Journal of Electrical & Electronics Engineering Research and Reviews

Academixs Open Access Publishers

Research Article

Usability and Accessibility of Blockchain E-voting Systems

Anshika Sharma[1*], Adhyan Negi[2], Sahana[3], Siya Singh[4] and Ashok Kumar[5]

[1,2,3,4]*Department of AIML, Dronacharya College of Engineering, India*

[5]*Department of Applied science and humanities, Dronacharya college of engineering, India*

Corresponding Author:
Anshika Sharma. Department of AIML, Dronacharya College of Engineering, India.

Received Date: 23.10.2025 **Accepted Date:** 27.10.2025 **Published Date:** 03.11.2025

Abstract

The emergence of blockchain technology has promised to revolutionize various sectors, elec-tronic voting (e-voting) being a significant area of interest [1-4]. The core tenets of block-chain—decentralization, immutability, and transparency—offer the potential to create e-voting systems that are more secure, trustworthy, and resistant to fraud than traditional or other electronic voting methods. However, the successful implementation and widespread adoption of blockchain-based e-voting systems hinge on more than just their security features. For these systems to be truly democratic and effective, they must be usable and accessible to all eligible citizens. This paper delves into the usability and accessibility in the context of blockchain e-voting systems. While the papers extensively cover the security and privacy aspects, they also shed light on the often-overlooked but critical factors of how real users interact with these complex systems. This deep dive will explore the definitions, challenges, current state (e.g., the Moscow internet voting experiment detailed in and future directions of usability and acces-sibility, as detailed in the provided literature (e.g., academic prototypes in), to paint a com-plete picture of this vital aspect of e-voting technology [2,5,4]. This survey also leverages in-sights from comprehensive reviews of blockchain-based e-voting systems and studies on secu-rity and privacy in smart city e-voting applications [1,3,6].

Introduction

A smart city has been an IT dream from as long as computers have existed. To benefit from smart city services, citizens must apply and participate; to do so, they need to be sure that their information and activities are well protected and secured. That is why smart cities must be secure, so it is necessary to develop security frameworks on it to enhance privacy and security. Moreover, blockchain technology plays a key role in IoT security solutions. Blockchain is a system that delivers a shared ledger technology that permits each network member to view the ledger, where the data blocks contain all transactions and a hash to the previous block. All transactions in the public ledger are validated, and the data blocks are immutable.

Defining Usability and Accessibility in the Context of Blockchain E-Voting

This paper offers clear definitions and frameworks for understanding usability and accessibility in the specific context of blockchain e-voting. These definitions are crucial for establishing the criteria against which such systems should be evaluated.

Usability: The User's Experience

Usability in e-voting refers to the ease with which a voter can effectively, efficiently, and satis-factorily cast their vote. A usable system is one that minimizes confusion and maximizes the voter's confidence that their choice has been accurately recorded. The papers break down usa-bility into several key components:

User-Centric Voting Design: This is a fundamental concept emphasizing that the voting system should be designed with the user at the center of the process. Key aspects of a user-centric design include:

• A user-friendly interface that is intuitive and easy to navigate for all individuals, regard-less of their technical proficiency.
• The system must present choices clearly and without any bias that could advantage one candidate or option over another.

Simplicity: The voting process should be as straightforward as possible. Complex procedures can lead to voter error, frustration, and a lack of trust in the system.

Understandability: Clarity in the system's operation is paramount. Voters must be able to understand how to cast their vote and be confident that their actions will result in their intended choice being recorded.

Efficiency: A usable system allows voters to cast their votes in a swift and inexpensive man-ner. This includes both time

efficiency, by speeding up the voting and vote-tallying process, and performance efficiency, by handling a large volume of votes accurately and securely.

Accessibility: Ensuring Equal Participation

Accessibility is about ensuring that all eligible voters have an equal opportunity to participate in the voting process, without any barriers due to disability, location, or lack of technical re-sources. The papers highlight several dimensions of accessibility:

Universal Access: The system must be designed to be effectively used by all eligible voters. This means considering a wide range of user abilities and circumstances.

Inclusivity for People with Disabilities: A core aspect of accessibility is providing the nec-essary access for individuals with functional limitations or disabilities to vote independently and privately. This includes accommodations for visual, auditory, motor, and cognitive impair-ments.

Addressing the Digital Divide: The system must be designed to be inclusive of those who are not familiar with the internet, people with limited access to technology, or technology novices. This is a significant challenge for any online voting system.

Availability: The system must be consistently available to all eligible voters during the elec-tion period. This includes protection against denial-of-service attacks and having redundant systems in place to prevent failures.

The Current State and Notable Implementations

The research papers provide a look at the current landscape of blockchain e-voting, including several real-world implementations. An analysis of these systems through the lens of usability and accessibility reveals both progress and persistent gaps.

AA Noted Lack of Emphasis

A recurring theme in the literature is the "relative lack of emphasis on aspects such as accessi-bility, compatibility, availability, and usability in the reviewed literature"[3]. While the core benefits of blockchain, such as security, transparency, and decentralization, are frequently highlighted, usability and accessibility are often treated as secondary concerns. This indicates a significant gap in the research and development of these systems.

Moscow: A Case Study

The internet voting experiment took place in September 2019 for local elections in Moscow, specifically for the city parliament [5].

• It was implemented in only three districts, but with no restrictions on who could regis-ter and use the internet voting system instead of traditional polling stations.

• The election occurred during a period of political tension, with protests related to the rejection of opposition candidates.

Public Testing and Source Code

• Despite the context, organizers proposed a public test of the system, making the source code public on GitHub.

• However, the source code was partial, and there was no comprehensive specification or documentation.

• The public testing was conducted under a tight schedule, with the code published on Ju-ly 17th and the election on September 8th.

Identified Attacks and Fixes

First Attack (Jerry Goudreau): The original encryption scheme used a multi-level variant of ElGamal, which was found to be weak. It used three independent keys and primes (p1, p2, p3) chosen to be less than 256 bits. This size is vulnerable to discrete log attacks, which can be performed in less than 12 hours with modern software like Cado-NFS. Goudreau demonstrated this vulnerability by cracking the encryption in under 10 minutes.

Fix: The developers removed the triple ElGamal encryption, increased the key size to 1024 bits, and changed the protocol so that decryption was no longer part of the smart contract. They also corrected the generator to be in the prime order subgroup.

• The plain Elgamal encryption of a message m: $Enc_{g,\ pk}(m) = (a, b) = (g^r, pk^r \cdot m)$

• The decryption using sk is: $Dec_{g,\ sk}(a, b) = b \cdot a^{-sk} = m$

• **g**: Generator of the group

• **pk**: Public key (pk=gskpk=gsk)

• **r**: Random value

• **m**: Message (vote/candidate identifier)

Second Attack (Alexander Golovnik): After the first fix, Alexander Golovnik discovered that messages (candidate identifiers) were not randomized and their quadratic residuosity was leaked. This effectively revealed one bit of information about the message, which could com-promise privacy in a two-candidate scenario.

Fix: The developers silently updated the source code (only two days before the election) to square the message before encryption, preventing the leakage of the quadratic residuosity.

General Weaknesses in the Protocol

• **Privacy:** The system relied on the server to cut the link between ballots and voters for privacy, which is difficult to implement reliably due to the need for backups and redun-dancy.

• **Verifiability:** While a blockchain was used, it was a private one, meaning it offered no true decentralization or transparency. Voters could only query the blockchain via a web server they had to trust. Access to the blockchain was cut a few hours after the election, defeating its purpose.

• **Coercion Resistance:** This crucial property for elections in contexts like Russia was not adequately addressed, potentially allowing individuals to be forced to vote in a cer-tain way or sell their vote.

• **Lack of Documentation:** A significant ongoing issue was the absence of public docu-mentation and specifications, making independent verification and analysis extremely challenging.

The 2020 Russian Constitutional Vote

• A year later, in June-July 2020, Russia held a much larger-scale internet vote for consti-tutional changes [5].

• Again, the system was designed by the Moscow Department of Information Technology, but this time the code was not public.

• While they used a standard cryptographic library (libsodium), it was again a private blockchain (Exonum) with no documentation.

• Reports indicated continued lack of coercion resistance and a

questionable key exchange method for each vote.
• The e-voting was used by a massive number of people (1 million ballots in Moscow, 130,000 in Nizhny Novgorod).
• There were accusations of coercion and statistical evidence of fraud, though these were mostly related to traditional voting, with some coercion concerns for e-voting.

Real-World Implementations and Their Usability/ Accessibility Features

Several countries and companies have piloted or adopted blockchain-based e-voting systems. Examining their features provides insight into the practical application of usability and accessi-bility principles:

Estonia: As a pioneer in e-voting, Estonia's system offers valuable lessons. Their system re-quires an Electronic National Identification Card for authentication, which, while secure, pre-sents a usability hurdle for those who do not have one or are not comfortable using it. The system also necessitates downloading a specific voting application, which could be a barrier for some users [3].

Switzerland: The Swiss e-voting system has utilized a mobile phone application with Short Message Service (SMS) confirmation [3]. Voters log in with their ID, follow on-screen instruc-tions, and enter a PIN, comparing a security symbol with one received in the mail. While this multi-step process enhances security, it could be perceived as complex by some voters.

Commercial Platforms

POLYAS: This platform, certified by the German Federal Office for Information Security, is used for various elections in Europe and the USA. The focus on certification suggests a high standard of security, but the papers do not provide extensive details on its specific usability and accessibility features [3].

Voatz: A mobile-based system that uses biometric validation like fingerprints or retinal scans. While biometrics can offer a convenient authentication method, it raises accessibility concerns for individuals who cannot use these features and privacy concerns for others [3].

Follow My Vote: This platform requires users to install a "voting booth" on their device and verify their identity by submitting legal documents to an approved Identity Identifier. This rig-orous authentication process, while secure, could be a significant usability barrier [3].

Challenges to Achieving Optimal Usability and Accessibility

The path to creating truly usable and accessible blockchain e-voting systems is fraught with challenges. The papers identify several key obstacles that need to be addressed.

The Inherent Complexity of Blockchain

At its core, blockchain is a complex technology [3]. This complexity can be a major hurdle for the average citizen:
• **Rejection by "Tech Agnostic Users":** There is a real concern that users who are not technologically savvy will reject or be unable to use blockchain-based systems. This could lead to disenfranchisement and a decrease in voter turnout.
• **Lack of Trust and Understanding:** The abstract nature of blockchain can make it dif-ficult for voters to trust the system. If they do not understand how their vote is being recorded and secured, they may be hesitant to use it.

The Security vs. Usability Trade-off

A persistent challenge in the design of any secure system is the trade-off between security and usability [3]. This is particularly acute in e-voting:
• **Balancing Act:** Achieving a balance between a user-friendly interface and the stringent security and integrity requirements of the voting process is a major challenge. Highly secure systems often involve multiple steps of authentication and verification, which can make them more cumbersome for the user.
• **Complex Authentication:** Methods like multi-factor authentication, while enhancing security, can add complexity to the user experience.

Significant Accessibility Barriers

Ensuring that everyone can vote requires overcoming several accessibility barriers:
• **The Digital Divide:** Limited internet access in certain locations is a significant chal-lenge to the accessibility of online e-voting systems. This can disproportionately affect rural, low-income, and elderly populations.
• **Offline Voting Complexity:** Providing an offline voting method that is consistent with the overall blockchain system is a complex technical and logistical challenge.
• **Lack of Inclusivity for People with Disabilities:** Many proposed systems do not adequately address the needs of voters with disabilities. The lack of features like screen readers or voice-guided interfaces can render these systems unusable for a segment of the population.

Immaturity and Lack of Real-World Testing

The relative newness of blockchain technology in the e-voting space presents its own set of challenges [3]:
• **Immaturity of the Technology:** The immaturity of blockchain for e-voting has re-sulted in a lack of real-world experiments, extensive testing, and comprehensive evalua-tion. This makes it difficult to assess the real-world usability and accessibility of these systems.
• **Lack of Stakeholder Engagement:** Without broad stakeholder engagement, includ-ing with voters, election officials, and accessibility experts, it is difficult to design sys-tems that meet the needs of all users.

Academic Prototype

Prototype Description

• **Platform:** Bitcoin testnet (simulation)
• **Participants:** Simulated university election (10–100 voters)
• **Voting Process:** Voters use Bitcoin addresses to represent votes.
• Transactions encode votes using OP_RETURN.
• **Results:** Successful simulation for small groups.
• **Limitations:** Scalability, privacy, and transaction cost issues.

Parameters	Value
Number of voters	10, 50, 100
Avg. transaction size	~250 bytes
Confirmation time	10–20 minutes
Transaction fee	0.0001 BTC
Usability	Not user tested
Scalability	Not suitable for large election

Simulated university election [4].

Platform: Bitcoin testnet
Participants: Simulated boardroom (5–20 voters)

Voting Process
• Voters register their public keys.
• Each vote is encrypted and submitted as a Bitcoin transaction.
• A smart contract (script) counts the votes.
• **Privacy:** Homomorphic encryption, mixnets for anonymity.
• **Results:** Demonstrated technical feasibility for small groups.
• **Limitations:** High transaction fees, slow confirmation times, limited scalability.

Parameters	Value
Number of voters	5, 10, 20
Avg. vote transaction size	~300 bytes
Bitcoin fee per vote	0.0001–0.0005 BTC
Confirmation time	~10 minutes
Privacy breach rate	0% (in simulation)
Usability feedback	Not formally measured; noted as "complex for non-experts"

Simulated boardroom [2].
Successful simulation for small groups [2,4].

Proposed Solutions and Best Practices for Improvement

Despite the challenges, the research papers offer a range of proposed solutions and best prac-tices to enhance the usability and accessibility of blockchain e-voting systems.

Designing for the User

A user-centered design approach is crucial for creating systems that are both usable and trust-ed:

Intuitive and Friendly Interfaces: There is a clear call for the development of "friendlier and more accessible" interfaces. This includes designing mobile apps with clear, guiding in-structions and reliable verification mechanisms to ensure a seamless and secure voting experi-ence.

Smart Contracts for Automation: Smart contracts can be used to automate many aspects of the electoral process, which can simplify the experience for both voters and election admin-istrators.

Bridging the Accessibility Gap

Several strategies are proposed to make e-voting more accessible to all:

Offline and Alternative Voting Methods: The development of hybrid systems that allow for both online and offline voting can help bridge the digital divide and ensure that all eligible voters can participate.

Assistive Technologies: Incorporating features like screen readers, voice navigation, and alternative input methods can make e-voting systems more inclusive for people with disabilities.

Stakeholder Engagement: Engaging with a broad range of stakeholders, including voters, accessibility experts, and election officials, is essential for identifying and addressing usability and accessibility challenges.

Conclusion

The integration of blockchain technology into electronic voting (e-voting) systems has the po-tential to revolutionize the democratic process by enhancing security, transparency, and trust. However, the success of these systems depends not only on their technical robustness but also on their usability and accessibility for all eligible voters. This paper examined the current state, challenges, and potential solutions for improving usability and accessibility in blockchain-based e-voting, drawing on real-world case studies and existing literature [8-11].

References

1. Hajian Berenjestanaki, M., Barzegar, H. R., El Ioini, N., & Pahl, C. (2024). Blockchain-based e-voting systems: a technology review. Electronics, 13(1), 17.
2. 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.
3. Saračević, M., Adamović, S. A. Š. A., Maček, N., Selimi, A., & Pepic, S. (2021). Source and channel models for secret-key agreement based on Catalan numbers and the lattice path combinatorial approach. J Inf Sci Eng, 37(2), 469-482.
4. Accioly, A., Giacchini, B. L., & Shapiro, I. L. (2017). Low-energy effects in a higher-derivative gravity model with real

and complex massive poles. Physical Review D, 96(10), 104004.
5. Estecahandy, H. (2023). The democratic illusion through the technological illusion: a case study of the implementation of a blockchain to support an e-voting platform in moscow (Active Citizen). arXiv preprint arXiv:2301.03954.
6. Chentouf, F. Z., & Bouchkaren, S. (2023). Security and privacy in smart city: a secure e-voting system based on blockchain. International Journal of Electrical and Computer Engi-neering, 13(2), 1848.
7. Chentouf, F. Z., & Bouchkaren, S. (2021). Blockchain for cybersecurity in IoT. In Artificial Intelligence and Blockchain for Future Cybersecurity Applications (pp. 61-83). Cham: Springer International Publishing.
8. Rajasekar, V., Predić, B., Saracevic, M., Elhoseny, M., Karabasevic, D., Stanujkic, D., & Ja-yapaul, P. (2022). Enhanced multimodal biometric recognition approach for smart cities based on an optimized fuzzy genetic algorithm. Scientific Reports, 12(1), 622.
9. Saračević, M. H., Adamović, S. Z., Miškovic, V. A., Elhoseny, M., Maček, N. D., Selim, M. M., & Shankar, K. (2020). Data encryption for internet of things applications based on catalan objects and two combinatorial structures. IEEE Transactions on Reliability, 70(2), 819-830.
10. Saračević, M., Adamović, S., Maček, N., Elhoseny, M., & Sarhan, S. (2020). Cryptographic keys exchange model for smart city applications. IET Intelligent Transport Systems, 14(11), 1456-1464.
11. Vladucu, M. V., Dong, Z., Medina, J., & Rojas-Cessa, R. (2023). E-voting meets blockchain: A survey. IEEE Access, 11, 23293-23308.

Citation: Anshika Sharma,. Adhyan Negi,. Sahana,. Siya Singh,. Ashok Kumar,. (2025). Usability and Accessibility of Blockchain E-voting Systems. *J. Electr. Electron. Eng. Res. Rev. 1*(1), 1-5.