JETIR.ORG ISSN: 2349-5162 | ESTD Year : 2014 | Monthly Issue
JOURNAL OF EMERGING TECHNOLOGIES AND INNOVATIVE RESEARCH (JETIR)
An International Scholarly Open Access, Peer-reviewed, Refereed Journal

Decentralized Voting using Blockchain

Dr.K.Gomathi

Assistant Professor, Department of Information Technology & Cognitive Systems,
Sri Krishna Arts and Science College, Coimbatore, India

Abstract

In the modern age, establishing a secure and transparent electoral process is paramount to ensure the integrity of democratic decision-making. An innovative solution to address the challenges of election security and voter trust is an electronic voting system leveraging blockchain technology. This technology guarantees that each voter can cast a single vote, free from any tampering or disruption. The blockchain's decentralized and transparent nature safeguards the sanctity of the electoral process, preventing any external interference.

This system transforms each vote into a unique transaction recorded on a distributed ledger, ensuring transparency and accountability. The real-time tallying of votes allows for prompt reporting of results. Elections, a cornerstone of democracy worldwide, have historically faced issues such as voter fraud and low turnout, undermining the democratic process.

To overcome these challenges and revitalize the electoral process, this paper introduces a suite of innovative electronic voting solutions. These advances are designed to bolster voter confidence, streamline the voting process, and strengthen the foundations of democracy in the digital age.

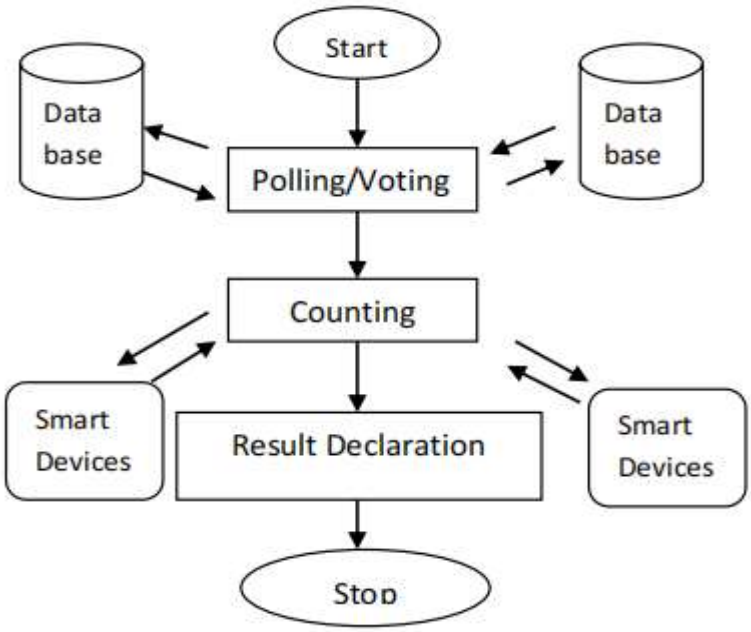
Keywords: *Blockchain, e-voting, security, transparency, decentralization, smart contracts.*

1 Introduction:

Extensive research has delved into the realm of electronic democratic systems, offering citizens the convenience of voting using a variety of electronic devices, including mobile phones, personal computers, and other electronic gadgets. Blockchain technology, with its core features of permanence, security, decentralization, transparency, and anonymity, has emerged as a robust contender for creating highly secure and direct electronic voting systems. Its rapid integration into various sectors has made blockchain-based voting a notably safe and viable option.

1.1 Online Voting Frameworks

Online voting systems represent a democratic evolution wherein citizens can exercise their voting rights from any corner of the country. While innovative and social media-driven political decision-making organizations have sparked debates on web-based voting, electronic voting stands ready to revamp traditional voting methods, making them more accessible and streamlined. The internet, if used as a medium for casting votes, presents the possibility of democratic participation through any computer with an internet connection. This approach not only simplifies the voting process but also reduces barriers to voting, thereby fostering broader civic engagement.



1.2 Benefits of Online Voting

The advantages of online voting extend to cost reduction and increased accessibility for a diverse range of voters. By providing multiple avenues for casting their votes, this method can eliminate the need for citizens to endure long lines at polling stations. Furthermore, it offers enhanced accessibility to individuals facing various challenges, such as those with mental health conditions, those in the military, expatriates, and those living in remote areas. Online voting also accommodates the flexibility of time, granting voters the opportunity to cast their ballots at their convenience.Internet connectivity for remote areas is important in the blockchain voting which is being referred to as one of the critical components. Drawings of offline blockchain solutions or mesh networks make it easier to understand how these methods work. An example of a diagram would illustrate mesh networks using decentralized communication frameworks so that things in distant parts can communicate with one another, thus entirely getting rid of the necessity for internet. There may also be another visual presentation showing how satellite-based internet allows a connection of on-the-ground voting systems with blockchain nodes for secure and fluid involvement in an election. Offline blockchain solutions, such as mesh networks and satellite-based internet, make it possible to ensure the participation of voters in low-connectivity regions. An example—mesh networks—can allow for decentralized communication frameworks that would enable the transfer of information without reliance on outdated internet infrastructure.

1.3 Engaging Young Voters

An intriguing aspect of online voting lies in its potential to attract younger voters, particularly those aged 18 to 30. The internet serves as a compelling platform to engage this demographic, which traditionally represents a challenging group to reach through conventional voting channels. The method of convergence is gamification tied to blockchain voting and providing rewards for participants or even having proof of involvement in a particular activity, which seems appealing to the younger segment. Targeting particular campaigns hinged like these, with social media analytics, on understanding the residents' concerns and what points of interest draw them and how they speak could likely contribute positively toward rate increase in participation. It's more interesting and easier.

Incorporating these advancements into the electoral process not only bolsters democracy but also aligns with the evolving digital landscape, ensuring that more citizens can participate in shaping the future of their nations.

The advantages of blockchain voting systems:

1. Transparency and Auditability
2. Security
3. Decentralization
4. Accessibility
5. Elimination of Double Voting

6. Real-time Verification
7. Trustworthiness
8. Reduced Administrative Costs
9. Accessibility for Remote Voting
10. Increased Voter Engagement

With regard to future threats caused by advancements in quantum computing, security enhancement incorporates the application of post quantum cryptography. Lattice based structures which have proven to be resistant to quantum attacks can be utilized to shield the blockchain systems from technological threats of the future.

2. Literature Survey

Syada Tasmia Alvi et al. (2022): Proposed "DVT Chain," a blockchain-based digital voting system utilizing Ethereum 2.0 and smart contracts to enhance security and transparency. Voter information is stored as hashes, ensuring privacy and reducing costs. Offers increased voter trust and verifiability by allowing voters to verify their votes after the election. Provides maximum security properties, including anonymity, integrity, security, privacy, fairness, verifiability, and mobility.

Mr. Shreeyash Pednekar et al. (2022): Explored the application of blockchain technology in electronic voting systems to enhance transparency and tamper resistance. Emphasized quicker, cost-effective elections, instant vote tabulation, open-source voting platforms, and improved accessibility.

Ahmed Ben Ayed (2017): Investigated the use of open-source blockchain technology to create a reliable and decentralized electronic voting system. Emphasized decentralization and transparency while highlighting the potential vulnerability to hacking due to malicious software on voters' devices.

Madhuri Chavan et al. (2020): Proposed an online voting system incorporating blockchain technology for security, efficiency, and transparency. Emphasized authentication methods and strong encryption for integrity. Highlighted cost-effectiveness, efficiency, and accessibility in the electoral process.

Prof. Pallavi Shejwal et al. (2019): Explored challenges in traditional electoral systems and introduced blockchain technology to address security and transparency concerns. Focused on blockchain's decentralized nature for database manipulation prevention.

Dipali Pawar et al. (2019): Explored blockchain as a service for secure and decentralized electronic voting. Addressed fairness, privacy, and verifiability while ensuring voter privacy, encryption, and vote integrity.

Prof. Anita A. Lahane et al. (2020): Proposed blockchain technology as a solution to challenges in modern elections, addressing issues like voter manipulation and hacking. Ensured transparency, cryptographic security, and voter anonymity. Discussed blockchain's potential for more democratic processes.

Haibo Yi (2019): Discussed the significance of secure electronic voting and introduced a blockchain-based solution within a peer-to-peer network. Addressed security through blockchain, user authentication, and vote change/update mechanisms. Acknowledged the need for further research in addressing potential vulnerabilities to quantum computer attacks.

The proposed systems require empirical comparisons from various studies to validate their efficacy. The table below summarizes all performance metrics that concerned scalability, security, and cost effectiveness of the voting blockchains versus traditional voting systems:

Metric	Blockchain Voting System	Traditional Voting System
Scalability	High (Supports large-scale elections with sharding or layer-2 solutions)	Medium (Limited by physical infrastructure)
Security	Very High (Incorporates cryptographic security and immutability)	Medium (Prone to tampering and fraud)
Cost-Effectiveness	High (Reduces administrative costs, especially for remote voting)	Low (Higher logistical and labor costs)
Voter Accessibility	High (Remote and disabled voters included)	Medium (Accessibility varies by location)
Real-time Results	Immediate (Real-time tallying via blockchain)	Delayed (Manual counting required

This comparison shows that blockchain voting systems outperform others with respect to scalability and security, although challenges in the implementation like integration of post-quantum cryptography in the system need to be dealt with for effective long term survival. In this case, however, such systems and their proposals have to be validated for effectiveness. Performance metrics such as transaction speed, cost per vote, and level of participation serve to illustrate the advantages and benefits of blockchain voting systems over voting systems already in existence.

3. Limitations:
While there are benefits of blockchain-based e-voting, it also presents several limitations and challenges:

- **Quantum Computing Vulnerability:** [9] acknowledges that the use of ECC public key cryptography in blockchain is not secure against quantum computer attacks. This is a significant limitation as quantum computing technology advances, and future research should focus on developing countermeasures to address this vulnerability.

Post-quantum cryptography, which entails lattice-based approaches, includes the use of complex mathematical structures such as lattices to develop encryption systems that can withstand quantum computer attacks. A diagram illustrating this can depict how lattice-based cryptographic operations, like key generation and encryption, integrate within the blockchain framework. For example, the diagram might show:

1. Key Generation: Using specific algorithms, users derive public and private keys from lattice problems (difficult mathematical lattices like the Shortest Vector Problem (SVP)).
2. Encryption Process: A transaction or a vote is encrypted using a public key, in a manner that can only be decrypted by the corresponding private key.
3. Blockchain Integration: The public transaction can be placed on the blockchain, providing quantum resistance as well as transparency and immutability.
4. Verification: Users that receive the transaction can verify the cryptographic proof of the transaction without revealing a previously agreed upon private value.

This visual will clarify how lattice cryptography not only enhances blockchain's security but also future-proofs it against quantum threats. and hash-based digital signatures, provides viable solutions to counter vulnerabilities introduced by quantum computing.

- **Cost:** The encrypted vote in the blockchain during vote casting is stored. This data will not be used after the end of the election. For storing these data, the cost has increased.[1].

- **Disguise Voting:** [3] While the system is secure, hackers have the ability to cast a vote using malicious software already installed on the voter's device.

- **Legal and Regulatory Challenges:** [8] Overcoming legal and regulatory obstacles, such as compliance with existing election laws and gaining the trust of regulatory bodies, is a crucial challenge.

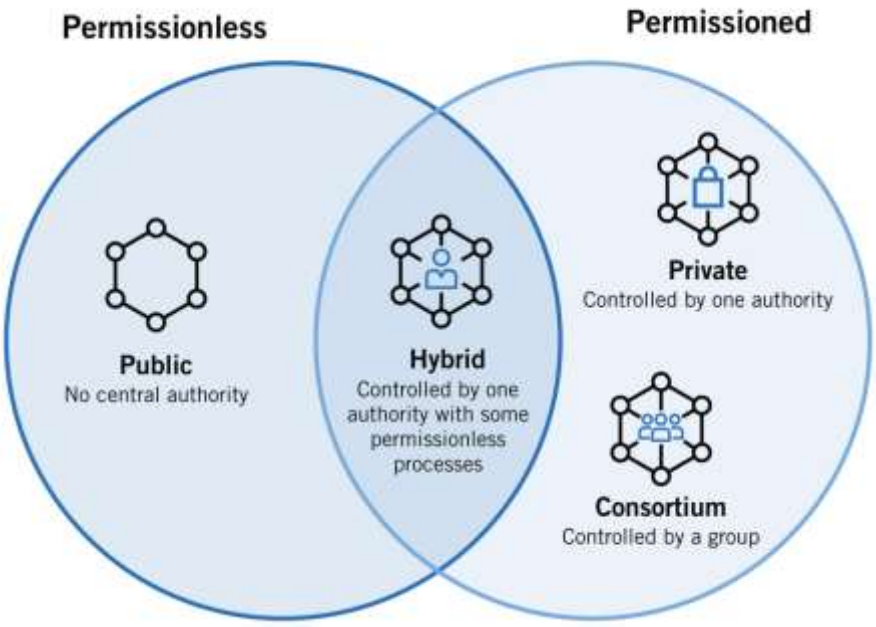
These limitations underscore the need for careful consideration and further research when implementing blockchain-based e-voting systems to ensure their effectiveness, security, and accessibility in real-world election scenarios.

4. Blockchain for E-Voting

Blockchain, initially introduced in the context of cryptocurrency by Nakamoto in 2008, has emerged as a significant trend for a wide range of businesses. It operates as a distributed ledger, where data is not held in a fixed dataset. Instead, information is continually updated across all nodes within the network, emphasizing three key elements: segregation, transparency, and consistency.

Blockchain transactions are grouped into blocks. Once a block is verified by peer nodes, it is permanently added to the blockchain, ensuring a chronological record of activities. Each block encapsulates a summary of transactions, creating a sequential, permissioned ledger for secure data sharing. Notably, the blockchain is decentralized, meaning it is maintained by the entire network rather than a single entity, enhancing security.

The name "blockchain" derives from its structure. Transactions are grouped into "blocks," and each new block is linked to the previous one, forming a chain. It operates as a distributed database managed by a peer-to-peer network, serving as a reliable repository for data storage and retrieval.



Within each block, a header includes essential information, such as a hash of the previous block, a timestamp, a nonce, and a Merkle root value. This cryptographic structure ensures the immutability of data once it's added to the blockchain. There are four types of Block Chain.

Public Blockchain:

✓ Open to anyone, permissionless.
✓ Decentralized, no central authority.
✓ Transparent transactions.
✓ Examples: Bitcoin,

Ethereum.Private Blockchain:
- ✓ Restricted, permissioned access.
- ✓ More centralized control.
- ✓ Privacy options.
- ✓ Examples: Hyperledger Fabric, Corda.

Consortium (Federated) Blockchain:
- ✓ Semi-permissioned, predefined group.
- ✓ Balances openness and control.
- ✓ Multiple organizations collaborate.
- ✓ Examples: R3 Corda, EEA (Enterprise Ethereum Alliance).

Hybrid Blockchain:
- ✓ Combines public and private elements.
- ✓ Offers flexibility in access control.
- ✓ Suitable for varied use cases.
- ✓ Examples: Dragonchain, MultiChain.

Blockchain serves as a tamper-resistant record, allowing multiple parties to share information with confidence. Unlike traditional data storage on a single server, blockchain data is distributed across various nodes, making it exceptionally challenging to alter or delete. This inherent trust in data integrity contributes to its growing importance in various industries.

Truffle

Truffle is a developer-friendly tool designed to simplify the creation of blockchain-based applications, particularly on the Ethereum platform. It offers developers the capability to build and test smart contracts using popular programming languages like JavaScript. One of its standout features is its command-line interface, providing essential commands for tasks such as compiling, deploying, and debugging smart contracts. This interface streamlines interaction with the blockchain, making development more efficient.

Ethereum and Ethers

Ethereum is an open-source blockchain platform known for its versatility. It allows developers to build and deploy decentralized applications (DApps) to meet various needs. Unlike traditional internet services, Ethereum uses a network of volunteer-operated nodes to replace centralized cloud servers. These nodes collaborate to form a global decentralized computer. Ethereum's decentralized model provides enhanced security and ensures that users maintain control over their personal information. Ether, the native cryptocurrency of Ethereum, acts as both a currency for transactions and a form of collateral. It doesn't rely on third-party intermediaries for validation, making it a powerful asset for applications running on the Ethereum network.

Web3.js

Web3.js serves as a JavaScript library that acts as a bridge between developers and smart contracts. It provides a simplified way to interact with decentralized applications, allowing developers to access the functionality of their smart contracts. Depending on the complexity of a DApp, developers can leverage Web3.js for integrating complex logic written in JavaScript or connecting their DApps to various blockchain networks through a JSON-RPC interface. This library facilitates direct communication with the blockchain and can be used in command-line operations.

MetaMask

MetaMask is a user-friendly cryptocurrency wallet and an essential tool for developers. It enables testing and evaluating transactions within DApps. MetaMask seamlessly integrates with local blockchain development environments. To connect your Truffle console to MetaMask, simply copy your localhost URL and set up a custom RPC (Remote Procedure Call) accessible for network expansion. It also provides a user-friendly interface and acts as an intermediary between users and the blockchain, making it easy for users to interact with DApps. MetaMask notifies users about transaction fees, which may need to be paid in cryptocurrencies for blockchain network usage.

Ganache

Ganache is an integral part of the Truffle Suite, which includes a set of developer tools. Ganache allows users to create a local, in-memory blockchain environment for development and testing purposes. It specifically focuses on executing smart contracts within the context of Ethereum transactions. This feature-rich tool aids developers in simulating blockchain environments locally, making it easier to test and deploy smart contracts.

5. Methodology:

In the process of implementing a blockchain-enabled electronic democratic framework, it's vital to consider the existing and previous e-voting systems. Various stages involving role definitions, structural assessments, security, and legal considerations should be carefully examined. Throughout this paper, the designed system is refred as "EVOTE," which aims to provide a real-time online application for voting, suitable for various scales, from organizations to villages and national elections. The goal is to create a user-friendly application that can function even on older systems used in villages. Detailed diagrams and the interplay of interactions with smart contracts is a positive improvement in the understanding of the advanced diagrams of the architecture of the EVOTE system. Such illustrations help to comprehend the processes of voter registration, authentication, voting, and the validation of results.

In the electoral system, we define each election as a smart contract. This means that in the network, the election is essentially a contract agreed upon by participating nodes. A well-defined smart contract outlines the roles of each participant, the election processes, and the terms and conditions during the election.

Each participant must be categorized into specific roles, and some individuals may hold the same or different roles:

a) Administrators:

- ✓ Administrators have oversight over all election operations.
- ✓ They are responsible for tasks such as validating the election, closing the election at the specified time, counting and disclosing the results.
- ✓ They can also be involved in creative aspects of the election process.

b) Voters:

- ✓ Voters are the primary participants who cast their votes in an election.
- ✓ They can verify their eligibility, provide self-certification, and submit their votes through the application.
- ✓ Voters have the ability to both cast their votes and confirm the votes they have submitted.

c) Constituency Nodes:

- ✓ Administrators use smart contracts to define the election process and incorporate the appropriate constituency nodes, each representing a distinct region.
- ✓ These constituency nodes play a critical role in voter authentication through smart contracts.
- ✓ Once a voter is verified by all constituency nodes, their vote is processed and added to the blockchain, ensuring security and transparency in the election process.

The EVOTE system leverages blockchain technology to facilitate trustworthy and secure elections, streamlining the voting process and enhancing the democratic experience for participants.

5.1 Election as a Smart Contract:

In our democratic framework, we define an election as a smart contract. Within our network, an election is essentially a binding agreement among participating nodes. Defining a smart contract for an election entails outlining the roles of each participant, the election processes, and the terms and conditions governing the election.

5.2 Election Process:

The election process is orchestrated through a set of smart contracts that are deployed onto the blockchain. These smart contracts are structured by the roles assigned to participants within the network.

Administrators: Administrators hold the authority to initiate the election, add candidates, verify registered candidates, and conclude the elections. They can create voting ballots using decentralized applications, define candidates, and designate voting constituencies. The smart contract generates the ballot and deploys it onto the blockchain.

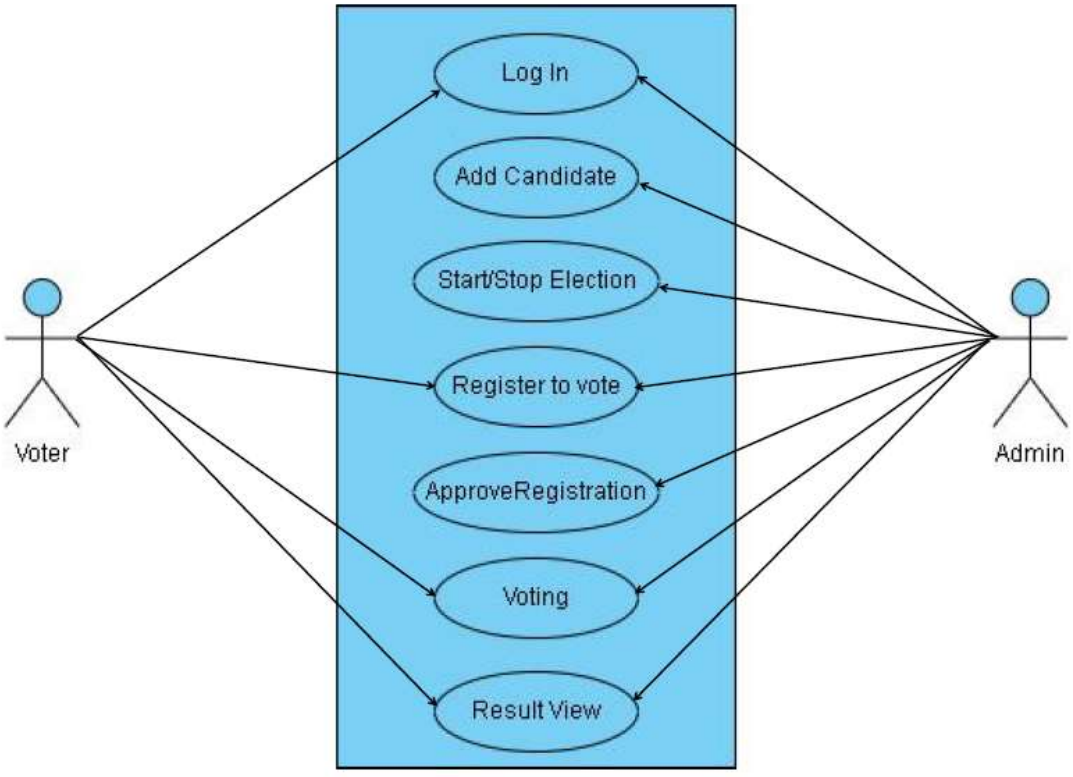
Voter Registration: The voting process consists of several procedures. Voters can register through the registration tab using a private key generated on the administrator's server. To verify each voter, the administrator is required to expend gas (ethers). Verification is based on the voter's ID and name provided during pre-registration.

Casting Votes: When an individual voter casts their vote, they interact with a secret ballot. The smart contract communicates with the blockchain, and if the code matches, the vote is added. Once a voter has cast their vote, they cannot cast another, as the private key generated is valid for a single use per individual.

Announcing Results: Concluding the election requires the crucial step of announcing the winner. Given the digital nature of the process, the count of votes cast for each candidate is automatically determined, and the administrator closes the polling. Subsequently, each voter can view the results on the website via their systems.

5.3 Actual Project Architecture:

The project's architecture is as follows:



a) Admin Actions:

- ✓ The administrator initiates a voting instance by deploying the system on a blockchain network, specifically the Ethereum Virtual Machine (EVM).
- ✓ Subsequently, the administrator creates an election instance and commences the election. During this setup, they input all relevant election details, including the list of candidates.

b) Voter Registration:

- ✓ Potential voters connect to the same blockchain network.
- ✓ They register as voters within the system.
- ✓ Upon successful registration, their details become visible in the administrator's panel, specifically on the verification page.

c) Admin Verification:

- ✓ The administrator reviews the registration information provided by users, which includes the blockchain account address, name, and phone number.
- ✓ The administrator validates the information and cross-references it with their records to ensure accuracy.
- ✓ If the information aligns and is valid, the administrator approves the registered user, granting them eligibility to participate and cast their vote in the election.

d) Casting Votes:

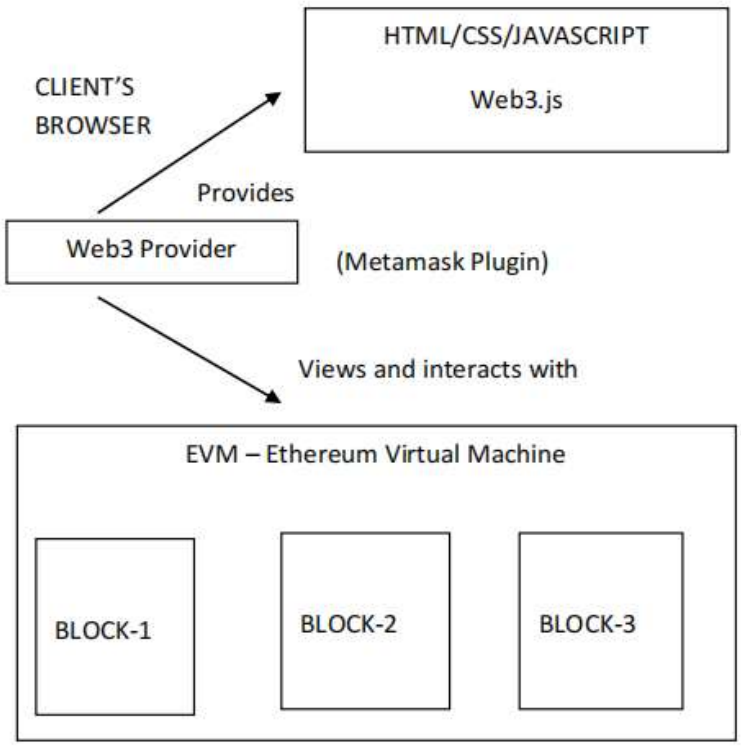
- ✓ Following approval from the administrator, registered users (voters) can cast their votes for their preferred candidate via the voting page.

e) Election Conclusion:

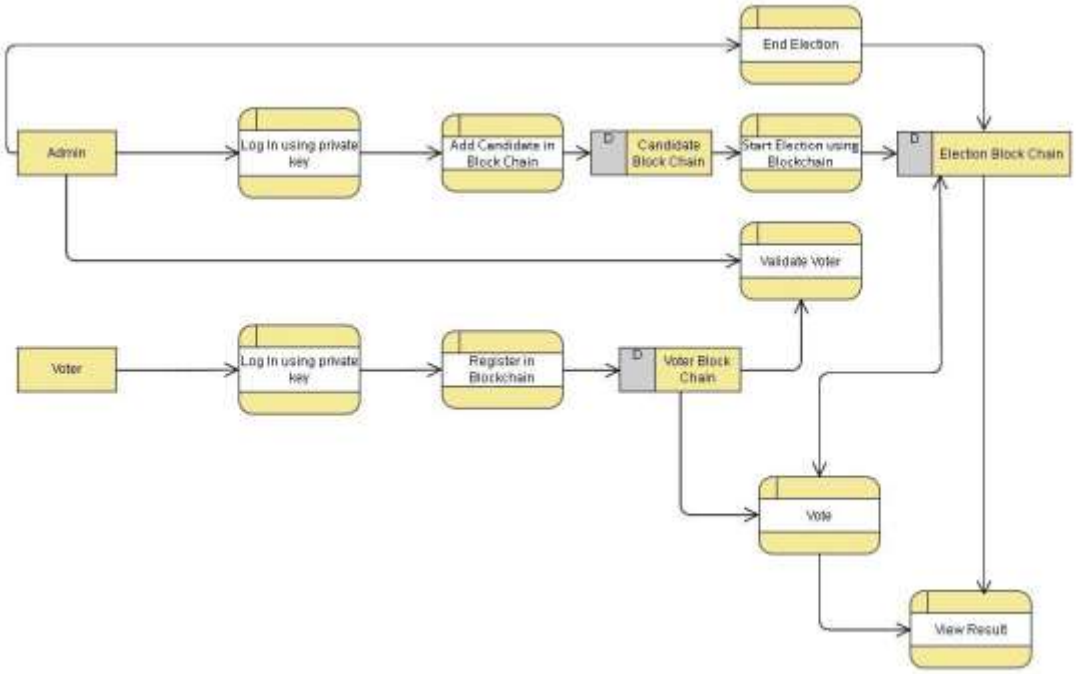
- ✓ The administrator concludes the election after a predetermined time, which may vary depending on the scale of the election.
- ✓ As the election closes, the voting process is terminated.
- ✓ The results are then displayed, announcing the winner at the top of the results page.

This architecture ensures a secure and transparent electoral process, where administrators oversee the setup and execution of elections, and registered voters can easily and confidently cast their votes.

The client's browser, serving as the Web3 provider, supplies web3.js with HTML, CSS, and JavaScript resources. Additionally, the client's browser is equipped with a MetaMask plugin, enabling it to view and interact with the Ethereum Virtual Machine.



The administrator initiates elections by deploying the system on the Ethereum Virtual Machine (EVM) and configuring the election details by adding the candidates for the election and the admin starts the election. Once the election is started the potential voters register through their browsers, and the administrator validates their information. Once verified, registered users access the voting page and cast their votes. After a set duration, the administrator concludes the election, and the system automatically tallies the votes, displaying the results. The data flows between the administrator, voters, and the system, utilizing browsers as the interface, while the EVM handles the underlying blockchain transactions. This architecture ensures secure and transparent online elections, enhancing the democratic process.



6. Implementation :

Proposing a comprehensive solution that harnesses the power of blockchain while mitigating potential risks

1. **Universal Identity Verification:** Establish a robust system that securely connects individuals to their digital identities on the blockchain using government-issued digital IDs, which are verified through biometrics. This foundational step ensures the authenticity of voters.
   Voter verification security measures include encryption of multiple parts of the body like fingerprints and facial recognition but at the same time, it is decentralized identity verification. This approach eliminates risks associated with single points of failure, thereby protecting voter identity.

2. **Decentralized Identity Authority:** Create a network of independent entities responsible for verifying identities, thereby preventing any single entity from having complete control over the verification process, thereby enhancing privacy and security.
   These audits must include simulated Sybil attacks, double voting, and DDoS denial of service attacks to test the systems strength. The documentation of these results can serve as a proof of the system's strength against attacks.

3. **Immutable Voter Registration:** Record verified voter identities on the blockchain, creating a transparent and immutable list of eligible voters that can be accessed and verified by anyone. Once a voter's identity is entered into the system, the blockchain makes sure that it is tamperproof. Not only can the list of tamperproof eligible voters not be deleted, but it is also available to anyone wishing to verify, from election observers to independent auditors. The voter registration decentralization allows their information to be securely stored since a centralized body wouldn't be able to edit or delete it. This enhances transparency and trust in fairness of an election.

4. **Voting Tokens:** Replace traditional ballots with cryptographic tokens that represent a voter's right to cast one vote, issued to verified voters and securely stored in their digital wallets. Voters are issued cryptographic tokens known as their "ballots." These tokens are permanently issued to authenticated voters and kept in their digital wallets. They take advantage of the blockchain to ensure that these tokens can only be used a single time, preventing double voting. Tokens cannot be replicated or hijacked to make the voting process more secure.

5. **Decentralized Consensus:** Implement a decentralized consensus mechanism, such as Proof of Stake (PoS) or Proof of Authority (PoA), to validate and record votes on the blockchain, ensuring transparency and fairness in the voting process. Votes are validated and recorded using a decentralized consensus mechanism such as PoS or PoA. In other words, vote verification is conducted by many separate, independent parties, thus ensuring no single entity owns the appeal. They are also more environmentally conscious and scalable than older models (ex. Proof of Work (PoW)), backed by the efforts to balance between security and environmental impact.

6. **Privacy-Enhancing Technologies:** Safeguard voter privacy through advanced cryptographic techniques, allowing voters to cast their ballots without revealing their choices while ensuring only authorized entities can verify votes. Cryptographic methods like zero-knowledge proofs or homomorphic encryption enables voters to vote without revealing their identities, while still proving the validity of the vote. The information necessary to verify that a vote has been cast accurately can only be accessed by authorized entities.What these methods can be used for is to keep the voters anonymous on the blockchain but still have a system that is transparent and tamper-proof. It raises voter competition and trust in the election process.

7. **Immutable Voting Records:** Store all voting records transparently and immutably on the blockchain, enabling public scrutiny while preserving voter anonymity. The immutable ledger of the blockchain permanently records voting records so that once a vote is submitted, it cannot be modified or erased. This transparency not only helps to prevent fraud, but also allows members of the public to verify the results of voting. This new feature of the encryption ensures that while the voting records will always be secured, they will still be accessible for auditing and transparency purposes, thus allowing the election observers and the public to be able to validate the integrity of the election more efficiently.

8. **Accessibility and Convenience:** Ensure accessibility for all eligible voters, including those with disabilities or limited technology access, through remote voting options and user-friendly interfaces. Blockchain makes voting from afar possible, which helps people with disabilities or those who live in far-off places. The system can have easy-to-use interfaces to make sure everyone even those who aren't tech-savvy, can take part without trouble. Giving voters special help makes sure all eligible people can vote, no matter how good they are with technology or what physical limits they might have.

9. **Smart Contracts for Election Rules:** Encode election rules and processes in smart contracts to automate and transparently manage the entire voting process, from registration to vote counting. Smart contracts run themselves and put election rules into action. They handle everything from signing up voters to counting votes without people getting involved. This cuts down on mistakes or cheating that people might cause. Smart contracts make things clearer because anyone can check them. They show a record of how election rules were used, which helps make sure voting is fair.

10. **Border Voting**: Support citizens residing abroad in participating in their home country's elections and referendums through cross-border voting mechanisms, enhancing democratic inclusivity. Blockchain provision in cross border polling authenticated and protected by blockchain will make the conditions possible to cast absentee votes accessible to expatriates. Blockchain utilization is able to guarantee the authenticity of the votes by eliminating possible fraudulent practices that can affect voting. Borderless blockchain-backed voting systems foster more openness and integration, thereby making it possible for people from different parts of the world to take part in an election, regardless of their residence.

11. **Scalability**: Implement sharding or layer-2 solutions to handle high transaction volumes during peak voting times while maintaining system security and performance. Sharding and layer-2 solutions will be added to enable the system to scale and process hundreds of thousands or even millions of transactions

per second. Sharding splits the network into smaller pieces (shards) that still work like a single blockchain but have parts at which are only responsible for processing a subset of all possible votes. Layer-2 solutions can also be used by creating small networks outside the main chain that channels can be opened between, these channels do not touch the blockchain unless they are closed again.The system will make an analysis if there is election time and scales up automatically in case we approach this period on time (only if there is an actual election!). This technique makes sure that during elections we still process everything in-blockchain while being able handle high transaction volumes as if using shardings/layer-2, then out-of-elections time we retain all goods of minimal energy waste.

12. **Continuous Security Audits**: Regularly conduct independent security audits to identify vulnerabilities and ensure the system's robustness, maintaining the trust of voters and stakeholders alike. Regular independent security audits are conducted to ensure that the system is secure and resilient against evolving threats. The system is attacked in a simulated manner to prove that it can withstand real world security challenges. Ongoing monitoring of the blockchain network during live elections will enable early attack/anomaly detection, and intervention if needed, in real time.

By implementing the proposed solution and continuously advancing blockchain-based e-voting systems, we can work towards a future where technology enhances the democratic process, ensuring the integrity and accessibility of elections on a global scale. Further research and collaboration are essential to overcome obstacles and ensure the successful integration of blockchain in strengthening democracies worldwide.

7. Conclusion:

This paper has explored various research papers on using blockchain technology for electronic voting systems. It has found multiple methods and approaches to create such a system with the help of technologies like Ethereum and Truffle. This shows the potential for innovation in blockchain-based electronic voting systems. Collaboration with the world's foremost industry leaders and academic institutions should be sought in order to pilot blockchain based voting systems, providing insights on scalability, usability and security towards global adoption.

8. References:

[1] Syada Tasmia Alvi , Mohammed Nasir Uddin , Linta Islam , Sajib Ahamed(2022). **"DVTChain: A blockchain-based** decentralized mechanism to ensure the security of digital voting system voting system", Journal of King Saud University – Computer and Information Sciences 34 (2022) 6855–6871

[2] Mr. Shreeyash Pednekar, Mr. Bhushan Halasagi, Ms. Chinmayee Kulkarni, Mr. Adarsh Mulik, Prof.Vaishali(2022). "BLOCKCHAIN BASED E-VOTING SYSTEM" IJCRT Volume 10, Issue 5 May 2022

[3] Ahmed Ben Ayed(2017). "A CONCEPTUAL SECURE BLOCKCHAIN- BASED ELECTRONIC VOTING SYSTEM" JOURNAL International Journal of Network Security & Its Applications (IJNSA) Vol.9, No.3 May 2017

[4] Madhuri Chavan,Soumi Banerjee,Shruti Saha,Nishita Sodhia,Akhil Shah(2020). "Blockchain Enabled Online-Voting System" JOURNAL ITM Web of Conferences 32, 03018 https://doi.org/10.1051/itmconf/20203203018 ICACC-2020

[5] Prof. Pallavi Shejwal, Aditya Gaikwad, Mayur Jadhav, Nikhil Nanaware, Noormohammed Shikalgar(2019). "E-voting using block chain Technology". JOURNAL IJSDR | Volume 4, Issue 5 May 2019

[6] Dipali Pawar, Pooja Sarode,Shilpa Santpure,Poonam Thore(2019). "Implementation of Secure Voting System using Blockchain". JOURNAL IJERT Vol. 9 Issue 06,June-2020

[7] Prof.AnitaA.Lahane,,JunaidPatel,Talif Pathan1 and Prathmesh Potdar(2020). "Block chain technology based e-voting system." JOURNAL ITM Web of Conferences 32, 03001 (2020)

[8] Haibo Yi(2019). "Securing e-voting based on blockchain in P2P network". JOURNAL Yi EURASIP Journal on Wireless Communications and Networking (2019) 2019:137 https://doi.org/10.1186/s13638-019-1473-6