Referendum Poll System: A Blockchain-Based Solution for Direct Democracy

Sonu Mondal*, Rohit Rana, Lina Pawar, Akanksha Vishwakarma, Prashant S. Lokhande
Department of Information Technology, Pillai College of Engineering, Navi Mumbai, India.

* Corresponding author. Email: mondalsoga19it@student.mes.ac.in (S.M.)
Manuscript received April 19, 2023; accepted June 25, 2023; published July 6, 2023.
DOI: 10.18178/IJBTA.2023.1.1.1-8

Abstract: The project, "Referendum Poll System," aims to enforce referendums and enable people to express their opinions directly, re-engaging them with politics and democracy. The current representative democracy fails to provide direct participation of people in the decision-making process. Online voting/polling systems can encourage active participation and prove to be cost-efficient and accessible to both state and voters. However, traditional voting systems pose challenges such as time-consuming processes and physical presence requirements. Vote tampering also poses credibility issues, and the risk of getting hacked or submitting to an authority with administrator access to the system exists. The blockchain technology used in the Referendum Poll System distributes authoritative power and provides data confidentiality, integrity, and voter anonymity. The voters can read and pass judgement on every clause in a policy and approve or reject the policy as a whole or just the clauses. The "policy flaw detection feature" helps identify problematic clauses in policies, and real-time poll results add transparency. Overall, the Referendum Poll System provides an opportunity for direct and secure participation of the public in the decision- making process, and the blockchain technology used in the system addresses several challenges posed by traditional voting systems.

Keywords: Blockchain, referendum, poll, proof of stake, Ethereum

1. Introduction

Democracy nowadays relies on population consensus achieved through voting. Most countries use the traditional ballot system, which needs centralized power with a trusted third party to conduct the voting process, as well as record and tally the ballots. However, this opens the door to corruption and vote manipulation. As a result, an electronic voting, has been proposed as a better alternative to the ballot system, asit promises to reduce costs and decrease manual intervention.

However, concerns about privacy, accountability, decentralized authority, data security, confidentiality, and compliance requirements have prevented the widespread implementation of e-voting systems. Elections are a competitive process, which requires us to create a systemthat is extremely secure and not vulnerable to attacks by participants. Cryptography alone cannot protect such a process. If the party conducting the elections discovers or manipulates the secret key used in the cryptographic process, the entire system is compromised.

In such an environment, it is important to utilize technologies such as Distributed Ledger, with Blockchain being an ideal option for this purpose. The Blockchain network can be either permissionless, allowing anyone to interact with the network like Bitcoin or Ethereum, or permissioned, such as Hyperledger Fabric, Hyperledger Sawtooth, or Exonum, where only authorized members can access the network.

Another crucial issue to address is the voter's anonymity. With new discoveries and developments in the field of bigdata analytics, voter information has become susceptibleto discovery and alteration. To preserve voter anonymity, techniques such as one-time wallets and encryption algorithmscan be employed.

2. Literature Survey

1) Vivek *et al*. (2020) [1] paper proposes a Smart Contracts based implementation and suggests various authentication and security methods, including Elliptical Curve Cryptography, Blind Signature, and Hyperledger Sawtooth Framework.
2) Ahmed *et al.* (2020) [2] provides a detailed examination of smart contracts, including their operationalmechanism using Ethereum and Hyperledger Fabric as example. The article also explores mainstream platforms and potential application scenarios for smart contracts. Additionally, it discusses the challenges currently facing smart contracts andfuture development trends.
3) Killer *et al.* (2020) [3] proposes a system that allowsfor querying and verifying votes, but it has poor integrityverification because the transactions are not signed.
4) Yi (2019) [4] proposes a P2P network e-voting system that uses Proof of Work. It is a Linux-based application and supports casting and withdrawing votes. It allows querying andverifications of votes.
5) Wang *et al.* (2019) [5] provides a comprehensive overview of smart contracts, and their operational mechanisms using Ethereum and Hyperledger Fabric as examples, mainstream platforms, and application scenarios. It also discusses the challenges ahead, possible solutions, and future development trends.
6) Ko *et al.* (2020) [6] proposes an extensible and modular staking architecture for PoS systems, which includes a bucket- based data structure for enhanced flexibility and extensibility. The article evaluates the security of the system against typical PoS attacks and concludes that the Polkadot (Hybrid POS) mechanism offers the best results.
7) Varma *et al.* (2020) [7] proposes a web-based voting system using distributed computing that doesn't need manual tallying. It involves using aadhar token for protection of the voter. It prohibits an individual from casting a ballot once again and voting from all party sources is weighted toget the final votes the participant has won.
8) Alvi *et al.* (2019) [8] proposes a blockchain-based distributed infrastructure that employs smart contracts to en- able all electors to participate in the registration and validityof ballots. Its goal is to increase trust among the electorate and reduce the waste of electoral resources. The future planis to make the solution cost-effective during implementation.
9) Lyu *et al.* (2019) [9] proposes an e-voting system that uses smart contracts, linkable ring signature, and a threshold encryption system on top of Ethereum to preserve privacy. The linkable ring signature is used to group a signing ring for each voter, which hides their identity and prevents multiple voting.
10) Mishra *et al.* (2020) [10] proposes a voting system that is transparent and tamper-proof. The system's efficiency improves over time through data analysis of the information collected during the election period. The data can be usedto make improvements to the system. Additionally, electronic counting produces accurate results instantly.
11) Patidar and Jain (2019) [11] paper proposes anelectronic voting portal that utilizes smart contracts from Ethereum for storing voter accounts, candidate details, and votes. The system was tested on a virtual client and overcomesthe limitations of centralized voting systems.
12) Yang *et al.* (2020) [12] paper introduces a blockchain-based asymmetric polling system model and pro- poses a clustering algorithm to analyze it. The model uses Markov chains and probability generating functions to derive the asymmetry Gated and asymmetry Exhaustive and establisha data model. The average queue length and average waiting time are used to compare and verify the correctness of the scheme.
13) Jafar *et al.* (2021) [13] paper says that blockchain-basedtechnology is still not adopted widely as an electronic voting option. To establish a sustainable blockchain-based electronic voting system, the security of remote participation needs to be viable, and transaction speed must be addressed for scalability.
14) Prabhu *et al.* (2021) [14] proposes a secure internet voting system that employs two-step authentication using face recognition and OTP systems to overcome draw- backs in traditional voting systems. The system's key features include correctness, verifiability, and convenience.
15) Kaudare *et al.* (2020) [15] proposes a blockchain-based electronic voting system that utilizes Hyperledger to conduct secure elections while guaranteeing user privacy. The study compares Ethereum and Hyperledger and concludes that Hyperledger is more efficient than Ethereum in most performance metrics. Being permissioned, Hyperledger allowsfor maintaining voter privacy.

3. Architecture

The proposed architecture for Referendum Poll System is based on blockchain technology (Fig. 1). The system is designed to ensure the anonymity of voters while providing a secure and transparent polling process. The architecture utilizes the Proofof Stake (PoS) consensus algorithm, which is considered a more efficient alternative to the traditional Proof of Work (PoW) algorithm.

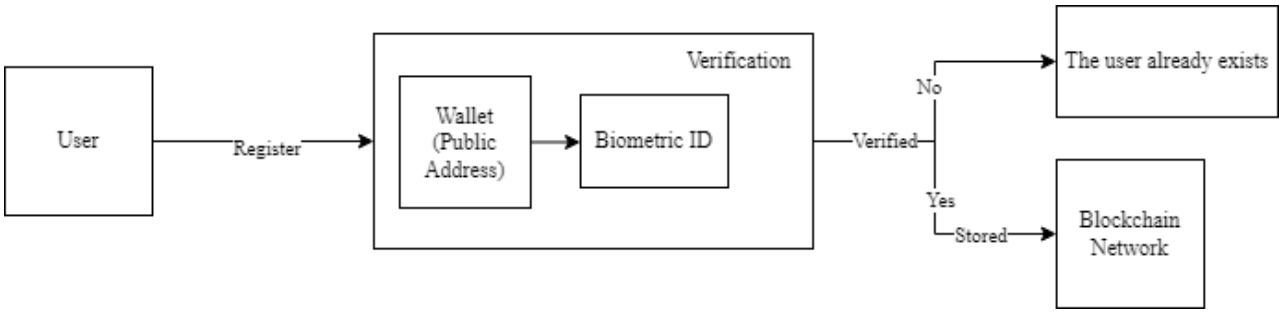

Fig. 1. User registration system architecture.

Anonymity is a crucial factor in any polling system to maintain the integrity of the process. The proposed architecture ensures that the voter's identity remains anonymous throughout the polling process. The system also verifies the voters to prevent fraud and ensure that only eligible individuals participate in the polling process. Additionally, the system ensures data integrity by not allowing voters to withdraw their votes after casting them.

The PoS consensus algorithm is used in the proposed architecture for several reasons. Firstly, it is a permissionless blockchain network that allows anyone to participate in the consensus process, ensuring transparency and openness. Secondly, PoS facilitates faster transactions as blocks are approved more quickly. Validators are chosen based on the number of tokens they hold, eliminating competition between miners as seen in PoW. Validators must stake cryptocurrency assets to participate and earn rewards, which also enhances the security of the network.

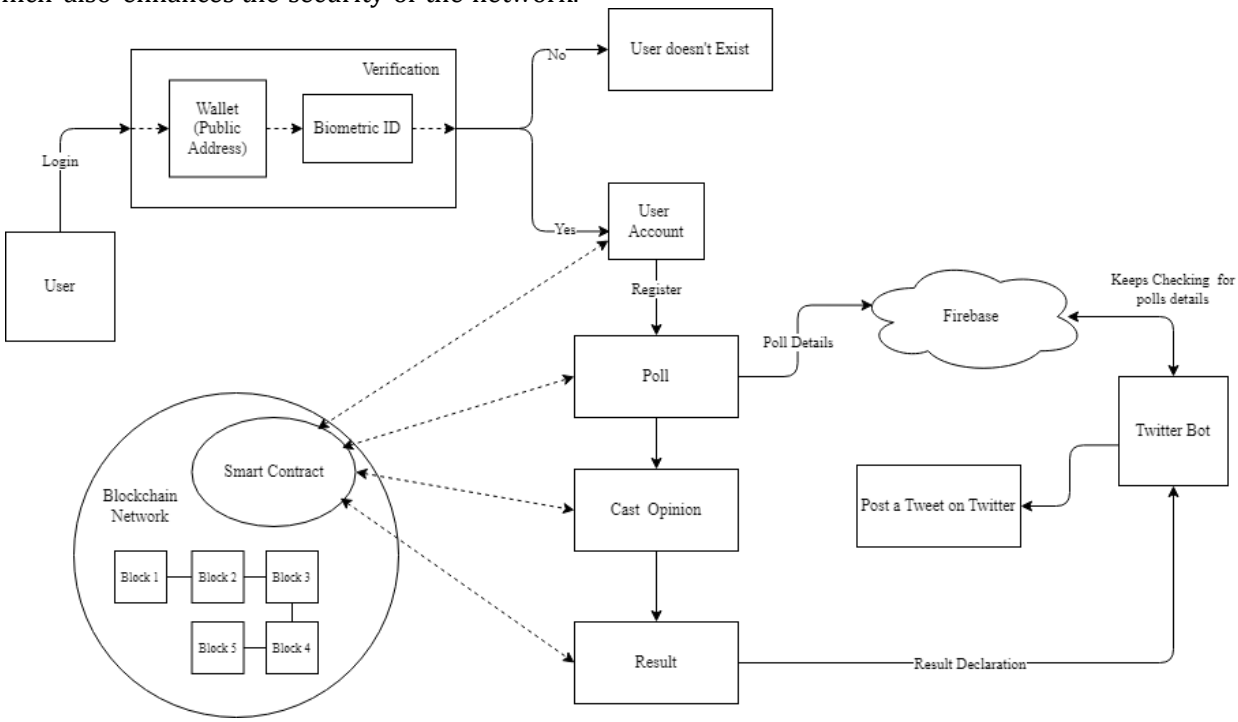

Fig. 2. System architecture.

Overall, the proposed architecture provides a secure and efficient solution for managing Referendum Poll System (Fig. 2). The architecture ensures anonymity, verification, and data integrity while utilizing a faster and more secure consensus algorithm in the form of PoS.

4. Design and Implementation

4.1. Methodology

1) **Ethereum**: Blockchain platform Ethereum is open- source and decentralized. The creation and execution of smart contracts and decentralized apps are supported by it (DApps). Ethereum is a decentralized system that runs on a global network of computers as opposed to conventional centralized systems, making it censorship- and single point of failure- resistant. The native cryptocurrency of the platform is referred to as Ether (ETH), and it is employed to cover transaction costs and provide incentives for network users to maintain network security. It supports the creation of decentralized autonomous organizations, which are organizations that work on the blockchain without any central authority. Ethereum is append-only ledger so any data stored inside is secured against manipulation.
2) **Solidity**: The Ethereum blockchain uses the high-level programming language Solidity to create smart contracts. With smart contracts, the details of the agreement between the buyer and seller are directly encoded into lines of code. These contracts self-execute. As a contract-oriented language, Solidity is intended for the creation of contracts that automatically carry out tasks when predetermined criteria are met. The most common language for this purpose is Solidity, which is used to create decentralized apps (DApps) on the Ethereum blockchain. Solidity is created to be dependable and safe, with built-in features like access control, data type, and exception handling to guard against frequent programming mistakes and weaknesses. Because it is object-oriented, developers may write reused code and control contract complexity.
3) **Truffle**: The Truffle Ethereum development framework offers a number of tools and modules that make it simpler for programmers to build, test, and deploy decentralized apps (DApps) and smart contracts on the Ethereum blockchain. Several helpful aspects of Truffle include:

a) Truffle makes it simple to write and test contracts in a development environment by streamlining the compilation and deployment of smart contracts on the Ethereum network.
b) Testing of contracts: Truffle comes with a framework for testing that enables programmers to create and execute tests to validate the functionality of their smart contracts.
c) Truffle has tools for managing smart contracts, including those for monitoring dependencies between contracts, confirming ownership, and controlling upgrades.
d) Interact with the blockchain: Through its console, Truffle allows developers to execute commands and interact directly with smart contracts on the Ethereum blockchain.

Truffle is a popular tool in the Ethereum development community for creating complex DApps and smart contracts.

4) **Ganache**: Developers can construct and test smart contracts and decentralized apps (DApps) in a local development environment using Ganache, a personal blockchain for Ethereum development. The Truffle collection of Ethereum development tools includes Ganache.

Developers can build a local blockchain with a set of pre-funded accounts using Ganache, which can then be used to communicate with smart contracts. In order to test their contracts and decentralized applications (DApps) in a sandboxed environment without having to connect to the live Ethereum network, developers can use Ganache, which simulates the behavior of the Ethereum blockchain, including mining, block confirmation, and transaction processing.

The graphical user interface (GUI) that comes with Ganache shows important details about the neighbourhood blockchain, such as account balances, transaction histories, and contract occurrences. This knowledge may be used by developers to test their contracts' functionality and debug any issues they may have. With the ability to quickly prototype and test their contracts and DApps in a safe and regulated environment, Ganache is an effective tool for Ethereum developers.

5) **MetaMask**: MetaMask is a cryptocurrency wallet and browser extension which allows users for storing, managing and interacting with decentralized applications securely on Ethereum blockchain. With MetaMask, users can simply connect to dapps with a few clicks, create and manage numerous Ethereum accounts, and transfer and receive ether and other ERC-20 tokens. Other security features provided by MetaMask are password protection, two-factor authentication and the ability to create and store encrypted backups of your wallet. Overall, MetaMask is a powerful and user-friendly tool.
6) **Smart Contracts**: Self-executing computer programs called as "smart contracts" are used to automatically enforce the terms of a contract between two parties. They are built on blockchain technology and allow safe transactions that are trustworthy. From financial transactions and supply chain management to voting systems and real estate deals, smart contracts can be used to

automate a variety of activities. They offer a high degree of security and dependability, transparency and are tamper-proof. Smart contracts have the ability to completely change how we conduct business and communicate with one another by facilitating quicker, less expensive, and more effective transactions.

7) **Proof of Stake**: Proof of stake (PoS) is a consensus mechanism used by blockchain networks for validating transactions and creating new blocks (Fig. 3). It is a way to decide which user or users validate new blocks of transactions and earn a reward for doing so correctly. It enables users to stake their own cryptocurrency as collateral for verifying transactions and build new blocks, in contrast to proof-of- work (PoW). PoW makes it necessary for miners to carry out difficult computations to solve mathematical equations. In a PoS system, a participant's chance of validating a block and earning a reward is proportional to the amount of cryptocurrency they stake. This approach is considered to be more cost-effective and energy-efficient than PoW.

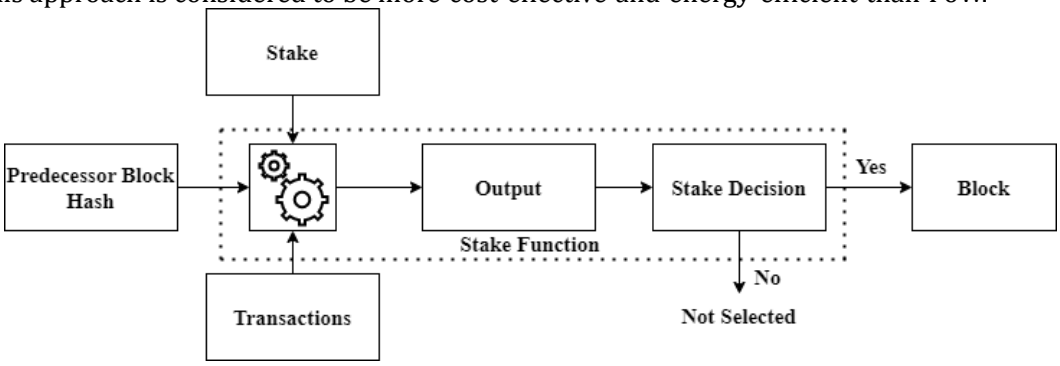

Fig. 3. Working of proof-of-stake.

4.2. Design

The system design for a blockchain-based referendum poll involves voter registration, poll creation, vote casting,and result publication (Fig. 4). The blockchain ensures security and immutability throughout the process.

Step 1: Setup

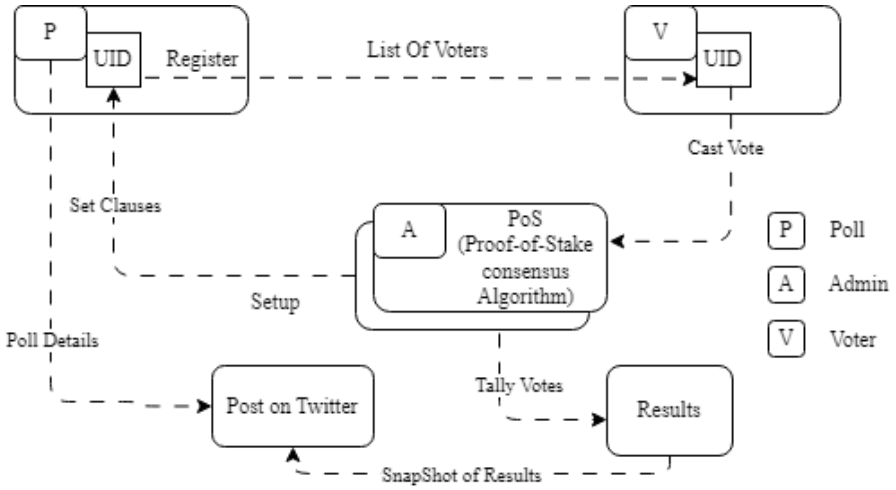

Fig. 4. System overview.

The process involves appointing an Admin who will havetshe authority to create polls, verify users, and publish results. The Admin's public address and unique id (UID) are taken into consideration during registration. The Admin establishes the parameters for the referendum poll, such as the age of participants, duration of the poll, and the voting options (yes, no, abstain). Once the required parameters are set, a blockis generated with the specified data. To eliminate the risk of collision, the Admin is kept separate from the voting process and does not participate in it.

Step 2: Register

Individuals who possess cryptocurrency wallets can enroll themselves on the platform by using their

public addresses along with biometric identification (UID). Once registered, they can view the active polls and join in by registering with the system. When users enroll, their public address is addedto the list of eligible voters for the poll.

Step 3: Cast Vote

To cast a valid vote the voter's public address is matched against the participant's list. If the address is confirmed as valid and the voter has not already cast a duplicate vote forthe policy, the vote is accepted. The system restricts voters from casting their votes after the voting period has elapsed.

Step 4: Results

Following the end of the voting period, the system releasesthe vote counts for public viewing. The poll results are published on social media via a bot for people to know their opinion. The bot will check the polls that have endedand then tweet the results snapshot with respective webpage links. The blockchain technology used ensures the results are tamper-proof, providing an added layer of security.

5. Results and Analysis

In order for a system to be extensively used, it should be cost-effective. For this, we've designed a system that is both efficient and cost-effective. Our system is built on Ethereum blockchain, which allows handling heavy network business with ease. The use of blockchain technology ensures that the datais tamper-proof and provides high security.

Table 1 provides a breakdown of the gas used for calculation of each function in the smart contract, the total Ether (Eth) needed for the transaction and cost in Indian Rupees (INR) grounded on the Eth conversion rates. The data clearly shows that the cost incurred while using our system is significantly lower than the overall cost that the government would have to bear for conducting a poll using traditional methods.

Our system offers a low-cost approach to conduct pollswithout compromising on security or reliability with tothe power of blockchain technology. This means that the government can save a significant amount of money while still ensuring that the polls are conducted in a fair and transparent manner. The tamper-proof nature of the data also ensures that the system is resilient to any attempts at malicious activity or tampering.

Our system offers an effective and secure solution for conducting polls, with low costs and high efficiency. Thepotential benefits of our system are highlighted in Table 1, demonstrating its significance in the field of democratic governance. Its reliability and ability to handle heavy traffic make it an attractive option for both personal and businessuse. We believe that our system represents a significant advancement in the field of democratic institutions, and weare confident that it will play a key role in shaping their future.

TABLE 1. Function Based Cost Analysis

Sr. No.	Function	Eth	Gas used	INR
1	User/Admin Register	0.0017584	87920	224.11
2	Poll Creation	0.08191666	4095833	10479.57
3	Register for Poll	0.00090242	45121	115.45
4	Cast Vote	0.00209656	104828	268.21

6. Conclusion and Future Scope

The main objective of developing a Referendum Poll System is to facilitate direct participation of citizens in the decision-making process pertaining to a proposed bill, law, or policy by their elected representatives or relevant organizations. The Referendum Poll system will handle the voter information and enable them to log in to exercise their voting rights. It will encompass all essential features of aVoting system and provide the necessary tools for managing votes on each bill or policy. The Referendum Poll System is a crucial tool in promoting transparency, accountability, and citizen participation in the democratic process.

One potential area of improvement for the referendum poll system on the blockchain network is to incorporate asmart contract mechanism that can verify the age of voters, thereby ensuring that only those who are eligible and meetthe minimum age requirement can participate in the voting process. To achieve this, an oracle service can be used to retrieve the age of the voter from a trusted third-party source, such as a government-issued ID or driver's license, and the smart contract can validate this information before allowing the voter to cast their vote. Additionally, Hyperledger can be used for cost-free transactions, and features like multilingual support and demographics-based poll restrictions can be added to improve the

user experience.

Conflict of Interest

The authors declare no conflict of interest

Author Contributions

All authors equally contributed.

References

[1] S. K. Vivek, R. S. Yashank, Y. Prashanth, N. Yashas, and M. Namratha, "E-voting systems using blockchain: An exploratory literature survey," in *Proc. 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA)*, Coimbatore, India, 2020, pp. 890–895.

[2] A. M. Razu *et al*., "The future of electronic voting system using blockchain," *International Journal of Scientific & Technology Research*, vol. 9, pp. 4131–4134, 2020.

[3] C. Killer, B. Rodrigues, R. Matile, E. Scheid, and B. Stiller, "Design and implementation of cast-as-intended verifiability for a blockchain-based voting system," in *Proc. the 35th Annual ACM Symposium on Applied Computing*, ACM, Mar. 30, 2020.

[4] H. Yi, "Securing e-voting based on blockchain in P2P network," *EURASIP Journal on Wireless Communications and Networking*, Springer Science and Business Media LLC, vol. 2019, no. 1, May 28, 2019.

[5] S. Wang, L. Ouyang, Y. Yuan, X. Ni, X. Han, and F.-Y. Wang, "Blockchain-enabled smart contracts: Architecture, applications, and future trends," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, Institute of Electrical and Electronics Engineers (IEEE), vol. 49, no. 11, pp. 2266–2277, Nov. 2019.

[6] S. Ko, X. Fan, Z. Zhong and Q. Chai, "EMS: An extensible and modular staking architecture for proof-of-stake systems," in *Proc. 2020 Second International Conference on Blockchain Computing and Applications (BCCA)*, Antalya, Turkey, 2020, pp. 122–128.

[7] C. S. P. Varma, D. S. Rahul, J. Jose, B. K. Samhitha and S. C. Mana, "Aadhar card verification base online polling," in *Proc. 2020 4th International Conference on Trends in Electronics and Informatics (ICOEI)(48184)*, Tirunelveli, India, 2020, pp. 479–483.

[8] S. T. Alvi, M. N. Uddin, L. Islam, and S. Ahamed, "A privacy-aware digital voting system employing blockchain and smart contracts," in *Proc. 2020 IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)*, Gold Coast, Australia, 2020.

[9] J. Lyu, Z. L. Jiang, X. Wang, Z. Nong, M. H. Au, and J. Fang, "A secure decentralized trustless e-voting system based on smart contract," in *Proc. 2019 18th IEEE International Conference on Trust, Security and privacy In Computing And Comm*unications*/13th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE)*, Rotorua, New Zealand, 2019, pp. 570–577.

[10] A. Mishra, A. Bajpai and A. Mishra, "Implementation of blockchain for fair polling system," in *Proc. 2020 International Conference on Smart Electronics and Communication (ICOSEC)*, Trichy, India, 2020, pp. 638–644.

[11] K. Patidar and S. Jain, "Decentralized e-voting portal using blockchain," in *Proc. 2019 10th International Conference on Computing, Com- munication and Networking Technologies (ICCCNT)*, Kanpur, India, 2019, pp. 1–4.

[12] Z. Yang and Q. Kou, "Research on performance of asymmetric polling system based on blockchain," in *Proc. 2020 IEEE 6th International Conference on Computer and Communications (ICCC)*, Chengdu, China, 2020, pp. 127–131.

[13] U. Jafar, M. J. A. Aziz, and Z. Shukur, "Blockchain for electronic voting system—review and open research challenges," *Sensors*, vol. 21, no. 17, p. 5874, Aug. 31, 2021.

[14] S. Ganesh Prabhu, A. Nizarahammed., S. Prabu., S. Raghul., R. R. Thirrunavukkarasu, and P. Jayarajan, "Smart online voting system," in *Proc. 2021 7th International Conference on Advanced Computing and Com- munication Systems (ICACCS)*, Coimbatore, India, 2021, pp. 632–634.

[15] A. Kaudare, M. Hazra, A. Shelar, and M. Sabnis, "Implementing electronic voting system with blockchain technology," in *Proc. 2020 International Conference for Emerging Technology (INCET)*, Belgaum, India, 2020, pp. 1–9.