Blockchain-Based Voting Systems for Transparency

Dr. Alexander P Rodriguez [1], Dr. Sarah M Chen [2], Dr. Emma L Johnson [3], Dr. Ahmed H Al-Mahmoud [4]
[1] Department of Computer Science and Cybersecurity, Massachusetts Institute of Technology, Cambridge, MA, USA
[2] School of Information Security and Cryptography, University of California, Berkeley, CA, USA
[3] Centre for Democratic Innovation, University of Cambridge, Cambridge, UK
[4] Department of Information Systems and Digital Society, King Abdullah University of Science and Technology, Thuwal, Saudi Arabia

* Corresponding Author: **Dr. Alexander P Rodriguez**

Article Info

P-ISSN: 3051-3618
E-ISSN: 3051-3626
Volume: 03
Issue: 01
January - June 2022
Received: 02-01-2022
Accepted: 03-02-2022
Published: 02-03-2022
Page No: 18-23

Abstract
Blockchain-based voting systems are transforming electoral processes by leveraging decentralized, immutable, and transparent ledger technology to enhance security and trust. This paper explores how blockchain technology addresses critical challenges in traditional and electronic voting, such as fraud, tampering, and lack of transparency. By recording votes as cryptographic transactions on a distributed ledger, these systems ensure immutability, real-time auditability, and voter privacy through advanced cryptographic tools like zero-knowledge proofs and blind signatures. Case studies, including pilots in West Virginia and Estonia, demonstrate the potential for secure, accessible, and cost-efficient elections. The paper evaluates key features like voter authentication, vote verifiability, and decentralized consensus, alongside challenges such as scalability, digital access gaps, and regulatory hurdles. By integrating smart contracts and permissioned networks, blockchain voting systems offer a scalable framework for transparent elections. However, public education and legal frameworks are critical for widespread adoption. Blockchain-based voting systems promise to strengthen democratic processes by fostering trust and inclusivity, paving the way for resilient electoral systems in the digital age.

Keywords: Blockchain Voting, Transparency, Secure Elections, Decentralized Ledger, Voter Privacy, Smart Contracts, Cryptographic Authentication, E-Voting, Auditability, Digital Democracy, Zero-Knowledge Proofs, Election Integrity.

Introduction

Democratic governance relies fundamentally on the integrity and transparency of electoral processes, yet traditional voting systems continue to face persistent challenges that undermine public confidence in democratic institutions [1, 2]. Paper-based voting systems, while providing physical audit trails, are susceptible to human error, logistical complications, and potential manipulation during counting and storage phases [3]. Electronic voting systems, though offering efficiency and accessibility improvements, have raised concerns about security vulnerabilities, lack of verifiable audit trails, and potential for large-scale fraud [4, 5].

The erosion of public trust in electoral processes has become a global phenomenon, with surveys indicating declining confidence in electoral integrity across established democracies [6]. This crisis of trust threatens the legitimacy of democratic governance and highlights the urgent need for voting systems that provide verifiable transparency while maintaining the security and privacy essential to democratic participation [7].

Blockchain technology, originally developed as the underlying infrastructure for cryptocurrencies, offers unprecedented opportunities to address these challenges through its core characteristics of immutability, transparency, decentralization, and cryptographic security [9, 10]. The distributed ledger approach enables the creation of tamper-evident voting records while maintaining voter privacy through advanced cryptographic techniques [10].

Recent developments in blockchain voting systems have demonstrated promising results in pilot programs and small-scale implementations worldwide, suggesting the potential for broader adoption in electoral processes [11, 12]. However, the transition from traditional to blockchain-based voting systems requires careful consideration of technical, legal, social, and political factors that influence both feasibility and acceptance [13].

Fundamental Principles of Blockchain Voting Systems

Blockchain-based voting systems leverage distributed ledger technology to create transparent, immutable, and verifiable electoral processes [14]. The fundamental architecture consists of a network of nodes that collectively maintain a synchronized ledger of all voting transactions, with each vote cryptographically secured and permanently recorded [15].

The immutability characteristic of blockchain technology ensures that once votes are recorded, they cannot be altered or deleted without detection, providing a permanent audit trail that enhances electoral integrity [16]. Transparency is achieved through the public visibility of the blockchain ledger, allowing any participant to verify the voting process while maintaining voter privacy through cryptographic anonymization techniques [17].

Decentralization eliminates single points of failure and reduces the potential for centralized manipulation or system compromises that could affect entire elections [18]. The distributed nature of blockchain networks ensures that voting records remain accessible and verifiable even if individual nodes fail or are compromised [19].

Cryptographic security protocols, including digital signatures, hash functions, and zero-knowledge proofs, protect voter privacy while enabling verification of vote authenticity and system integrity [20]. Advanced cryptographic techniques such as homomorphic encryption allow for vote tallying without revealing individual voting choices [21].

Smart contracts, self-executing programs deployed on blockchain networks, can automate various aspects of the electoral process, including voter registration verification, ballot distribution, vote validation, and result calculation [22]. These automated processes reduce human intervention and potential for manipulation while ensuring consistent application of electoral rules [23].

Technical Architecture and Implementation Models

Several technical architectures have been proposed and implemented for blockchain-based voting systems, each with distinct advantages and trade-offs [24]. Public blockchain implementations leverage existing networks like Ethereum to provide maximum transparency and decentralization but face challenges related to scalability, transaction costs, and energy consumption [25].

Private blockchain networks offer greater control over network participants and can provide improved performance and lower costs, but may sacrifice some transparency and decentralization benefits [26]. Consortium blockchain approaches, involving trusted institutions as network validators, attempt to balance transparency with practical governance requirements [27].

Hybrid architectures combine blockchain technology with traditional voting infrastructure to address specific implementation challenges while maintaining core security and transparency benefits [28]. These systems may use blockchain for vote recording and verification while employing conventional systems for voter authentication and ballot presentation [29].

Layer-2 solutions, including state channels and sidechains, have been proposed to address scalability limitations of main blockchain networks while maintaining security guarantees [30]. These approaches can significantly reduce transaction costs and processing times for large-scale elections [31].

The integration of biometric authentication systems with blockchain voting platforms enhances security by ensuring voter identity verification while preventing double voting [32]. Advanced biometric techniques, combined with zero-knowledge proof systems, can verify voter eligibility without revealing personal information [33].

Security Analysis and Threat Mitigation

Blockchain voting systems must address numerous security challenges to ensure electoral integrity and public trust [34]. Cryptographic security forms the foundation of blockchain voting, with digital signature schemes ensuring vote authenticity and hash functions providing tamper evidence [35].

Consensus mechanisms play a crucial role in maintaining network integrity and preventing malicious actors from manipulating voting records [36]. Proof-of-Stake and Proof-of-Authority consensus algorithms have been specifically adapted for voting applications to reduce energy consumption while maintaining security [37].

Network security considerations include protection against distributed denial-of-service attacks, Sybil attacks, and other forms of network disruption that could affect voting accessibility [38]. Robust network design and redundancy measures are essential for maintaining system availability during critical electoral periods [39].

Privacy protection mechanisms must balance transparency requirements with voter confidentiality obligations [40]. Ring signatures, zero-knowledge proofs, and homomorphic encryption enable vote verification without revealing individual voting choices [41]. These cryptographic techniques allow for public auditability while maintaining the secret ballot principle fundamental to democratic voting [42].

Smart contract security represents another critical consideration, as vulnerabilities in voting contract code could compromise entire elections [43]. Formal verification methods and extensive security auditing are essential for ensuring smart contract reliability and security [44].

Transparency and Auditability Features

The transparency characteristics of blockchain voting systems provide unprecedented opportunities for public verification and audit of electoral processes [45]. Real-time vote tracking allows authorized observers to monitor voting progress and identify potential irregularities as they occur [46].

Public audit trails enable post-election verification by independent parties without compromising voter privacy [47]. Citizens, candidates, and electoral observers can verify that their votes were correctly recorded and counted without relying solely on election officials [48].

Cryptographic proofs of vote integrity allow voters to verify that their individual votes were included in the final tally while maintaining overall ballot secrecy [49]. These verification mechanisms enhance public confidence by providing mathematical certainty of electoral accuracy [50].

Immutable record keeping ensures that historical electoral data remains available for future analysis and verification, supporting long-term democratic accountability [51]. The permanent nature of blockchain records provides researchers and policymakers with reliable data for studying electoral trends and improving democratic processes [52].

Distributed verification enables multiple independent parties to validate election results simultaneously, reducing the potential for disputes and increasing confidence in electoral outcomes [53]. This distributed approach eliminates the need to trust single institutions or individuals with exclusive access to voting records [54].

Global Implementation Case Studies

Several countries and organizations have conducted pilot programs and limited implementations of blockchain voting systems, providing valuable insights into practical challenges and benefits [55]. Estonia's e-Residency program has explored blockchain integration for digital voting, building on their existing electronic voting infrastructure [56].

Switzerland has conducted blockchain voting trials in several cantons, focusing on maintaining the country's tradition of direct democracy while enhancing security and transparency [57]. These pilots have demonstrated both the potential benefits and practical challenges of implementing blockchain voting in established democratic systems [58].

Municipal elections in various jurisdictions have served as testing grounds for blockchain voting technologies, allowing for controlled evaluation of system performance and public acceptance [59]. These smaller-scale implementations provide valuable data on scalability requirements and user experience considerations [60].

Corporate governance applications have demonstrated blockchain voting capabilities in shareholder elections and board decisions, showing the technology's potential beyond public elections [61]. These implementations have highlighted the importance of user interface design and stakeholder education in successful blockchain voting deployment [62].

Military and overseas voting applications represent particularly promising use cases for blockchain technology, addressing longstanding challenges in absentee voting security and verification [63]. Remote voting capabilities enabled by blockchain systems can increase participation among geographically dispersed populations while maintaining security standards [64].

Challenges and Limitations

Despite significant potential benefits, blockchain voting systems face substantial challenges that must be addressed before widespread adoption [65]. Scalability remains a primary concern, as existing blockchain networks may not support the transaction volumes required for large-scale elections [66].

Digital divide issues could exacerbate existing inequalities in voting access, as blockchain voting systems require reliable internet connectivity and technological literacy [67]. Ensuring equitable access to blockchain voting platforms requires significant investment in digital infrastructure and education [68].

Regulatory frameworks for blockchain voting remain underdeveloped in most jurisdictions, creating uncertainty about legal requirements and compliance standards [69]. The intersection of election law, data protection regulations, and emerging technology governance presents complex challenges for policymakers [70].

User experience considerations are critical for public acceptance and successful implementation of blockchain voting systems [71]. Complex cryptographic concepts must be translated into intuitive interfaces that enable all eligible voters to participate effectively [72].

Energy consumption concerns associated with some blockchain consensus mechanisms raise environmental and sustainability questions about large-scale voting implementations [73]. The development of energy-efficient consensus algorithms specifically designed for voting applications remains an active area of research [74].

Technical literacy requirements may create barriers for certain voter populations, potentially affecting electoral participation and democratic representation [75]. Comprehensive education and support programs are essential for ensuring inclusive access to blockchain voting systems [76].

Future Directions and Research Opportunities

Emerging research areas in blockchain voting include quantum-resistant cryptographic methods to protect against future quantum computing threats [77]. The development of post-quantum cryptographic standards will be essential for long-term security of blockchain voting systems [78].

Integration with artificial intelligence and machine learning technologies offers opportunities for enhanced fraud detection, user experience optimization, and system performance improvement [79]. AI-powered analytics can identify patterns indicative of malicious activity while protecting voter privacy [80].

Cross-chain interoperability solutions may enable voting systems that leverage multiple blockchain networks for enhanced security and functionality [81]. These approaches could combine the benefits of different blockchain architectures while mitigating individual network limitations [82].

Governance token mechanisms could enable new forms of participatory democracy and citizen engagement beyond traditional voting [83]. These systems might support continuous civic participation and policy input rather than periodic electoral events [84].

Mobile voting applications built on blockchain technology represent a significant opportunity for increasing voter participation and accessibility [85]. However, mobile implementation requires careful consideration of device security, network reliability, and user authentication challenges [86].

Regulatory and Policy Implications

The implementation of blockchain voting systems requires comprehensive regulatory frameworks that address technical standards, security requirements, audit procedures, and privacy protections [87]. Policymakers must balance innovation encouragement with risk mitigation to ensure public trust and electoral integrity [88].

International cooperation in developing blockchain voting standards could facilitate global best practices and interoperability while respecting national sovereignty over electoral processes [89]. Collaborative approaches to regulation can help address the transnational nature of blockchain technology [90].

Conclusion

Blockchain-based voting systems represent a transformative approach to addressing persistent challenges in democratic electoral processes, offering unprecedented levels of transparency, security, and verifiability. The immutable and distributed nature of blockchain technology provides solutions to longstanding concerns about electoral integrity while enabling new forms of citizen engagement and participation.

The evidence from pilot programs and theoretical analysis demonstrates significant potential for blockchain voting to enhance public trust in democratic institutions through cryptographically verifiable transparency. The ability to provide public audit trails while maintaining voter privacy represents a fundamental advancement in electoral technology that could strengthen democratic governance worldwide.

However, successful implementation requires careful attention to scalability, usability, digital inclusion, and regulatory considerations that affect both technical feasibility and public acceptance. The digital divide and technological literacy requirements present particular challenges that must be addressed to ensure equitable access to blockchain voting systems.

Future research should focus on developing energy-efficient consensus mechanisms, quantum-resistant security protocols, and user-friendly interfaces that make blockchain voting accessible to all citizens. The integration of artificial intelligence and mobile technologies offers promising directions for enhancing both security and usability of blockchain voting platforms.

The regulatory landscape for blockchain voting requires continued development to provide clear standards and guidelines while fostering innovation and maintaining public trust. International cooperation in establishing best practices and technical standards could accelerate adoption while ensuring consistency and interoperability across different jurisdictions.

As blockchain technology continues to mature and public understanding of its capabilities grows, blockchain-based voting systems are likely to play an increasingly important role in strengthening democratic processes. The combination of mathematical verifiability, cryptographic security, and transparent auditability offers a compelling vision for the future of electoral technology that could restore and enhance public confidence in democratic institutions.

The successful deployment of blockchain voting systems will ultimately depend on collaborative efforts among technologists, policymakers, election officials, and civil society organizations to address technical challenges while ensuring that these systems serve the fundamental democratic principles of transparency, accessibility, and public trust.

References

1. Norris P. Why electoral integrity matters. New York: Cambridge University Press; 2014.
2. Birch S. Electoral malpractice. Oxford: Oxford University Press; 2011.
3. Alvarez RM, Hall TE. Electronic elections: The perils and promises of digital democracy. Princeton: Princeton University Press; 2008.
4. Kohno T, Stubblefield A, Rubin AD, Wallach DS. Analysis of an electronic voting system. In: Proceedings of the 2004 IEEE Symposium on Security and Privacy. 2004. p. 27-40.
5. Mercuri RT. A better ballot box? IEEE Spectr. 2002;39(10):46-50.
6. Norris P, Frank RW, Martinez i Coma F, editors. Advancing electoral integrity. New York: Oxford University Press; 2014.
7. Pew Research Center. Public trust in government remains near historic lows. Washington DC: Pew Research Center; 2022.
8. Nakamoto S. Bitcoin: A peer-to-peer electronic cash system. 2008. Available from: https://bitcoin.org/bitcoin.pdf
9. Swan M. Blockchain: Blueprint for a new economy. Sebastopol: O'Reilly Media; 2015.
10. Kshetri N, Voas J. Blockchain-enabled e-voting. IEEE Softw. 2018;35(4):95-9.
11. Hjálmarsson FÞ, Hreiðarsson GK, Hamdaqa M, Hjálmtýsson G. Blockchain-based e-voting system. In: Proceedings of the 2018 IEEE 11th International Conference on Cloud Computing. 2018. p. 983-6.
12. Pawlak M, Poniszewska-Marańda A. Trends in blockchain-based electronic voting systems. Inf Process Manag. 2021;58(4):102595.
13. Acharya V, Yerukala A, Prakash J. A secure and transparent election system using blockchain technology. Int J Adv Trends Comput Sci Eng. 2020;9(1):1120-6.
14. Zhang S, Wang L, Xiong H. Chaintegrity: Blockchain-enabled large-scale e-voting system with robustness and universal verifiability. Int J Inf Secur. 2020;19(3):323-41.
15. Taş R, Tanrıöver ÖÖ. A systematic review of challenges and opportunities of blockchain for e-voting. Symmetry. 2020;12(8):1328.
16. Yaga D, Mell P, Roby N, Scarfone K. Blockchain technology overview. NIST Interagency Rep. 2018;8202:1-68.
17. Noizat P. Blockchain electronic vote. In: Handbook of digital currency. Amsterdam: Elsevier; 2015. p. 453-61.
18. Pilkington M. Blockchain technology: principles and applications. In: Research handbook on digital transformations. Cheltenham: Edward Elgar Publishing; 2016. p. 225-53.
19. Crosby M, Pattanayak P, Verma S, Kalyanaraman V. Blockchain technology: Beyond bitcoin. Appl Innov. 2016;2(6-10):71.
20. Boneh D, Shacham H. Group signatures with verifier-local revocation. In: Proceedings of the 11th ACM conference on Computer and communications security. 2004. p. 168-77.
21. Gentry C. A fully homomorphic encryption scheme. Stanford: Stanford University; 2009.
22. Szabo N. Smart contracts: building blocks for digital markets. EXTROPY. 1996;16(18):2.
23. Christidis K, Devetsikiotis M. Blockchains and smart contracts for the internet of things. IEEE Access. 2016;4:2292-303.
24. Zheng Z, Xie S, Dai HN, Chen X, Wang H. Blockchain challenges and opportunities: A survey. Int J Web Grid Serv. 2018;14(4):352-75.
25. Buterin V. Ethereum: A next-generation smart contract and decentralized application platform. 2014. Available from: https://ethereum.org/whitepaper/
26. Androulaki E, Barger A, Bortnikov V, et al. Hyperledger fabric: a distributed operating system for permissioned blockchains. In: Proceedings of the thirteenth EuroSys

conference. 2018. p. 1-15.
27. Baliga A, Subhod I, Kamat P, Chatterjee S. Performance evaluation of the quorum blockchain platform. arXiv preprint arXiv:1809.03421. 2018.
28. Casino F, Dasaklis TK, Patsakis C. A systematic literature review of blockchain-based applications: current status, classification and open issues. Telemat Inform. 2019;36:55-81.
29. Shinde PP, Borkar S. Study of blockchain based e-voting system. Int J Eng Appl Sci Technol. 2020;4(12):508-16.
30. Poon J, Dryja T. The bitcoin lightning network: Scalable off-chain instant payments. 2016. Available from: https://lightning.network/lightning-network-paper.pdf
31. McCorry P, Shahandashti SF, Hao F. A smart contract for boardroom voting with maximum voter privacy. In: International Conference on Financial Cryptography and Data Security. Berlin: Springer; 2017. p. 357-75.
32. Jain AK, Ross A, Prabhakar S. An introduction to biometric recognition. IEEE Trans Circuits Syst Video Technol. 2004;14(1):4-20.
33. Blum M, Feldman P, Micali S. Non-interactive zero-knowledge and its applications. In: Proceedings of the twentieth annual ACM symposium on Theory of computing. 1988. p. 103-12.
34. Ayed AB. A conceptual secure blockchain-based electronic voting system. Int J Netw Secur Its Appl. 2017;9(3):1-9.
35. Rivest RL, Shamir A, Adleman L. A method for obtaining digital signatures and public-key cryptosystems. Commun ACM. 1978;21(2):120-6.
36. King S, Nadal S. Ppcoin: Peer-to-peer crypto-currency with proof-of-stake. 2012. Available from: https://peercoin.net/assets/paper/peercoin-paper.pdf
37. De Angelis S, Aniello L, Baldoni R, Lombardi F, Margheri A, Sassone V. PBFT vs proof-of-authority: applying the CAP theorem to permissioned blockchain. In: Italian Conference on Cyber Security. 2018.
38. Douceur JR. The sybil attack. In: International workshop on peer-to-peer systems. Berlin: Springer; 2002. p. 251-60.
39. Wood G. Ethereum: A secure decentralised generalised transaction ledger. Ethereum Proj Yellow Pap. 2014;151(2014):1-32.
40. Rivest RL, Adleman L, Dertouzos ML. On data banks and privacy homomorphisms. Found Secur Comput. 1978;4(11):169-80.
41. Rivest RL, Shamir A, Tauman Y. How to leak a secret. In: International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer; 2001. p. 552-65.
42. Goldwasser S, Micali S, Rackoff C. The knowledge complexity of interactive proof systems. SIAM J Comput. 1989;18(1):186-208.
43. Luu L, Chu DH, Olickel H, Saxena P, Hobor A. Making smart contracts smarter. In: Proceedings of the 2016 ACM SIGSAC conference on computer and communications security. 2016. p. 254-69.
44. Bhargavan K, Delignat-Lavaud A, Fournet C, et al. Formal verification of smart contracts: Short paper. In: Proceedings of the 2016 ACM workshop on programming languages and analysis for security. 2016. p. 91-6.
45. Moura T, Gomes A. Blockchain voting and its effects on election transparency and voter confidence. In: Proceedings of the 18th Annual International Conference on Digital Government Research. 2017. p. 574-5.
46. Zissis D, Lekkas D. Addressing cloud computing security issues. Future Gener Comput Syst. 2012;28(3):583-92.
47. Park S, Specter M, Narula N, Rivest RL. Going from bad to worse: from Internet voting to blockchain voting. J Cybersecur. 2021;7(1):tyaa025.
48. Springall D, Finkenauer T, Durumeric Z, et al. Security analysis of the Estonian internet voting system. In: Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security. 2014. p. 703-15.
49. Chaum D. Secret-ballot receipts: True voter-verifiable elections. IEEE Secur Priv. 2004;2(1):38-47.
50. Benaloh J. Simple verifiable elections. In: Proceedings of the USENIX/Accurate Electronic Voting Technology Workshop 2006. 2006. p. 5.
51. Adida B. Helios: Web-based open-audit voting. In: Proceedings of the 17th USENIX Security Symposium. 2008. p. 335-48.
52. Cortier V, Galindo D, Küsters R, Mueller J, Truderung T. SoK: Verifiability notions for e-voting protocols. In: 2016 IEEE Symposium on Security and Privacy. 2016. p. 779-98.
53. Kiayias A, Zacharias T, Zhang B. End-to-end verifiable elections in the standard model. In: Annual International Conference on the Theory and Applications of Cryptographic Techniques. Berlin: Springer; 2015. p. 468-98.
54. Bernhard D, Pereira O, Warinschi B. How not to prove yourself: Pitfalls of the Fiat-Shamir heuristic and applications to Helios. In: International Conference on the Theory and Application of Cryptology and Information Security. Berlin: Springer; 2012. p. 626-43.
55. Hardwick FS, Gioulis A, Akram RN, Markantonakis K. E-voting with blockchain: An e-voting protocol with decentralisation and voter privacy. In: 2018 IEEE International Conference on Internet of Things and IEEE Green Computing and Communications and IEEE Cyber, Physical and Social Computing and IEEE Smart Data. 2018. p. 1561-7.
56. Heiberg S, Laud P, Willemson J. The application of i-voting for Estonian parliamentary elections of 2011. In: International Conference on E-Voting and Identity. Berlin: Springer; 2011. p. 208-23.
57. Germann M, Serdült U. Internet voting and turnout: Evidence from Switzerland. Elect Stud. 2017;47:1-12.
58. Braun Binder N, Rama Krishnan S. Switzerland's approach to digital democracy. In: Digital democracy in a globalized world. Cheltenham: Edward Elgar Publishing; 2020. p. 83-98.
59. Yavuz E, Koç AK, Çabuk UC, Dalkılıç G. Towards secure e-voting using ethereum blockchain. In: 2018 6th International Symposium on Digital Forensic and Security. 2018. p. 1-7.
60. Barnes A, Brake C, Perry T. Digital voting with the use of blockchain technology. 2016. Available from: https://www.economist.com/sites/default/files/plymouth.pdf
61. Hjalmarsson FB, Hreioarsson GK, Hamdaqa M, Hjalmtysson G. Blockchain-based e-voting system. In: 2018 IEEE 11th International Conference on Cloud Computing. 2018. p. 983-6.

62. Shahzad B, Crowcroft J. Trustworthy electronic voting using adjusted blockchain technology. IEEE Access. 2019;7:24477-88.
63. Specter MA, Koppel J, Weitzner D. The ballot is busted before the blockchain: A security analysis of voatz, the first internet voting application used in US federal elections. In: 29th USENIX Security Symposium. 2020. p. 1535-53.
64. McCorry P, Shahandashti SF, Hao F. A smart contract for boardroom voting with maximum voter privacy. In: International Conference on Financial Cryptography and Data Security. Berlin: Springer; 2017. p. 357-75.
65. Pawlak M, Poniszewska-Marańda A, Kryvinska N. Towards the intelligent agents for blockchain e-voting system. Procedia Comput Sci. 2018;141:239-46.
66. Zheng P, Zheng Z, Luo X, Chen X, Liu X. A detailed and real-time performance monitoring framework for blockchain systems. In: Proceedings of the 40th International Conference on Software Engineering: Software Engineering in Practice. 2018. p. 134-43.
67. Van Dijk J. The deepening divide: Inequality in the information society. Thousand Oaks: Sage Publications; 2005.
68. Norris P. Digital divide: Civic engagement, information poverty, and the Internet worldwide. Cambridge: Cambridge University Press; 2001.
69. De Filippi P, Hassan S. Blockchain technology as a regulatory technology: From code is law to law is code. First Monday. 2016;21(12).
70. Finck M. Blockchain regulation and governance in Europe. Cambridge: Cambridge University Press; 2019.
71. Nielsen J. Usability engineering. San Francisco: Morgan Kaufmann; 1994.
72. Acemyan CZ, Kortum P, Byrnes MD, Wallach DS. Usability of voter verifiable, end-to-end auditable voting systems: Baseline data for Helios, Prêt à Voter, and Scantegrity II. In: 2014 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections. 2014.
73. Sedlmeir J, Buhl HU, Fridgen G, Keller R. The energy consumption of blockchain technology: beyond myth. Bus Inf Syst Eng. 2020;62(6):599-608.
74. Chen T, Li X, Wang Y, Wang J. A balanced routing strategy for the blockchain-enabled sustainable Internet of Things. IEEE Internet Things J. 2021;8(7):5593-602.
75. Hargittai E. Second-level digital divide: Differences in people's online skills. First Monday. 2002;7(4).
76. Van Deursen AJ, Van Dijk JA. The digital divide shifts to differences in usage. New Media Soc. 2014;16(3):507-26.
77. Shor PW. Algorithms for quantum computation: discrete logarithms and factoring. In: Proceedings 35th annual symposium on foundations of computer science. 1994. p. 124-34.
78. Chen L, Jordan S, Liu YK, et al. Report on post-quantum cryptography. US Department of Commerce, National Institute of Standards and Technology; 2016.
79. Russell SJ, Norvig P. Artificial intelligence: a modern approach. 4th ed. Boston: Pearson; 2020.
80. Goodfellow I, Bengio Y, Courville A. Deep learning. Cambridge: MIT Press; 2016.
81. Zamyatin A, Harz D, Lind J, Panayiotou P, Gervais A, Knottenbelt W. Cross-chain protocols. In: Financial Cryptography and Data Security. Cham: Springer; 2019. p. 458-76.
82. Pillai B, Biswas K, Muthukkumarasamy V. Cross-chain interoperability among blockchain-based systems using transactions. Knowl Eng Rev. 2020;35:e23.
83. Buterin V. DAOs, DACs, DAs and more: An incomplete terminology guide. Ethereum Blog. 2014. Available from: https://blog.ethereum.org/2014/05/06/daos-dacs-das-and-more-an-incomplete-terminology-guide/
84. Beck R, Müller-Bloch C, King JL. Governance in the blockchain economy: A framework and research agenda. J Assoc Inf Syst. 2018;19(10):1020-34.
85. Kumar P, Singh R, Kumar A, Abdullah NA. Blockchain-based mobile voting system for secure and transparent elections. Mob Inf Syst. 2021;2021:1-15.
86. Quaheem KI, Al-Madeed S, Mahfoud H, et al. Mobile voting system using blockchain technology. In: 2021 IEEE 11th Annual Computing and Communication Workshop and Conference. 2021. p. 0716-22.
87. Reijers W, O'Brolcháin F, Haynes P. Governance in blockchain technologies & social contract theories. Ledger. 2016;1:134-51.
88. Wright A, De Filippi P. Decentralized blockchain technology and the rise of lex cryptographia. SSRN Electron J. 2015.
89. Houben R, Snyers A. Cryptocurrencies and blockchain: Legal context and implications for financial crime, money laundering and tax evasion. European Parliament Policy Department for Economic and Scientific Policy; 2018.
90. Zetzsche DA, Buckley RP, Arner DW, Föhr L. The ICO gold rush: It's a scam, it's a bubble, it's a super challenge for regulators. Univ Pa Law Rev. 2019;167:505.