities (e.g., voice-assisted navigation, larger fonts) ensures equitable participation for all voters.

3) Global Accessibility:

- Implementing systems for expatriates or citizens living abroad to vote securely from their location.

D. *Integration with Emerging Technologies*

1) *Artificial Intelligence (AI) for Anomaly Detection:*
- Using AI to monitor blockchain transactions and identify unusual voting patterns in real-time can enhance system security.
- AI algorithms could flag potential fraud or technical issues for immediate action.

2) *Quantum-Resistant Cryptography:*
- Preparing for the future of quantum computing by integrating quantum-resistant encryption algorithms ensures the long-term security of the system.

3) *IoT Integration:*
- Using IoT devices in polling stations to automate voter identity verification and streamline processes.

E. *Broader Applications of the System*

1) *Local and Municipal Elections:*
- Testing the system in smaller, localized elections can serve as a pilot for larger implementations, helping to refine its functionality.

2) *Corporate and Organizational Voting:*
- Extending the system for use in corporate board elections, university student elections, or non-governmental organizational votes.

3) *Multi-Election Support:*
- Allowing simultaneous management of multiple elections on the same blockchain infrastructure.

F. *Strengthening Legal and Policy Frameworks*

1) *Legal Adaptations:*
- Collaborating with governments to develop regulations for blockchain-based voting systems.
- Establishing legal standards for vote verification and dispute resolution.

2) *Policy Recommendations:*
- Proposing policies for integrating e-voting systems into existing electoral frameworks.
- Ensuring ethical guidelines for voter privacy and data protection.

G. *Research Opportunities*

1) *Data Privacy Enhancements:*
- Researching advanced cryptographic techniques like zero-knowledge proofs to enhance voter privacy.
- Developing methods to anonymize data further while maintaining auditability.

2) *System Performance Studies:*
- Conducting simulations and stress tests to evaluate the system's performance under various scenarios.
- Exploring innovative consensus mechanisms to improve efficiency and reduce energy consumption.

3) *Public Awareness and Education:*
- Studying the impact of digital literacy campaigns on voter confidence and adoption rates.
- Researching strategies to address skepticism and build trust in digital voting technologies.

VII. CONCLUSION

The proposed blockchain-based e-voting system demonstrates the potential to revolutionize the electoral process by addressing the limitations of traditional voting methods. Through the integration of blockchain technology and Merkle trees, the system ensures the security, transparency, and efficiency of elections while maintaining voter anonymity.

A. *Summary of Contributions*

1) *Enhanced Security:*
- By utilizing cryptographic techniques and Merkle tree structures, the system provides tamper-proof data storage and quick detection of anomalies.
- Blockchain’s immutability prevents unauthorized alterations to recorded votes.

2) *Transparency and Trust:*

- The decentralized nature of the system ensures public access to the ledger, allowing for independent audits and increased voter confidence.
- Voters receive transaction IDs to verify their votes in the blockchain without compromising privacy.

3) *Efficiency:*

- The real-time vote tallying capability eliminates delays and ensures prompt announcement of results.
- The system's scalability accommodates large-scale elections with millions of participants.

4) *Voter Privacy:*

- Hashing techniques and the use of private keys ensure that voters' identities remain confidential.

B. Key Takeaways

The system combines blockchain's decentralized and immutable framework with Merkle trees' efficient data verification, achieving:

1) Accurate and tamper-proof elections.
2) Streamlined processes for voters and election administrators.
3) Cost and resource savings compared to traditional methods.

C. Implications for Electoral Systems

Adopting this system in real-world elections has the potential to:

1) Build public trust in the electoral process.
2) Increase voter turnout by providing a convenient and secure digital voting platform.
3) Minimize disputes over election outcomes by offering verifiable and transparent results.

D. Limitations and Challenges

While the system offers significant advantages, certain challenges must be addressed:

1) The need for robust digital infrastructure and reliable internet connectivity.
2) Educating voters and stakeholders on using and trusting the new system.
3) Legal and regulatory adjustments to accommodate blockchain-based voting systems.

VIII. CONCLUSION

This research highlights the transformative potential of blockchain and Merkle tree technology in electoral systems. Although implementation on a national or global scale requires overcoming technical, infrastructural, and regulatory hurdles, the proposed system lays a strong foundation for secure and transparent elections.

By leveraging modern technologies, the system ensures that every vote counts, fostering a democratic process that is fair, efficient, and trustworthy.

REFERENCES

[1] Laskowski, S. J., Autry, M., Cugini, J., Killam, W., & Yen, J. (2004). Improving the usability and accessibility of voting systems and products. NIST Special Publication (NIST SP) 500-256. https://www.nist.gov/publications/improving-usability-and-accessibility-voting-systems-and-products

[2] U.S. Election Assistance Commission (2021) Voluntary Voting System Guidelines. (EAC, Washington, D.C.). Available at https://www.eac.gov/voting-equipment/voluntary-voting-system-guidelines

[3] Help America Vote Act of 2002 (HAVA), Pub. L. No. 107-252, 116 Stat. 1666- 1730. https://www.govinfo.gov/content/pkg/PLAW-107publ252/pdf/PLAW-107publ252.pdf

[4] Laskowski, S. J., Dawkins, S., Quesenbery, W., Chisnell, D., Summers, K., & Rinn, C. (2015). A roadmap for future usability and accessibility guidance. NIST and Center for Civic Design. https://civicdesign.org/wpcontent/uploads/2015/05/Roadmap-V2-15-0715.pdf

[5] Chisnell, D. (2017). The epic journey of American voters. Civic Designing – Medium, March 22, 2017. https://medium.com/civic-designing/the-epic-journey-of-american-voters-ed07bd0e6c57

[6] Lola, P., Eugene, W., Hall, P., & Gilbert, J. E. (2013). Balloting: speeding up the voting process. Proceedings of the International Conference on Human-Computer Interaction, HCI 2013, 373–377. https://doi.org/10.1007/978-3-642-39476-8_76

[7] Los Angeles County (nd). Interactive Sample Ballot. https://www.lavote.gov/home/voting-elections/votingoptions/interactive-sample-ballot

[8] Caltech/MIT Voting Technology Project. (2001). Voting: What Is, What Could Be. Report 1. https://vote.caltech.edu/reports/1

[9] Norden, L., (2006). The Machinery of Democracy: Voting System Security, Accessibility, Usability and Cost. Brennan Center for Justice at NYU School of Law. https://www.brennancenter.org/publication/machinerydemocracy

[10] National Conference of State Legislatures. (2022) Report: Risk Limiting Audits. Checking the Election: RiskLimiting Audits (September 2022) https://www.ncsl.org/elections-and-campaigns/risk-limiting-audits

[11] Morrell, J. (2019). Knowing It’s Right: A two-part guide to risk limiting audits. Democracy Fund, May 22, 2019. https://www.democracyfund.org/publications/knowing-its-right

[12] Garg, V., Benton, K., & Camp, L. J. (2014). The privacy paradox: a Facebook case study. 2014 TPRC Conference Paper. https://doi.org/10.2139/ssrn.2411672

[13] Balebako, R., Schaub, F., Adjerid, I., Acquisti, A., & Cranor, L. (2015). The impact of timing on the salience of smartphone app privacy notices. In Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices - SPSM ’15. https://doi.org/10.1145/2808117.2808119

[14] Everett, S. P. (2007). The usability of electronic voting machines and how can be changed without detection. 2007 Doctoral Dissertation, Rice University. https://hdl.handle.com