International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

SECURE AND TRANSPARENT BLOCKCHAIN-BASED E-VOTING SYSTEM WITH SMART CONTRACTS, DIFFERENTIAL PRIVACY, AND EMAIL AUTHENTICATION

Ishrath Begum[1], Dr. Safia Khanam[2]
[1]PG Scholar, Department of CSE, Shadan Women's College of Engineering and Technology, Hyderabad, ishrathnazeer2003@gmail.com
[2]Associate Professor, Department of CSE, Shadan Women's College of Engineering and Technology safiakhanam89@gmail.com

ABSTRACT:
The primary mechanism usually used to preserve democracy in a particular society is election. Blockchain (BC) and other recent technology developments have previously been used in earlier projects to implement unconventional e-Voting systems. The primary objective of these suggestions is to retain openness, confidence, and distant elections while offering the required degree of security and dependability. However, BC's notoriety and dispersed nature created additional privacy and performance trade-off issues. By combining smart contracts for dependability and transparency, Differential Privacy to improve vote anonymity, and Self-Sovereign Identities (SSI) for maintaining decentralized identity and verifiable credentials, this study seeks to overcome current privacy and performance difficulties in e-voting. Specifically, a novel (k, ε)-differential privacy strategy is created that allows statistical vote approximation while maintaining anonymity by using a randomly chosen candidate as a pivot to redistribute retrievable votes to other candidates. In order to improve user engagement, the system also incorporates a real-time notification system that, following completion of the voting process, sends a confirmation message to the user's registered mobile device, such as "Vote successfully cast". Different transaction arrival speeds (10–80 TX/s), total votes cast (10k–50k), and numbers of elected candidates (2–8) are among the parameters under which the suggested techniques are assessed. The smart contract is built on a cloud-hosted, permissioned blockchain network utilizing Hyperledger Besu, with geographically dispersed nodes in Google's EU and USA data centers, in order to verify its realistic implementation. According to experimental data, BP-Vot outperforms current solutions in latency by 24% (≈ 1 s/TX vs. 1.24 s/TX). Additionally, the system regularly provides over 98% accuracy in estimated vote outcomes using a standardized Min-Max regression algorithm; accuracy increases linearly with vote volume. Additionally, the robustness of the suggested differential privacy model against reconstruction assaults is officially confirmed.
KEYWORDS: leakage-resilient anonymous multi-receiver encryption (LR-AMRE), leakage-resilient anonymous heterogeneous multi-receiver hybrid encryption (LR-AHMR-HE)

1. INTRODUCTION

Throughout history, voting has been an essential instrument for preserving democracy all across the world. Voting procedures are traditionally carried out using centralized, paper-based systems that are ineffective in terms of expense and public risk. E-Voting frameworks, which enable the use of electronic devices or systems to cast or count votes in an election, have been advocated in the literature as a solution to these problems [1]. E-voting still has numerous benefits over traditional paper-based voting, including increased accessibility, reduced cost, and superior efficiency, even if it is mostly centralized and has single points of failure [2]. These benefits have led to the announcement of numerous proposals and initiatives worldwide [3], [4], encouraging the adoption of e-Voting schemes to improve the prosperity of their nations' democratic processes (e.g. Switzerland [5], Kenya [6], Sri Lanka [7], Australia [8], India [9], Brazil [10], Nigeria [11], Russia [12], among others [13]). More sophisticated and reliable decentralized solutions typically use the Blockchain (BC) technology to achieve the required levels of decentralization, leading to public trust. A distributed ledger of transactions (TXs) that is safe, transparent, and unchangeable may be created and maintained thanks to BC, a ground-breaking technology [14]. Satoshi Nakamoto initially presented this technology in 2008 as the foundation for the cryptocurrency known as bitcoin [15]. Since then, BC has been used in a number of fields, including the Internet of Things (IoT) [16], banking [17], supply chain [18], healthcare [19], and electronic voting (e-Voting) [20]. By offering a decentralized and distributed platform for e-Voting that can improve the reliability and transparency of the voting process, BC technology presents a potential solution to some of the aforementioned issues [21]. Votes may be stored in an unchangeable, tamper-proof manner via BC-enabled e-Voting systems, and anybody can confirm the votes' accuracy and validity. By employing cryptographic methods like encryption, hashing, and zero-knowledge proofs, they can additionally safeguard voters' privacy and anonymity [22]. However, state-of-the-art technologies are rarely used in practical situations since they usually do not follow the most advised privacy-by-design principles. Ensuring the security, integrity, privacy, and verifiability of the voting process and outcomes presents several issues for BC-based e-Voting [23]. For example, contemporary e-Voting systems sometimes have

Received: 02-07-2026 | Accepted: 09-08-2026 | Published: 13-08-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

inadequate privacy controls despite technical developments, which might jeopardize voter data integrity and erode faith in these systems. Furthermore, while implementing e-Voting systems across different network tiers, from tiny communities to large-scale elections, scalability and performance concerns are crucial factors to take into account [24]. Additionally, as voters may not be aware with the technical features of the system, BC-based e-Voting systems must offer user-friendly interfaces and experiences. The security and privacy risks associated with their portions of the solution deployment are usually known to front-end DevOps teams. However, understanding BC technology as a facilitator of e-Voting through various ways (e.g. Smart Contracts) is closely tied to addressing privacy problems in the back-end. When developers are ignorant of the intricate techniques utilized by BC, it becomes more difficult for front-end, back-end, and system architects to handle privacy, security, and scalability requirements. The legal and regulatory frameworks of many nations and areas, which may have varying e-Voting needs and norms, must also be complied with by BC-based e-Voting systems [25]. For example, despite the mass adoption of BC technology in Europe, any application must adhere to the very strict General Data Protection Regulations (GDPR), aiming to protect the privacy of citizens in the continent. Neglecting the GDPR-compliance requirement might lead to billions of Euros paid as fines against system developers. We use a scenario where three votes are cast to our smart contract, simulating the three different forms of votes, to assess the system's privacy preservation. In this instance, demonstrating that our system offers a likely loss of privacy equal to ϵ (for all vote kinds) shows the robustness of our differential privacy approach. In order to protect privacy, we also consider the worst-case situation, in which there are only two candidates to choose from. In other words, the largest value of ϵ (φ = 0.5) may be obtained with the fewest candidates d = 2, as expressed in Equation 2. We begin with a user's vote for pivot candidate c0, as shown in Figure 11a. To determine whether this vote should be registered for C0 or transferred to another candidate, the smart contract creates a random float number ω. This vote is included in the list of c0 votes since ω was in fact smaller than ϵ. We may view the vote numbers at the conclusion of this phase.

OBJECTIVE

The primary goal of the BP-Vot-Lite project is to use blockchain technology to create a secure, decentralized, and privacy-preserving electronic voting system that guarantees the secrecy, integrity, and transparency of the whole voting process. The goal of this project is to use smart contracts to automate vote validation and result calculation, doing away with human interaction and reducing the possibility of fraud or manipulation. The system allows voters to verify themselves using verified digital identities in accordance with forthcoming Web 3.0 standards by integrating self-sovereign identity (SSI) techniques. Additionally, it uses sophisticated cryptographic and differential privacy approaches to protect voter anonymity, guaranteeing that individual votes are untraceable while preserving aggregate verifiability. The goal also includes making elections open and auditable so that all parties involved may confirm the outcomes without jeopardizing privacy. The project also places a strong emphasis on usability by providing administrators and voters with a contemporary, responsive, and user-friendly interface that enables easy registration, safe voting, and real-time result presentation. By achieving these objectives, BP-Vot-Lite hopes to create a reliable, GDPR-compliant, and cutting-edge electronic voting system appropriate for widespread democratic applications.

PROBLEM STATEMENT

Traditional voting systems, being centralized and paper-based, often suffer from inefficiency, high costs, and a lack of transparency, which can undermine public trust in democratic processes. While electronic voting (e-Voting) systems were introduced to address some of these challenges, most existing solutions remain centralized, creating single points of failure and making them vulnerable to tampering, data breaches, and operational inefficiencies. Although blockchain technology has emerged as a promising solution for enabling secure, transparent, and tamper-proof e-Voting, current blockchain-based systems still face significant issues. These include ensuring voter privacy, scalability, and regulatory compliance—particularly with frameworks such as the General Data Protection Regulation (GDPR). Additionally, the complexity of blockchain technology often hinders its adoption, as developers and system architects may struggle to implement privacy-by-design principles effectively. Therefore, there is a critical need for a reliable, privacy-preserving, and decentralized blockchain-based e-Voting framework that ensures data integrity, voter anonymity, and compliance with legal standards while maintaining user accessibility and operational efficiency.

EXISTING SYSTEM

Transparency, security, and tamper-resistance are the goals of current blockchain-based electronic voting systems. However, preserving voter privacy and attaining maximum speed are difficult due to blockchain's dispersed and public nature. These systems may pose privacy problems since they

Received: 02-07-2026 | Accepted: 09-08-2026 | Published: 13-08-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

frequently lack sophisticated ways to completely anonymize votes. Such systems are less practical for real-time or remote voting scenarios since managing large-scale elections with high transaction volumes can lead to performance bottlenecks and increased delay.

Disadvantages of Existing System

- Voters' selections might be exposed since votes are publicly viewable on the blockchain.
- Fake identities and Sybil attacks are possible due to the lack of a robust authentication technique.
- After voting, users do not receive a confirmation, which creates doubt.
- Vote counts are precise, providing no defense against inference or reconstruction assaults.

PROPOSED SYSTEM

In order to overcome these constraints, the proposed system introduces differential privacy for improved voter anonymity, smart contracts for transparent and dependable vote processing, and Self-Sovereign Identity (SSI) for decentralized identity management utilizing verified credentials. A pivot candidate technique is used to anonymize votes through redistribution in order to implement a new (k,ε)-differential privacy algorithm. A real-time notification system confirms successful voting by sending mobile alerts to enhance user participation. In a geographically dispersed, cloud-based blockchain network, the use of Hyperledger DIDs shows notable gains in latency, correctness, and privacy protection.

Advantages of Proposed System

- Self-Sovereign Identity (SSI) is integrated for safe and private voter verification.
- Uses tamper-proof algorithms to automate vote processing on a permissioned blockchain.
- Confirms "Vote Successfully Cast" to people by SMS or mobile message.

2. RELATED WORKS

Electronic voting has attracted significant research interest as governments and organizations seek secure, transparent, and efficient alternatives to traditional paper-based voting. Conventional electronic voting systems improve the speed of vote collection and counting; however, they often face challenges related to data integrity, voter privacy, transparency, and resistance to cyberattacks. These limitations have motivated researchers to investigate blockchain technology as a foundation for secure digital voting systems.[1]

Blockchain has emerged as a promising solution because of its decentralized architecture, immutable ledger, and cryptographic security. Several studies have proposed blockchain-based e-voting frameworks that eliminate the need for a central authority while ensuring that votes cannot be altered once recorded. These systems improve transparency by allowing authorized participants to verify election records without compromising the integrity of the voting process. However, many early blockchain-based approaches primarily focused on data immutability and auditability, while providing limited mechanisms for protecting voter privacy.[2]

To enhance election automation and trust, researchers have incorporated smart contracts into blockchain-based voting systems. Smart contracts automate essential election activities such as voter registration, vote validation, ballot casting, and result computation according to predefined rules. By eliminating manual intervention, smart contracts reduce the possibility of human error and unauthorized manipulation. Nevertheless, vulnerabilities in smart contract implementation and insufficient access control can introduce security risks if not carefully designed and tested.[3]

Protecting voter anonymity remains a critical challenge in electronic voting. Several research efforts have explored privacy-preserving techniques, including cryptographic protocols, homomorphic encryption, zero-knowledge proofs, and differential privacy. Among these methods, differential privacy provides an additional layer of protection by introducing controlled randomness into published statistical information, reducing the likelihood of identifying individual voters while preserving the overall usefulness of election results. Although differential privacy enhances confidentiality, it must be carefully configured to balance privacy protection and data accuracy.[4]

Authentication is another essential component of secure electronic voting. Existing voting systems employ various authentication mechanisms such as biometric verification, national identity cards, one-time passwords (OTP), and multi-factor authentication. Email-based authentication has gained attention as a practical and cost-effective approach for verifying voter identities, particularly in academic institutions and organizational elections. While email verification simplifies voter authentication, additional security measures such as encrypted communication and time-limited verification links are necessary to prevent unauthorized access and replay attacks.[5]

Despite the significant progress in blockchain-enabled electronic voting, many existing solutions focus on only one or two aspects of election security. Some systems emphasize transparency but provide limited privacy guarantees, whereas others strengthen privacy without offering comprehensive authentication mechanisms. Similarly, certain frameworks utilize blockchain and smart contracts but overlook practical voter verification techniques.[6]

The proposed research addresses these limitations by integrating blockchain technology, smart contracts, differential privacy, and email-based voter authentication into a unified electronic voting

Received: 02-07-2026 | Accepted: 09-08-2026 | Published: 13-08-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

framework. The proposed system ensures secure voter authentication, immutable vote storage, automated election management, enhanced voter privacy, and transparent result verification. By combining these complementary technologies, the system aims to provide a reliable, scalable, and trustworthy electronic voting solution suitable for modern digital elections.[7]

3. METHODOLOGY

MODULES:

Design of User Interfaces

In this module, we build the project's windows. These windows allow all users to safely log in. Users can only connect to the server after entering their username and password. If the user has already departed, they can log in straight to the server; otherwise, they must register their details, which include their email address, password, and username. The server will create an account for each user in order to maintain the upload and download speeds. The name will be linked to the user ID. Typically, you may access a certain site by logging in.

User Authentication Module

Both administrators and voters may securely log in using this module. To avoid credential breaches, passwords are hashed using SHA-256 or bcrypt before being stored. Voters and administrators can only view their own dashboards thanks to role-based access. Additionally, the system provides session management, keeps track of login attempts, and may incorporate OTP or CAPTCHA verification for added protection.

Voter Verifier

Administrators can confirm voter registration with this module. The administrator has the ability to verify identity papers, examine voter information, and accept or reject registrations. Voters who have been approved can log in to cast ballots after receiving activation emails. Only valid and distinct voters are allowed to cast ballots thanks to the verification.

Candidate Management

The administrator can add, modify, or remove candidate profiles using this module. Each candidate's name, party, and manifesto are included. The information is safely kept and then connected to votes when voting takes place. Voters may view candidate information on the voting page in real time.

Voting Module

This is the main functional module where authorized voters may safely cast their ballots. Using blockchain transaction linkage and authentication, the system guarantees one vote per voter. To avoid manipulation or repetition, every vote is digitally signed, encrypted, and sent to the blockchain ledger using a smart contract interface.

Vote Validation Module

After vote submission, the admin uses this module to validate and confirm recorded votes. The validation process includes checking digital signatures, timestamp verification, and ensuring integrity within the blockchain ledger. Invalid or duplicate votes are automatically rejected.

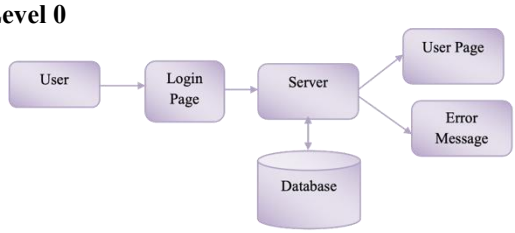
4. ALGORITHM

- **BP-Vot (Blockchain-based Private Voting with Differential Privacy and SSI)**

Numerous secure applications are needed Because of the growing risks of data manipulation, identity theft, and centralized manipulation, protecting the privacy, openness, and integrity of electronic voting systems has become a crucial concern in the current digital era. Blockchain-based Private Voting with Differential Privacy and Self-Sovereign Identity (SSI), or BP-Vot algorithm, is a sophisticated cryptographic voting system that combines decentralized blockchain technology with identity self-sovereignty and privacy-preserving strategies. Building a safe and auditable electronic voting environment that ensures voter anonymity, data security, and verifiable integrity without depending on a central authority is the main objective of BP-Vot. By distributing voting records across a blockchain ledger, BP-Vot ensures immutability, non-repudiation, and tamper-proof storage, in contrast to traditional electronic voting systems that rely on centralized databases susceptible to breaches or manipulation. Before being added to the chain, each transaction in BP-Vot represents a single vote and is hashed and encrypted. The blockchain framework ensures end-to-end verifiability and transparency of the election process by guaranteeing that once a vote is recorded, it cannot be changed or erased.

5. DATA FLOW DIAGRAM

Level 0



Level 1

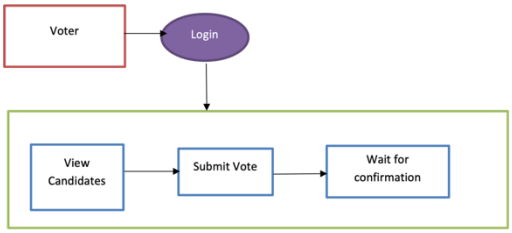


Fig 5: Data Flow Diagram

6. SYSTEM ARCHITECTURE

Received: 02-07-2026 | Accepted: 09-08-2026 | Published: 13-08-2026

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

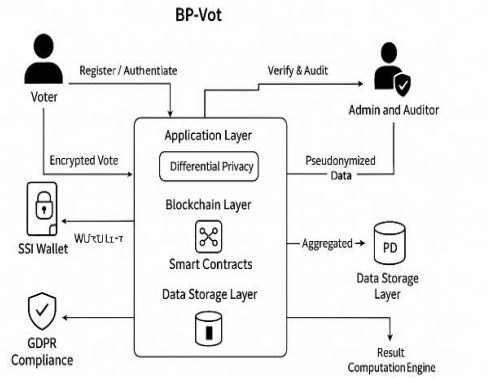
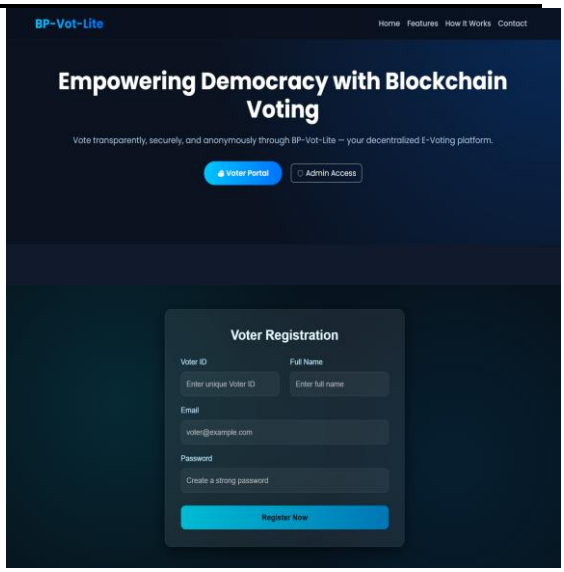


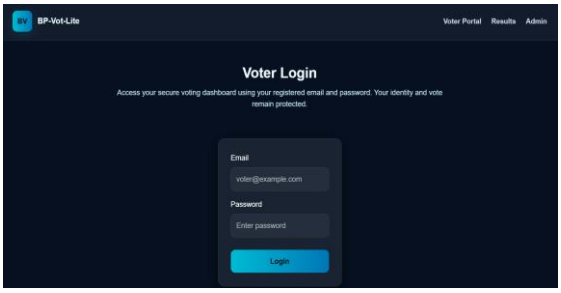
Fig 6: System Architecture

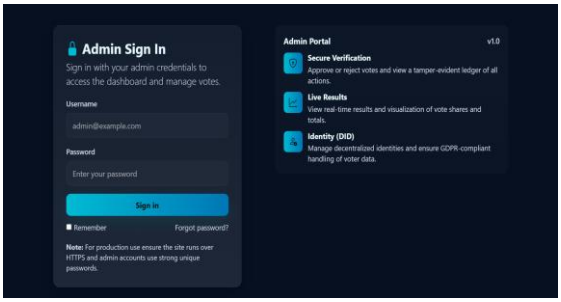
For example, when implemented on fully distributed infrastructure, BC and SC techniques are usually used to provide data immutability while preserving high levels of consistency. When anonymizing large data frameworks, differential privacy techniques are usually used to get high accuracy outputs in comparison to the original outputs. We developed a standardized self-sovereign identity management scheme since the combination of those techniques necessitated a third approach, which is in charge of maintaining identities at the end-user level before applying differential privacy measures. This intricate technology was made open-source so that the community may continue to contribute and conduct study. We anticipated during pre-testing that our system's latency would be marginally greater than that of systems without differential privacy techniques. Despite BC nodes being installed on separate continents (Cloud VMs hosted in the US and EU), our system beat both simulated and state-of-the-art systems when benchmarked with increasing the batch size. The hyperledger DID solution's refined techniques, which aim to achieve optimal processing costs in industry-level solutions as opposed to simulation-based non-optimized solutions, may serve as justification for the simulation.

7. RESULTS

The performance of the proposed blockchain-based e-voting system was evaluated based on registration efficiency, voter verification accuracy, vote processing speed, blockchain transaction performance, security validation, and result generation time. The analysis demonstrates that the system provides secure, transparent, and efficient election management while maintaining data integrity and voter privacy.







International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

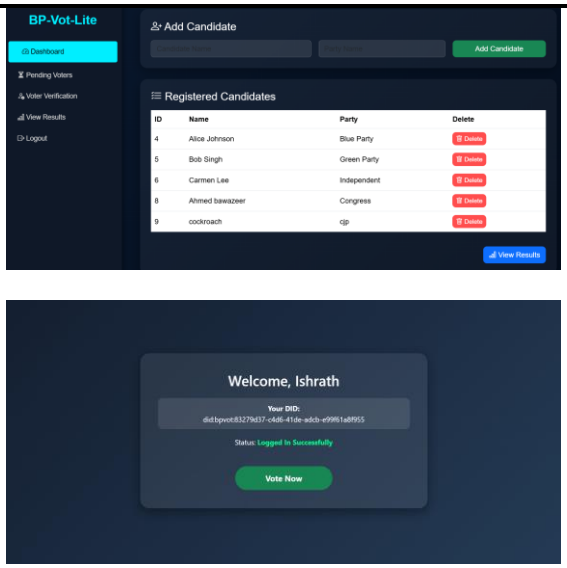


Fig 7: Results

8. FUTURE ENHANCEMENT

We developed and put into practice our differential privacy approach so that just one pivot candidate is chosen in order to demonstrate the concept. This is essentially enough to ensure the anonymity of every vote, regardless of the candidate who was first elected, as we have demonstrated. In the meanwhile, only estimated vote numbers are released, which is insufficient to determine who was first elected. We intend to look into the viability and usefulness of a parallel differential privacy approach in the future, where the anonymization mechanism is guided by many pivot possibilities rather than just one.

9. CONCLUSION

A safe, decentralized, and transparent voting system that guarantees voter anonymity and result integrity is successfully shown by the proposed BP-Vot: Blockchain-based Privacy-Preserving e-Voting System. The solution successfully tackles major issues with conventional and centralized e-voting platforms, including data manipulation, identity leakage, and single points of failure, by combining Blockchain technology, Smart Contracts, Differential Privacy, and Self-Sovereign Identity (SSI). By offering tamper-proof and auditable election records, the deployment on a Hyperledger Besu blockchain network improves decentralization and trust. According to experimental assessments, the system retains over 98% accuracy in vote aggregating while achieving up to 24% reduced latency, even when candidate numbers and vote volume change. The qualitative analysis demonstrates that BP-Vot maintains system scalability and performance while providing robust privacy protection as the number of votes rises. All things considered, BP-Vot is a major advancement toward the realization of a decentralized e-voting system that is trustworthy, GDPR-compliant, and privacy-preserving for practical democratic applications.

REFERENCES:

[1] J. P. Gibson, R. Krimmer, V. Teague, and J. Pomares, ‘‘A review of E voting: The past, present and future,’’ Ann. Telecommun., vol. 71, nos. 7–8, pp. 279–286, Aug. 2016.
[2] W. Bokslag and M. de Vries, ‘‘Evaluating e-voting: Theory and practice,’’ 2016, arXiv:1602.02509.
[3] M. Hapsara, ‘‘Reinstating e-voting as a socio-technical system: A critical review of the current development in developing countries,’’ in Proc. IEEE Region 10 Symp. (TENSYMP), May 2016, pp. 282–287.
[4] S. Risnanto, Y. B. A. Rahim, and N. Suryana, ‘‘Success implementation of E-voting technology in various countries: A review,’’ in Proc. FoITIC, Jan. 2020, pp. 150–155.
[5] L. E. Pleger and A. Mertes, ‘‘Use and assessment of E-voting systems: Findings from an online-survey among Swiss nationals living abroad,’’ Yearbook Swiss Administ. Sci., vol. 9, no. 1, p. 1, Sep. 2018.
[6] J. JumaandC.O.Oguk,‘‘Election results’ verification in e-voting systems in Kenya: A review,’’ Int. J. Social Sci. Inf. Technol., vol. 2020, pp. 1–14, Dec. 2020.
[7] R. H. A. Rathnayake, ‘‘Electronic voting system based on blockchain for Sri Lanka: Conceptual overview,’’ Int. J. Sci. Res., vol. 12, no. 2, pp. 114–125, Feb. 2023.
[8] T. Haines, ‘‘Review of the overseas e-voting (OSEV) system used in the Australian capital territory,’’ in Proc. 7th Int. Joint Conf. Electron. Voting, 2022, p. 102.
[9] M. Alam, I. R. Khan, and S. Tanweer, ‘‘Blockchain technology: A critical review and its proposed use in E-voting in India,’’ in Proc. Int. Conf. Innov. Comput. Commun. (ICICC), Jan. 2020, pp. 1–8.
[10] O. Okuro, ‘‘Comparative review of e-voting in India and Brazil: Key lessons for Kenya,’’ Lagos Historical Rev., vol. 21, no. 1, pp. 26–56, 2021.
[11] O. Osho, V. L. Yisa, and O. J. Jebutu, ‘‘E-voting in Nigeria: A survey of voters’ perception of security and other trust factors,’’ in Proc. Int. Conf. Cyberspace (CYBER-Abuja), Nov. 2015, pp. 202–211.
[12] A. Polushin, Y. Lanrong, and M. S. Nisar, ‘‘Exploring e-voting in Moscow region, Russia: A survey of voters’ perception of trust in government and other factors,’’ Int. J. Basic Sci. Appl. Comput., vol. 2, no. 5, pp. 1–9, 2018.
[13]M.O’Meara,‘‘Survey&analysisofe-votingsolutions,’’ M.S. thesis, Univ. Dublin,

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

Dublin, Ireland, 2013. [14] H. Baniata, A. Anaqreh, and A. Kertesz, ''Distributed scalability tuning for evolutionary sharding optimization with random-equivalent security in permissionless blockchain,'' Internet Things, vol. 24, Dec. 2023, Art. no. 100955.
[15] S. Nakamoto, ''Bitcoin: A peer-to-peer electronic cash system,'' Decentralized Bus. Rev., Oct. 2008, Art. no. 21260, doi: 10.2139/ssrn.3440802.
[16] A. Reyna, C. Martín, J. Chen, E. Soler, and M. Díaz, ''On blockchain and its integration with IoT. Challenges and opportunities,'' Future Gener. Comput. Syst., vol. 88, pp. 173–190, Nov. 2018.
[17] P. Treleaven, R. Gendal Brown, and D. Yang, ''Blockchain technology in finance,'' Computer, vol. 50, no. 9, pp. 14–17, 2017.
[18] P. Dutta, T.-M. Choi, S. Somani, and R. Butala, ''Blockchain technology in supply chain operations: Applications, challenges and research opportunities,'' Transp. Res., E, Logistics Transp. Rev., vol. 142, Oct. 2020, Art. no. 102067.
[19] A. Hasselgren, K. Kralevska, D. Gligoroski, S. A. Pedersen, and A. Faxvaag, ''Blockchain in healthcare and health sciences—A scoping review,'' Int. J. Med. Informat., vol. 134, Dec. 2019, Art. no. 104040.
[20] N. Kshetri and J. Voas, ''Blockchain-enabled E-voting,'' IEEE Softw., vol. 35, no. 4, pp. 95–99, Jul. 2018.
[21] J. Huang, D. He, M. S. Obaidat, P. Vijayakumar, M. Luo, and K.-K. R. Choo, ''The application of the blockchain technology in voting systems: A review,'' ACM Comput. Surv., vol. 54, no. 3, pp. 1–28, Apr. 2021.
[22] Y. Lin and P. Zhang, ''Blockchain-based complete self-tallying E-voting protocol,'' in Proc. Asia–Pacific Signal Inf. Process. Assoc. Annu. Summit Conf. (APSIPA ASC), Nov. 2019, pp. 47–52.
[23] R. Taş and Ö. Ö. Tanrıöver, ''A systematic review of challenges and opportunities of blockchain for E-voting,'' Symmetry, vol. 12, no. 8, p. 1328, Aug. 2020.
[24] K. M. Khan, J. Arshad, and M. M. Khan, ''Investigating performance constraints for blockchain based secure e-voting system,'' Future Gener. Comput. Syst., vol. 105, pp. 13–26, Apr. 2020.
[25] S. Tanwar, N. Gupta, P. Kumar, and Y.-C. Hu, ''Implementation of blockchain-based e-voting system,'' Multimedia Tools Appl., vol. 83, no. 1, pp. 1449–1480, Jan. 2024.
[26] M. Chaieb, M. Koscina, S. Yousfi, P. Lafourcade, and R. Robbana, ''DABSTERS: A privacy preserving e-voting protocol for permissioned blockchain,'' in Proc. Theor. Aspects Comput.-ICTAC, R. M. Hierons and M. Mosbah, Eds., Cham, Switzerland: Springer, Jan. 2019, pp. 292–312.
[27]S.Islam,M.J.Islam,M.Hossain,S.Noor,K.-S.Kwak,andS.M.R.Islam, ''A survey on consensus algorithms in blockchain-based applications: Architecture, taxonomy, and operational issues,'' IEEE Access, vol. 11, pp. 39066–39082, 2023.
[28] S. King and S. Nadal, ''PPCoin: Peer-to-peer crypto-currency with proof-of-stake,'' White Paper, Aug. 2012. [Online]. Available: https://api.semanticscholar.org/CorpusID:42319203
[29] V. Costan and S. Devadas. (2016). Intel SGX Explained. Cryptol. ePrint Arch.
[30] G.Wood,''Polkadot: Vision for a heterogeneous multi-chain framework,'' White paper, vol. 21, no. 2327, p. 4662, 2016.
[31]S.Wang,L.Ouyang,Y.Yuan,X.Ni,X.Han,andF.-Y.Wang,''Blockchain enabled smart contracts: Architecture, applications, and future trends,'' IEEE Trans. Syst., Man, Cybern., Syst., vol. 49, no. 11, pp. 2266–2277, Nov. 2019.
[32] H. Baniata and A. Kertesz, ''Partial pre-image attack on proof-of-work based blockchains,'' Blockchain, Res. Appl., vol. 5, no. 3, Sep. 2024, Art. no. 100194.
[33] N. Szabo, ''Formalizing and securing relationships on public networks,'' 1st Monday, vol. 2, no. 9, pp. 1–17, Sep. 1997.
[34] P. De Filippi, C. Wray, and G. Sileno, ''Smart contracts,'' Internet Policy Rev., vol. 10, no. 2, pp. 1–9, 2021.
[35] R. M. Aziz, R. Mahto, K. Goel, A. Das, P. Kumar, and A. Saxena, ''Modified genetic algorithm with deep learning for fraud transactions of Ethereum smart contract,'' Appl. Sci., vol. 13, no. 2, p. 697, Jan. 2023.
[36] P. Sharma, R. Jindal, and M. D. Borah, ''A review of smart contract-based platforms, applications, and challenges,'' Cluster Comput., vol. 26, no. 1, pp. 395–421, Feb. 2023.
[37] Home | Ethereum.org. Accessed: May 18, 2024. [Online].
[38] M. Jansen, F. Hdhili, R. Gouiaa, and Z. Qasem, ''Do smart contract languages need to be Turing complete?'' in Proc. Blockchain Appl., Int. Congr. Cham, Switzerland: Springer, Jun. 2019, pp. 19–26.
[39] Home | Go-Ethereum. Accessed: May 18, 2024.
[40] H. Foundation. (2019). Hyperledger BESU. Accessed: Apr. 19, 2024. [Online]. Available: https://www.hyperledger.org/projects/besu
[41] NetherMind | Blockchain Research & Software Engineering. Accessed: May 18, 2024. [Online]. Available: https://www.nethermind.io/
[42] Sepolia on Etherscan. Accessed: Mar. 30, 2024. [Online]. Available: https://sepolia.etherscan.io/
[43] Goerli TestNet. Accessed: Mar. 30, 2024. [Online]. Available: https:// goerli.net/
[44] R. H. Sahib and E. S. Al-Shamery, ''A review on distributed blockchain technology for E-voting systems,'' J. Phys., Conf. Ser., vol. 1804, no. 1, Feb. 2021, Art. no. 012050.
[45] N. A. Majeed, ''Review on blockchain based e-voting systems,'' Kon ferenzband

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

ZumSci.TrackderBlockchainAutumnSchool,vol.2021,no .4, pp. 1–8, 2021.
[46] S. A.-B. Salman, S. Al-Janabi, and A. M. Sagheer, ‘‘A review on E-voting based on blockchain models,’’ Iraqi J. Sci., vol. 2022, pp. 1362–1375, Mar. 2022.
[47] A. Benabdallah, A. Audras, L. Coudert, N. El Madhoun, and M. Badra, ‘‘Analysis of blockchain solutions for E-voting: A systematic literature review,’’ IEEE Access, vol. 10, pp. 70746–70759, 2022.
[48] M. H. Jumaa and A. C. Shakir, ‘‘Review study of E-voting system based on smart contracts using blockchain technology,’’ Iraqi J. Sci., vol. 2023, pp. 2001–2022, Apr. 2023.
[49] R. Barelli, ‘‘Towards secure electronic voting: A literature review on e voting systems and attacks,’’ Master thesis, Dept. Comput. Sci. Eng., School Ind. Inf. Eng., Milan, Italy, 2023.
[50] M.-V. Vladucu, Z. Dong, J. Medina, and R. Rojas-Cessa, ‘‘E-voting meets blockchain: A survey,’’ IEEE Access, vol. 11, pp. 23293–23308, 2023.
[51] N. S. Aswale, M. S. Mali, S. S. Irale, S. S. Dhoka, T. H. Mudaliar, G. Machhale, and R. G. Sonkamble, ‘‘Privacy preserved E-voting system using blockchain,’’ in Proc. Int. Conf. Smart Data Intell. (ICSMDI, Jan. 2021, pp. 1–7, doi: 10.2139/ssrn.3852951.
[52] J. Goyal, M. Ahmed, and D. Gopalani, ‘‘A privacy preserving e-voting system with two-phase verification based on Ethereum blockchain,’’ Preprint Res. Square, pp. 1–33, Jun. 2022.
[53] K. Košt’áll, R. Bencel, M. Ries, and I. Kotuliak, ‘‘Blockchain E-voting done right: Privacy and transparency with public blockchain,’’ in Proc. IEEE 10th Int. Conf. Softw. Eng. Service Sci. (ICSESS), Oct. 2019, pp. 592–595.
[54] W. Zhang, Y. Yuan, Y. Hu, S. Huang, S. Cao, A. Chopra, and S. Huang, ‘‘A privacy-preserving voting protocol on blockchain,’’ in Proc. IEEE 11th Int. Conf. Cloud Comput. (CLOUD), Jul. 2018, pp. 401–408.
[55] V. Neziri, I. Shabani, R. Dervishi, and B. Rexha, ‘‘Assuring anonymity and privacy in electronic voting with distributed technologies based on blockchain,’’ Appl. Sci., vol. 12, no. 11, p. 5477, May 2022.
[56] J. Thakkar, N. Patel, C. Patel, and K. Shah, ‘‘Privacy-preserving E voting system through blockchain technology,’’ in Proc. IEEE Int. Conf. Technol., Res., Innov. Betterment Soc. (TRIBES), Dec. 2021, pp. 1–6.
[57] S.T.Alvi,M.N.Uddin,L.Islam,andS.Ahamed,‘‘Aprivacy-awaredigital voting system employing blockchain and smart contracts,’’ in Proc. IEEE Asia–Pacific Conf. Comput. Sci. Data Eng. (CSDE), Dec. 2020, pp. 1–6.
[58] S. Chaisawat and C. Vorakulpipat, ‘‘Towards achieving personal privacy protection and data security on the integrated E-voting model of blockchain and message queue,’’ Secur. Commun. Netw., vol. 2021, pp. 1–14, Sep. 2021.
[59] Z. Xu and S. Cao, ‘‘Efficient privacy-preserving electronic voting scheme based on blockchain,’’ in Proc. IEEE Int. Conf. Smart Internet Things (SmartIoT), Aug. 2020, pp. 190–196.
[60] A. Alshehri, M. Baza, G. Srivastava, W. Rajeh, M. Alrowaily, and M. Almusali, ‘‘Privacy-preserving E-voting system supporting score voting using blockchain,’’ Appl. Sci., vol. 13, no. 2, p. 1096, Jan. 2023. [Online]. Available: https://www.mdpi.com/2076-3417/13/2/1096
[61] J. Huang, D. He, Y. Chen, M. K. Khan, and M. Luo, ‘‘A blockchain-based self-tallying voting protocol with maximum voter privacy,’’ IEEE Trans. Netw. Sci. Eng., vol. 9, no. 5, pp. 3808–3820, Sep. 2022.
[62] M. Sallal, R. de Fréin, and A. Malik, ‘‘PVPBC: Privacy and verifia bility preserving E-voting based on permissioned blockchain,’’ Future Internet, vol. 15, no. 4, p. 121, Mar. 2023. [Online]. Available: https://www.mdpi.com/1999-5903/15/4/121
[63]T.NguyenandM.T.Thai,‘‘ZVote:Ablockchain-basedprivacy-preserving platform for remote E-voting,’’ in Proc. IEEE Int. Conf. Commun. (ICC), May 2022, pp. 4745–4750.
[64] A. Mukherjee, S. Majumdar, A. Kumar Kolya, and S. Nandi, ‘‘A privacy preserving blockchain-based E-voting system,’’ 2023, arXiv:2307.08412.
[65] W. Chai, M. Liu, Z. Zhang, and L. Lv, ‘‘Blockchain-based privacy preserving electronic voting protocol,’’ Int. J. Netw. Secur., vol. 24, no. 2, pp. 230–237, Mar. 2022.
[66] V. Diaconita, A. Belciu, and M. G. Stoica, ‘‘Trustful blockchain-based framework for privacy enabling voting in a university,’’ J. Theor. Appl. Electron. Commerce Res., vol. 18, no. 1, pp. 150–169, Jan. 2023. [Online]. Available: https://www.mdpi.com/0718-1876/18/1/8
[67] T. Liu, Z. Cui, H. Du, and Z. Wu, ‘‘Privacy-preserving and verifiable electronic voting scheme based on smart contract of blockchain,’’ Int. J. Netw. Secur., vol. 23, no. 2, pp. 296–304, Mar. 2021.
[68]W.Xue,Y.Yang,Y.Li,H.H.Pang,andR.H.Deng,‘ ‘ACB-vote:Efficient, f lexible, and privacy-preserving blockchain-based score voting with anonymously convertible ballots,’’ IEEE Trans. Inf. Forensics Security, vol. 18, pp. 3720–3734, 2023.
[69] EIDAS Supported Self-Sovereign Identity, Eur. Parliament, Brussels, Belgium, 2019.
[70] Regulation (EU) 2024/1183 of the European Parliament and of the Council, Eur. Parliament Council Eur. Union, Brussels, Belgium, 2024.
[71] M. U. Hassan, M. H. Rehmani, and J. Chen, ‘‘Integration of differential privacy in blockchain for enhanced privacy preservation,’’ J. Parallel Distrib. Comput., vol. 145, pp. 50–74, Nov. 2020.

International Journal of
AI Electronics and Nexus Energy
Peer Reviewed, Referred & Indexed Journal
ISSN: 3070-0515 www.zesterapublications.com Original Research Paper

[72] N. Holohan, S. Antonatos, S. Braghin, and P. M. Aonghusa, ‘‘(k, ϵ)-anonymity: k-anonymity with ϵ-differential privacy,’’ 2017, arXiv:1710.01615.
[73] E-Voting Smart Contract. Accessed: Nov. 18, 2024. [Online]. Available: https://github.com/HamzaBaniata/Blockchain-based-e-Voting
[74] H. Baniata and A. Kertesz, ‘‘PriFoB: A privacy-aware fog-enhanced blockchain-based system for global accreditation and credential verifica tion,’’ J. Netw. Comput. Appl., vol. 205, Sep. 2022, Art. no. 103440. [75] B.Norton,‘‘Navigating the legal framework: Implementing a government backed digital identity in the United States,’’ Jurimetrics, J. Law, Sci. Technol., vol. 64, no. 2, p. 169, 2024.
[76] (2024). Memorandum of Cooperation on Digital Identities and Trust Ser vices to Implement Data Free Flow With Trust. Accessed: Oct. 31, 2024. [Online]. Available: https://instarstandards.org/news/eu-and-japan-sign memorandum-cooperation-digital-identities
[77] Ledgerwatch. GitHub—Ledgerwatch/Erigon: Ethereum Implementation on the Efficiency Frontier. Accessed: May 18, 2024. [Online]. Available: https://github.com/ledgerwatch/erigon
[78] Paradigmxyz. GitHub—Paradigmxyz/Reth: Modular, Contributor Friendly and Blazing-Fast Implementation of the Ethereum Protocol, in Rust. Accessed: Dec. 3, 2024. [Online]. Available: https://github.com/paradigmxyz/reth
[79] ChainLens EVMBlockchain Explorer. Accessed: Mar. 30, 2024. [Online]. Available: https://www.chainlens.com/
[80] Ganache One Click Blockchain. Accessed: Mar. 30, 2024. [Online]. Available: https://archive.trufflesuite.com/ganache/
[81] A. Kertesz, ‘‘Block the chain: Software weapons of fighting against COVID-19,’’ Computer, vol. 55, no. 9, pp. 43–53, Sep. 2022.
[82] C. Dwork and A. Roth, ‘‘The algorithmic foundations of differential privacy,’’ Found. Trends Theor. Comput. Sci., vol. 9, nos. 3–4, pp. 211–407, 2014.
[83] T. Pflanzner, H. Baniata, and A. Kertesz, ‘‘Latency analysis of blockchain based SSIapplications,’’ Future Internet, vol. 14, no. 10, p. 282, Sep. 2022.
[84] P. Jain, M. Gyanchandani, and N. Khare, ‘‘Differential privacy: Its technological prescriptive using big data,’’ J. Big.