DemocracyGuard: Blockchain-based Secure Voting Framework for Digital Democracy

Mritunjay Shall Peelam[1], Gaurav Kumar[1], Kunjan Shah[1], and Vinay Chamola[1]

[1]Birla Institute of Technology & Science Pilani

June 25, 2024

Abstract

Online voting is gaining traction in contemporary society to reduce costs and boost voter turnout, allowing individuals to cast their ballots from anywhere with an internet connection. This innovation is cautiously met due to the inherent security risks, where a single vulnerability can lead to widespread vote manipulation. Blockchain technology has emerged as a promising solution to address these concerns and create a trustworthy electoral process. Blockchain offers a decentralized network of nodes that enhances transparency, security, and verifiability. Its distributed ledger and non-repudiation features make it a compelling alternative to traditional electronic voting systems, ensuring the integrity of elections. To further bolster the security of online voting, we propose *DemocracyGuard* platform on the Ethereum blockchain, which incorporates facial recognition technology to authenticate voters. By leveraging these advancements, *DemocracyGuard* aims to provide a secure and resilient platform for online voting, paving the way for its broader adoption and revolutionizing the electoral landscape.

DemocracyGuard: Blockchain-based Secure Voting Framework for Digital Democracy

Mritunjay Shall Peelam[1,*], Gaurav Kumar[2], Kunjan Shah[2], Vinay Chamola[3] *Senior Member, IEEE*

***Abstract*—Online voting is gaining traction in contemporary society to reduce costs and boost voter turnout, allowing individuals to cast their ballots from anywhere with an internet connection. This innovation is cautiously met due to the inherent security risks, where a single vulnerability can lead to widespread vote manipulation. Blockchain technology has emerged as a promising solution to address these concerns and create a trustworthy electoral process. Blockchain offers a decentralized network of nodes that enhances transparency, security, and verifiability. Its distributed ledger and non-repudiation features make it a compelling alternative to traditional electronic voting systems, ensuring the integrity of elections. To further bolster the security of online voting, we propose *DemocracyGuard* platform on the Ethereum blockchain, which incorporates facial recognition technology to authenticate voters. By leveraging these advancements, *DemocracyGuard* aims to provide a secure and resilient platform for online voting, paving the way for its broader adoption and revolutionizing the electoral landscape.**

***Index Terms*—Blockchain, Electronic Voting, Digital Democracy, Elections, Decentralized, Ethereum.**

I. INTRODUCTION

CONVENTIONAL voting systems have been designed to uphold the essential tenets of democratic elections and referendums. These principles encompass safeguarding the right to vote, ensuring ballot secrecy, preserving the integrity of voters' intentions, and preventing intimidation or coercion during the voting process. Conversely, e-voting refers to electronic systems for casting and tallying votes in electoral processes [1]. Voting is a widespread practice ingrained in diverse societies in various forms. Nevertheless, peer voting stands apart from conventional voting procedures, such as presidential elections. Peer voting primarily occurs in an online environment as opposed to traditional physical ballot casting, which consequently presents unique challenges [2]. People gradually recognize the electoral system's significance as more votes are cast in real-life elections. Currently, most voting systems are centralized, encompassing mixnet-based voting, blind signatures, and homomorphic encryption technology. These systems involve the central agency recording, managing, calculating, and verifying the votes. Nevertheless, it is essential to assume the existence of a trustworthy bulletin board and corresponding credible vote-counting authorities. The reliance on single central institutions and the handling of extensive data pose vulnerabilities to the security of electronic voting [3]. Voting in India has been a contentious issue for many years, from the initial implementation of the Balloting System during the 1951-52 General Elections to the more recent adoption of "Electronic Voting Machines" in 1998. Under the balloting system shown in Fig. 1, voters cast their votes using pre-printed ballot papers under the supervision of a voting official. These physical ballots were then collected and transported to a centralized vote-counting center. This method had its shortcomings, which were subsequently addressed by transitioning to an electronic voting system. This updated approach records votes on electronic balloting devices, transfers them to a central location, and tabulates them using a control unit. While Electronic Voting Machines (EVMs) are touted as tamper-proof, concerns persisted regarding the need for oversight during the voting process and allegations of political party interference in their favor, highlighting two prominent challenges associated with the system. These issues underscore the persistent problems of the system's reliance on an authority to monitor the voting process and accusations of political party influence to support their cause. [4]. Even in the world's most prominent democracies, such as India and the United States, the electoral systems still grapple with imperfections. Notable concerns within the current voting process include vote tampering, electronic voting machine hacking, election manipulation, and the capture of polling booths [5].

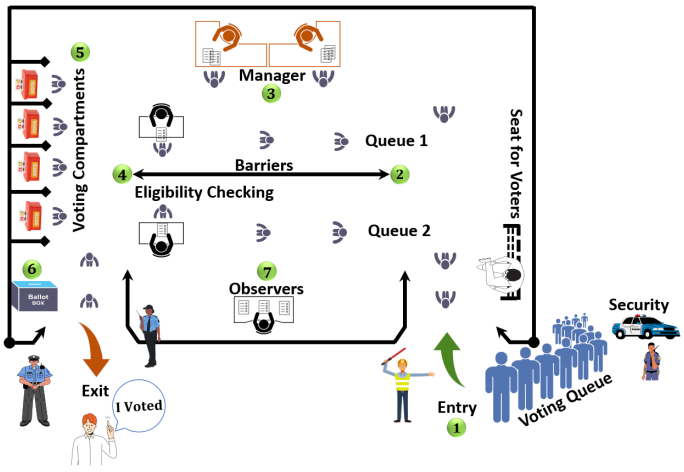

Fig. 1: Ballot Box Memories: The Way Voting Was Conducted in the Past in India

Mritunjay Shall Peelam, Gaurav Kumar, Kunjan Shah, and Vinay Chamola are with the Department of Electrical and Electronics Engineering, BITS-Pilani, Pilani Campus, India 333031 (e-mail: mritunjay.iete@gmail.com, f20200145@pilani.bits-pilani.ac.in, f20190072@pilani.bits-pilani.ac.in, vinay.chamola@pilani.bits-pilani.ac.in).

A. Electronic Voting Machine (EVM)-Based Voting in Democracy

A simple electronic device, the Electronic Voting Machine (EVM), has replaced paper ballots and voting boxes in modern elections. Because they are not easily duplicated, stolen, or shared, biometric identifiers are considered more trustworthy for individual identification than conventional tokens or knowledge-based techniques [6]. In 1977, the Chief Election Commissioner advocated using electronic voting machines. The Election Commission of India worked with two primary businesses, Bharat Electronics Limited (BEL) of Bangalore and Electronics Corporation of India Limited (ECIL) of Hyderabad, on the creation and design of EVMs. Three main parts make up an EVM, as shown in Fig. 2.

i. Balloting Unit (BU)
ii. Control Unit (CU)
iii. Voter Verifiable Paper Audit Trail (VVPAT)

A cable of five meters joins these two parts together. The Balloting Unit is kept safely within the voting compartment, while the Presiding Officer or a Polling Officer holds the Control Unit [7]. In many countries, like India, where they are widely utilized, Voter Verifiable Paper Audit Trails (VVPATs) are stored in the voting compartment. Using a paper copy of their electronic vote cast on an Electronic Voting Machine (EVM), voters may validate their vote using the Voter Verifiable Paper Audit Trail (VVPAT) method. After casting their ballot, voters are given a few seconds to look at the printed results to ensure accuracy [8].

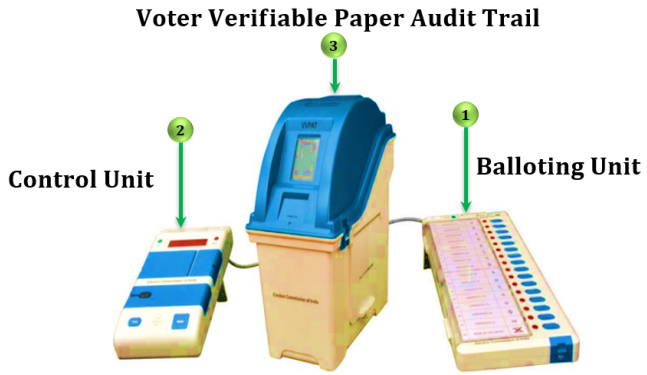

Fig. 2: A close-up of an EVM with its Control Unit (CU), VVPAT, and Ballot Unit (BU).

B. Blockchain-Based Voting in Democracy

Integrate blockchain technology with Cryptographic Hash Functions and Digital Signatures to establish a decentralized electronic voting system that fulfills all the voting process requirements without relying on a trusted third party. This e-voting protocol leverages blockchain as transparent ballot boxes connected through cryptographic methods. It is implemented as a smart contract running on the Ethereum network and utilizes Node.js to create nodes for each user. These nodes store encrypted vote details in individual blocks, ensuring a transparent and resilient system suitable for medium-sized elections [9]. Blockchain technology has recently emerged as a transformative solution, augmenting the efficiency of systems across various domains. Initially conceived for tracking cryptocurrency transactions, its applications have expanded considerably in recent years. Notably, blockchain-based e-voting systems have become a robust solution to address challenges inherent in electronic voting. These systems are poised to revolutionize modern electronic voting, leveraging the blockchain's immutable nature to establish a decentralized, distributed ballot box. By incorporating sustainability information into voting systems, blockchain encourages governments to embrace intelligent and sustainable voting practices, ensuring that all participants access dependable data on sustainable assets. Acknowledging that several challenges persist despite the increasing adoption of blockchain for electronic voting security enhancement is crucial [10].

TABLE I: Comparison of Centralized and Blockchain-Based Voting Systems (DemocracyGuard)

Disadvantages of Centralized Voting	**Improvements with DemocracyGuard**
Lack of Accessibility [11]	Enhanced Accessibility for All
Limited Voting Hours [12]	Extended Voting Timeframes
Long Lines at Polling Stations [13]	Reduced Wait Times
Voter Suppression [11]	Reduced Risk of Suppression
Difficulty for Disabled Voters [11, 12, 14]	Improved Accessibility for Disabled
Limited Voting Locations [9, 15]	Increased Voting Venues
Potential for Voter Intimidation [1, 16]	Enhanced Voter Privacy
Inconsistent Ballot Design [17, 18]	Standardized Ballot Format
Paper Ballot Errors [19]	Reduced Human Errors
Possibility of Lost Ballots [20, 21]	Immutable Ballot Records
Voter Misidentification [22]	Enhanced Voter Verification
Potential for Ballot Tampering [23]	Secure and Transparent System
Lack of Transparency [24]	Enhanced Transparency
Inefficient Voter Registration [25]	Streamlined Registration Process
Difficulty for Out-of-State Voters [26]	Simplified Out-of-State Voting
Lack of Verifiable Results [27]	Enhanced Results Verification
Miscounted Votes [28]	Reduced Risk of Vote Miscount

Numerous online voting systems have been developed utilizing blockchain technology to prevent ballot tampering. These existing systems can be broadly classified into two categories. The first category involves systems with a tallying authority. Despite leveraging the tamper-resistant nature of blockchain to record votes, these schemes still depend on a centralized authority, like a tallying authority, to decrypt the encrypted ballots and calculate the election results. Consequently, other entities cannot verify the accuracy of the voting results as the authority's secret key remains confidential. In contrast, the second category comprises self-tallying systems, which treat the tallying algorithm as a transparent process. This allows all entities, including voters and candidates, to verify all ballots and obtain the final election results [29]. Blockchain technology provides a decentralized online voting and electronic balloting framework. Distributed

TABLE II: Blockchain-based Voting System Requirements with DemocracyGuard Integration

Requirement	Description
Blockchain Security	
• Immutable Ledger	Ensure the integrity of the voting records through an immutable blockchain ledger
• Cryptographic Hashing	Implement cryptographic hashing for secure and tamper-evident data
• Decentralization	Utilize decentralized blockchain technology to prevent a single point of failure
• Smart Contract Integration	Incorporate smart contracts for automated and transparent execution of voting rules
Voter Privacy	
• Anonymous Transactions	Enable anonymous transactions to protect voter privacy
• Confidentiality	Ensure confidential handling of voter data through encryption techniques
Accessibility and Usability	
• User-Friendly Interface	Design an intuitive and user-friendly interface for all voters
• Inclusive Design	Ensure the system is accessible to voters with disabilities
• Multilingual Support	Provide support for multiple languages
Transparent Verification	
• Public Verification	Allow public verification of the voting results on the blockchain
• Voter Verification	Enable voters to verify that their votes are correctly recorded on the blockchain
Resilience and Redundancy	
• Distributed Storage	Use distributed storage for redundancy and resilience against data loss
• Fault Tolerance	Implement fault-tolerant mechanisms to ensure continuous operation
Scalability	
• Scalable Architecture	Design the system with scalability to handle a growing number of voters
• Efficient Consensus Mechanism	Employ an efficient consensus mechanism to handle a large number of transactions
Regulatory Compliance	
• Legal Framework	Adhere to legal and regulatory frameworks governing elections
• Standards Compliance	Ensure compliance with industry standards for blockchain technology
Cybersecurity Measures	
• DDoS Protection	Implement measures to mitigate the risk of DDoS attacks
• Encryption	Use advanced encryption techniques to secure communication and data

ledger technologies, like blockchain, have been increasingly leveraged to develop electronic voting systems, primarily due to their end-to-end verification capabilities. Blockchain presents an attractive alternative to traditional electronic voting systems, boasting decentralization, non-repudiation, and robust security measures. It finds utility in corporate boardroom decisions and public voting processes [12]. In the age of digital advancements, the traditional methods of conducting elections face numerous challenges that threaten the integrity and fairness of the democratic process, as shown in TABLE I. The need for a secure and transparent voting framework has become increasingly urgent. With the proliferation of technology and the growing concern over election interference and fraud, it has become imperative to develop a robust and trustworthy voting system that can safeguard the principles of democracy. This problem statement lays the foundation for developing *DemocracyGuard*. A robust blockchain-based voting system must prioritize security, decentralization, and transparency. Utilizing strong cryptographic algorithms, a distributed ledger, and a reliable consensus mechanism ensures the integrity and immutability of the voting process. Incorporating secure identity verification methods and maintaining voter anonymity is essential for building trust. The system should be user-friendly, accessible, and scalable to accommodate many transactions. Auditability through transparent processes, timestamping, and open-source code enhances accountability. The integration of smart contracts automates key aspects of the voting process. The inclusion of *DemocracyGuard*, as detailed in Table II, further fortifies the system, adding an extra layer of security, privacy, and adherence to legal and regulatory requirements, ensuring a resilient, fair, and democratic electoral experience.

C. Research Motivation and Novelty

DemocracyGuard is driven by the increasing recognition of the essential role that electoral systems play in democracies and the persistent challenges they face, such as vote tampering, electronic voting machine hacking, and election manipulation. The development of DemocracyGuard is motivated by the desire to address these challenges by implementing a blockchain-based system that enhances security, transparency, and verifiability in the voting process. The integration of facial recognition technology for voter authentication further aims to support the security of online voting, addressing inherent security risks and promoting the adoption of this technology for a more secure and resilient electoral process.

The Novelty of this research lies in the combination of blockchain technology with facial recognition to authenticate voters, a feature that sets DemocracyGuard apart from existing voting systems. Blockchain ensures a decentralized, tamper-proof system where votes are recorded as immutable transactions, enhancing trust in the electoral process. Incorporating facial recognition technology for voter authentication represents a significant advancement in ensuring the integrity of the voting process. This innovative approach to combining blockchain with biometric verification aims to revolutionize online voting, making it more secure, accessible, and efficient. There are several contributions listed below.

i. *Blockchain and Facial Recognition Integration:* The novel integration of blockchain technology with facial recognition for voter authentication distinguishes DemocracyGuard from existing solutions.
ii. *Decentralized, Tamper-proof System:* Utilizing a decentralized network of nodes, the framework provides a tamper-proof system where votes are recorded as immutable transactions, enhancing the integrity of elections.
iii. *Enhanced Voter Verification:* The innovative use of facial recognition technology offers a more reliable method of

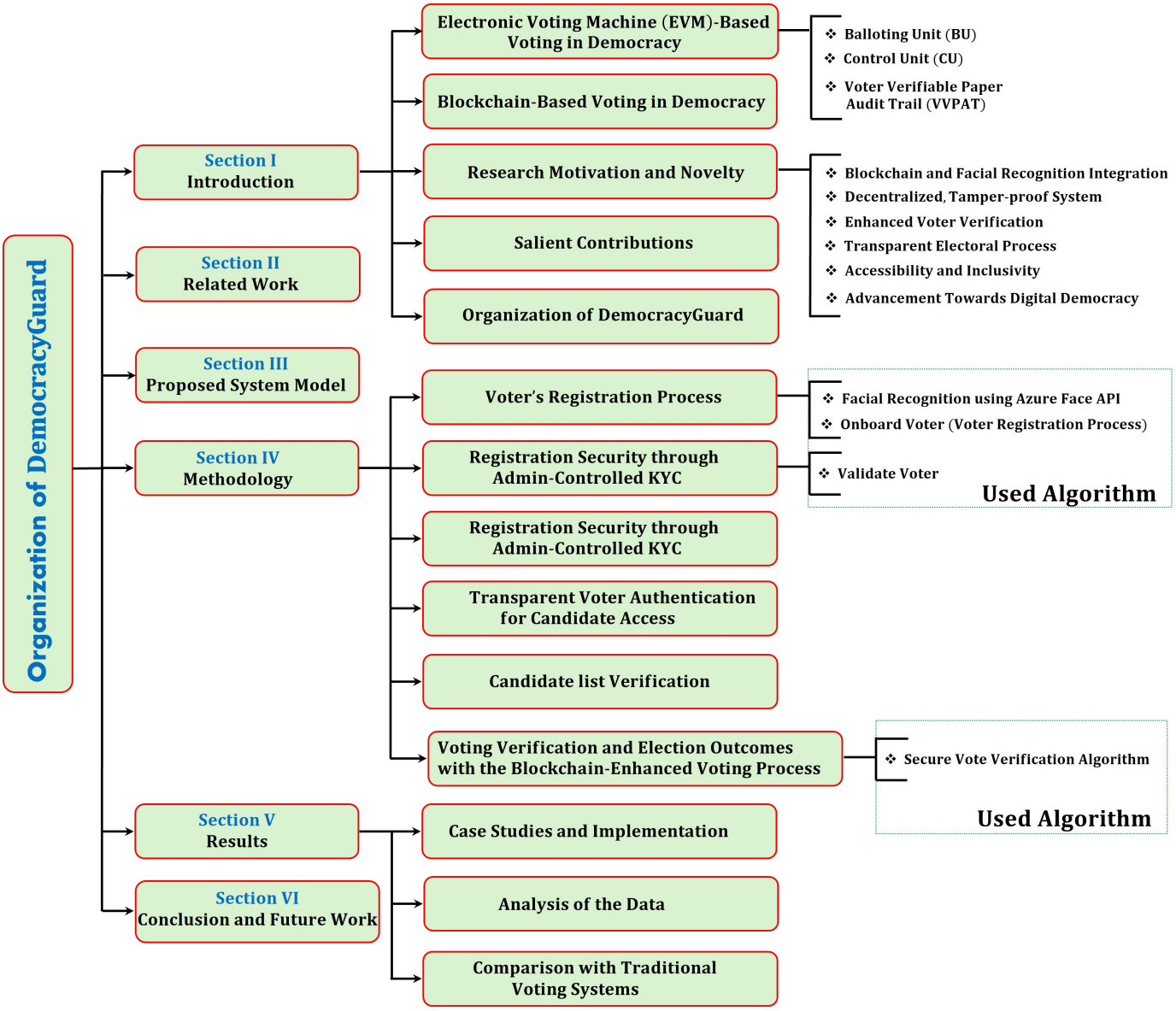

Fig. 3: Comprehensive layout of DemocracyGuard outlining the structure and flow of content

voter authentication compared to traditional tokens or knowledge-based techniques.

iv. *Transparent Electoral Process:* DemocracyGuard introduces a transparent electoral process, with every transaction being verifiable and recorded on the blockchain, ensuring that all participants have access to reliable data.

v. Accessibility and Inclusivity: The framework's design focuses on making voting more accessible and inclusive, catering to a wide range of voters with different needs and capabilities.

vi. *Advancement Towards Digital Democracy:* By addressing key challenges of traditional and electronic voting systems, DemocracyGuard represents a significant advancement towards realizing a secure, efficient, and transparent digital democracy.

D. Salient Contribution

DemocracyGuard contributes to the advancement of digital democracy, making electoral processes more transparent, verifiable, and resilient against fraud. The following are the contributions of DemocracyGuard.

i. This paper presents a novel approach to combine blockchain technology with facial recognition to authenticate voters, which is both secure and efficient.

ii. Distributed ledger technology inherent to blockchains, the system ensures that records cannot be altered after they have been logged, promoting a tamper-proof electoral environment.

iii. The system introduces an enhanced method for voter verification that surpasses traditional means, providing a more reliable verification process.

iv. It offers transparency in the electoral process, allowing all participants to verify the procedures and outcomes, thus

enhancing trust in the system.

v. DemocracyGuard is designed to be accessible to all eligible voters, regardless of location or mobility, promoting inclusivity in the electoral process.

vi. DemocracyGuard represents a significant step forward in the use of digital technologies to conduct democratic processes, moving towards a more modernized and efficient model of governance.

E. Organization of DemocracyGuard

Fig. 3 shows the organization of DemocracyGuard, which outlines the use of Electronic Voting Machines (EVM)-Based Voting in Democracy and introduces a blockchain-based voting system. Section I introduces the concept and covers the research motivation, novelty, and salient contributions, including integrating blockchain and facial recognition for a decentralized, tamper-proof system. Section II systematically analyzes and synthesizes the existing research and discussions on electronic voting systems. Section III presents the "Proposed System Model," detailing the voter's registration process using Azure Face API and admin-controlled Know Your Customer (KYC) for registration security. Section IV describes the "Methodology" employed, including transparent voter authentication and candidate list verification, as well as a secure vote verification algorithm. The "Results" in Section V showcase case studies and implementation data. Section VI, "Conclusion and Future Work," offers an analysis of data and a comparison with traditional voting systems. Table III compares frequently utilized standard terms and their respective acronyms within the DemocracyGuard.

TABLE III: Comparison of Abbreviations and Terms used in DemocracyGuard

Abbreviation	Term used in DemocracyGuard
EVMs	Electronic Voting Machines
BEL	Bharat Electronics Limited
ECIL	Electronics Corporation of India Limited
BU	Balloting Unit
CU	Control Unit
VVPAT	Voter Verifiable Paper Audit Trail
KYC	Know Your Customer
SUS	System Usability Scale
PoW	Proof of Work
PoS	Proof of Stake
PBFT	Practical Byzantine Fault Tolerance
PoET	Proof of Elapsed Time
LPoS	Liquid Proof-of-Stake
DPoS	Delegated Proof-of-Stake
FBA	Federated Byzantine Agreement
dBFT	Delegated Byzantine Fault Tolerance
PPoS	Pure Proof-of-Stake
NPoS	Nominated Proof-of-Stake
OPOS	Ouroboros Proof-of-Stake
PoSA	Proof of Stake Authority
PoH	Proof of History
IBFT	Istanbul Byzantine Fault Tolerance
TBD	To Be Determined
AI	Artificial Intelligence
EVS	Electronic Voting Systems
UI	User Interface
SC	Smart Contract

II. Literature Review

In the realm of voting systems, blockchain technology, developed over the past decade, has emerged as a game-changer. It offers a secure, transparent, and tamper-proof method for casting and counting votes. Blockchain ensures the integrity of the process by recording votes as unchangeable transactions, increasing participation, and enhancing trust in elections. It's a significant step in modernizing and securing the democratic process. TABLE IV represents a comparative analysis of blockchain frameworks crucial for protecting digital democracy. It highlights their consensus mechanisms, generation times, accessibility, transaction rates, scalability, and transaction costs. *DemocracyGuard* can use this information to select the most suitable blockchain framework to enhance the security, efficiency, and inclusivity of digital voting and decision-making processes. This table provides a valuable resource for fortifying the digital infrastructure supporting democratic systems. D. Ashok Kumar *et al.* compares three fingerprint-matching methods using EVMs for election accuracy and time efficiency. [51]. Election integrity depends on fair procedures, but fraud can occur in various ways. Leemann *et al.* propose a method for fraud detection, addressing multiple forms and instances. Using a Swiss referendum case, we apply statistical tests revealing irregularities in some municipalities that lost ballots. Managing multiple tests presents challenges, and we discuss two strategies with their strengths and weaknesses [20]. In 2018, Hjalmarsson *et al.* explored using blockchain for distributed electronic voting. It introduces a novel blockchain-based voting system that overcomes limitations in current systems. Various blockchain frameworks are evaluated to construct this system, focusing on distributed ledger technologies. A case study outlines the election process, showing how a blockchain application enhances security and reduces nationwide election costs [52]. In 2019, Yi *et al.* discussed the application of blockchain in a peer-to-peer network to enhance the security of electronic voting (e-voting). They introduce models for voting records, user credentials, and vote withdrawal to create a practical and secure e-voting system that addresses forgery concerns, utilizing distributed ledger technology and elliptic curve cryptography [53]. In 2021, Kamil *et al.* addressed the rising concerns related to the COVID-19 pandemic and its impact on public safety and elections. The author proposed a solution in the form of a blockchain-based E-voting system, allowing remote voting through electronic devices. This innovative approach enhances security, minimizes data fraud, and provides real-time access to decentralized voting results. Kamil's research, using the System Usability Scale (SUS), yielded a high score of 90, indicating the system's acceptability and positive impact on effectiveness and efficiency during the pandemic [54]. In 2021, Yang *et al.* examined the significance of elections in democracies and the cryptographic challenges of E-voting. Their research introduced PriScore, a blockchain-based self-tallying election system ensuring privacy in score voting. The system employs a dual zero-knowledge proof technique to satisfy range and sum constraints, delivering fairness, dispute resolution, and robust security [29]. In 2021, Jafar *et al.* explored the growing trend of online voting in modern society. They acknowledged its potential to reduce costs and boost voter participation. However, security concerns led them to

TABLE IV: Comparative Analysis of Blockchain-based Frameworks for Digital Democracy

Blockchain Framework	Consensus Mechanism	Generation Time	Accessibility	Transaction Rate	Scalability	Transaction Cost (USD)
Ethereum [30]	Proof of Work (PoW) transitioning to Proof of Stake (PoS)	15 seconds	Public	30 TPS	Moderate to High	$0.50
Hyperledger Fabric [31]	Practical Byzantine Fault Tolerance (PBFT)	3-5 seconds	Permissioned	1,000+ TPS	Moderate to High	Free
Hyperledger Sawtooth [32]	Proof of Elapsed Time (PoET)	5-10 seconds	Permissioned	Scalable	High	$0.80
Corda [33, 34]	Notary (Permissioned, no global consensus)	10-30 seconds	Permissioned	Customizable	High	$1.00
Tezos [35]	Liquid Proof-of-Stake (LPoS)	1 minute	Public	40 TPS	To Be Determined (TBD)	$0.30
EOS [36]	Delegated Proof-of-Stake (DPoS)	0.5 seconds	Public	4,000+ TPS	High	$0.20
Stellar [37]	Federated Byzantine Agreement (FBA)	2-5 seconds	Public	1,000+ TPS	High	$0.40
NEO [38]	Delegated Byzantine Fault Tolerance (dBFT)	15 seconds	Public	1,000+ TPS	High	$0.60
TRON [39]	Delegated Proof-of-Stake (DPoS)	3 seconds	Public	2,000+ TPS	High	$0.25
Algorand [40]	Pure Proof-of-Stake (PPoS)	4.5 seconds	Public	1,000 TPS	High	$0.70
Avalanche [41]	Avalanche Consensus	1-2 seconds	Public	4,500+ TPS	High	$0.90
Polkadot [42]	Nominated Proof-of-Stake (NPoS)	6 seconds	Public	1,000 TPS (per parachain)	High	$1.10
Cardano [43]	Ouroboros Proof-of-Stake	20 seconds	Public	1,000+ TPS (Ongoing optimization)	High	$0.75
Binance Smart Chain (BSC) [44]	Proof of Stake Authority (PoSA)	3 seconds	Public	100 TPS	Moderate to High	$0.35
Solana [45]	Proof of History (PoH) + Proof of Stake (PoS)	400 milliseconds	Public	65,000+ TPS	Very High	$0.05
Flow [46]	Flow Consensus (Proof of Stake)	1 second	Public	1,000+ TPS (initially)	Scalable	$0.60
Bitcoin [47]	Proof of Work (PoW)	10 minutes	Public	7 TPS	Limited (by design)	$2.00
Exonum [48]	Proof of Stake (Exonum Consensus)	3-5 seconds	Permissioned	2,000+ TPS	High	$1.30
Quorum [49]	Istanbul Byzantine Fault Tolerance (IBFT)	15 seconds	Permissioned	100-200+ TPS	Moderate to High	$1.20
ZCash [50]	Proof of Work (Equihash)	2.5 minutes	Public	20-30 TPS (approx.)	Moderate to High	$0.95

investigate blockchain technology as a solution. Their research provided an overview of blockchain-based electronic voting systems, highlighting the need for improved privacy and transaction speed to ensure the sustainability of such systems [12]. In 2022, Farooq *et al.* addressed the widespread mistrust in traditional voting systems, acknowledging the violations of fundamental rights and the lack of transparency in existing digital voting systems. They identified the vulnerability of these systems to exploitation and aimed to rectify these issues. Their research proposed a blockchain-based platform to ensure election fairness, fostering trust between voters and election authorities. This framework enables digital voting without physical polling stations, supported by scalable blockchain and robust security measures, including the Chain Security Algorithm and smart contracts [55]. In 2022, Bhadoria *et al.* addressed the paramount significance of democratic elections and governmental efforts to enhance their competitiveness and equity. Their paper explored the adoption of blockchain technology in election processes, utilizing a distributed digital ledger to record transactions securely. This technology ensures transparency and confidentiality by employing encryption algorithms and tamper-proof data storage [18]. In 2022, Alvi *et al.* explored the significance of voting in democratic societies and the limitations of paper balloting, which is prone to errors and abuse. Their research introduced a blockchain-based voting system, ensuring anonymity, privacy, and integrity. Implemented on Ethereum 2.0, the system employs smart contracts to enhance security and reduce infrastructure costs [15]. In 2023, Vladucu *et al.* conducted a study emphasizing the increasing global adoption of electronic voting systems for public office elections. These systems offer benefits such as remote voting and expedited tallying while enhancing privacy and reducing voting bias. Blockchain technology fortifies the process by ensuring immutable vote storage, thwarting tampering, and safeguarding the legitimacy of elections. Countries like Germany, Russia, Estonia, and Switzerland have integrated blockchain into their e-voting systems [16]. In 2023, Neloy *et al.* conducted a study highlighting the limitations of traditional voting methods, which lack remote access, are time-consuming, and suffer from security issues. Electronic voting systems (EVS), while improving efficiency, raise concerns regarding security, legitimacy, and transparency. To address these challenges, the researchers utilized blockchain technology, incorporating smart contracts

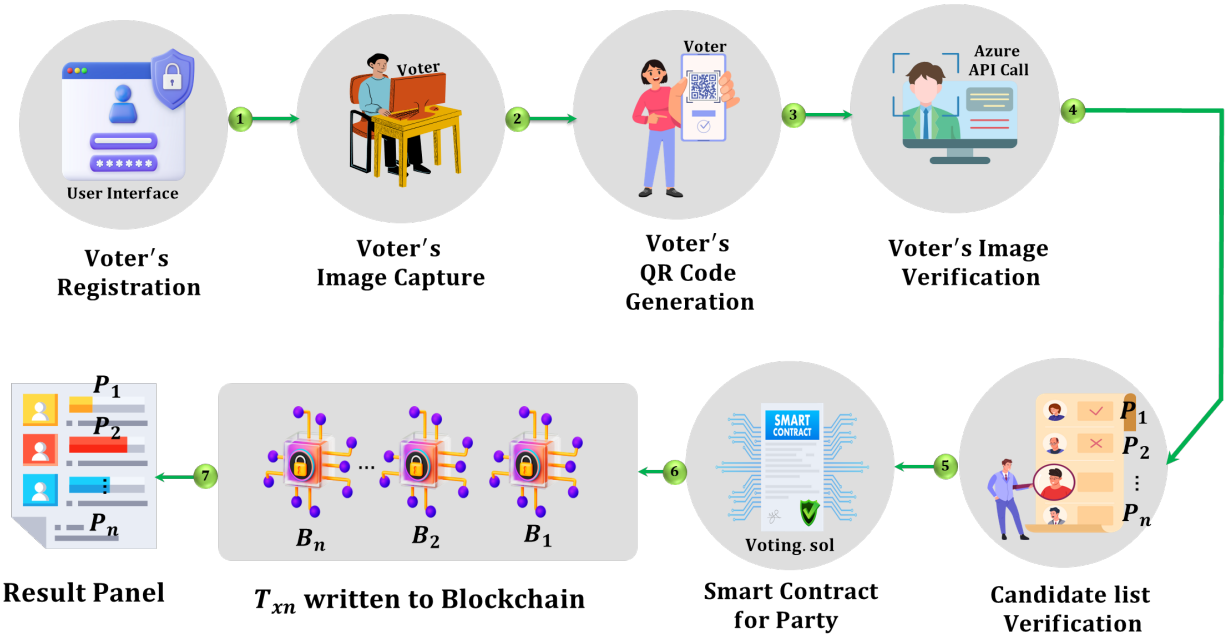

Fig. 4: DemocracyGuard's Blockchain Smart Contract-Based Architecture: Ensuring Trust from Voter Registration to Transparent Election Results

and artificial intelligence (AI) to develop a remote voting system that enhances transparency, decentralization, and security [56].

III. PROPOSED SYSTEM MODEL

The proposed system model, shown in Fig. 4 begins with voter registration, where eligible voters are registered. Each registered voter is assigned a unique identifier (a voter ID). Subsequently, the voter image capture process captures biometric data for enhanced security. Voter QR Code Generation then creates a QR code linked to the voter's information. For voter image verification, the system utilizes Azure's facial recognition API, ensuring the voter's identity through biometric matching. In the Voting Party List phase, the voter selects their preferred candidate or party, represented as Voting Party List $P_1, P_2 ... P_n$. The selection triggers the execution of the *Voting.sol* smart contract on the Ethereum Blockchain, securely recording the voter's choice, initiating the transaction, and writing to the Ethereum Blockchain $B_1, B_2 ... B_n$, guaranteeing transparency and immutability. The system offers a result panel to display the election outcomes for the parties $P_1, P_2 ... P_n$, assuring a fair and secure electoral process.

IV. METHODOLOGY

1) Voter's Registration Process: The registration phase commences with the Voter User Interface (UI) page, where voters input their details, such as their name (N), Aadhaar number (A), and constituency (C). Subsequently, the voter is prompted to capture a photograph (P). This photograph is then transmitted to the Azure Face API, which, through advanced facial recognition algorithms as shown in Algorithm 1, uniquely identifies the individual in the photo, resulting in a photo identifier string, U. The collected data is encoded into a QR code, denoted as $QR(N, A, C, U)$. Additionally, two essential Boolean variables, $isValid$ and $hasVoted$, are initialized as follows:

$$isValid = \begin{cases} \text{True} & \text{if the voter's details are validated,} \\ \text{False} & \text{otherwise.} \end{cases} \tag{1}$$

$$hasVoted = \begin{cases} \text{True} & \text{if the voter has participated} \\ & \text{in the electoral process,} \\ \text{False} & \text{otherwise.} \end{cases} \tag{2}$$

These variables are crucial for tracking the voter's eligibility and participation in the electoral process, and during the registration phase, these variables are *False*. The logic ensures that voting status is accurately recorded. The complete voter registration process is shown in Fig. 5, and Algorithm 2 shows the complete registration process of voters.

2) Registration Security through Admin-Controlled KYC Procedures: Registration security through admin-controlled KYC procedures establishes a robust and trustworthy voter onboarding mechanism. Upon completion of the registration process, voters receive a QR code, denoted as QR_{code}, initially tagged as $isValid$ = False, signifying that it has yet to undergo verification by the admin through KYC protocols. To bolster security, voters must seek manual KYC verification from the administration, as illustrated in Fig. 6. Within the admin panel, a comprehensive scrutiny of the voter's information takes place, with an unwavering commitment to upholding the integrity of voter data. Let $Voter_{\text{info}}$ represent the voter's information. KYC verification can be expressed as follows:

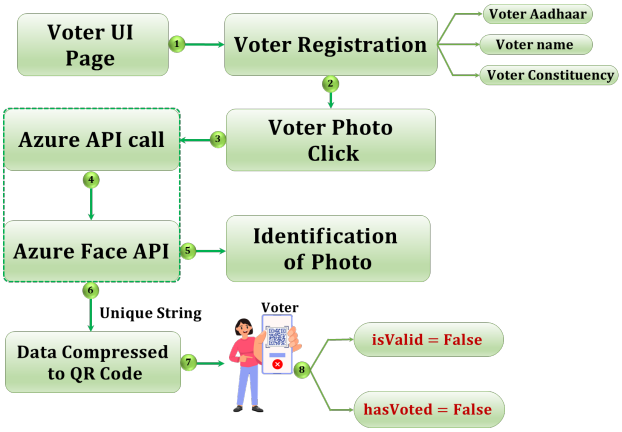

Fig. 5: Architecture of Voter Registration Process

Algorithm 1 Facial Recognition using Azure Face API

Input : Azure Subscription Key $subscription\_key$,
Azure Endpoint $endpoint$,
Image URL $image\_url$,
Person ID $person\_group\_id$
Output: Recognized faces and their attributes

Create a FaceClient instance with the provided $subscription\_key$ and $endpoint$ $face\_client \leftarrow$ FaceClient($endpoint$, CognitiveServicesCredentials($subscription\_key$)) DetectFaces($image\_url$) $\leftarrow$ detect_faces($image\_url$)
if *DetectFaces($image\_url$) is empty* **then**
  Print("No faces detected in the image.") **return**
end
for $face$ ***in*** *DetectFaces($image\_url$)* **do**
  $face\_id \leftarrow$ face.face_id IdentifiedFaces($face\_id$, $person\_group\_id$) $\leftarrow$ identify_face($face\_id$, $person\_group\_id$)
  if *IdentifiedFaces($face\_id$, $person\_group\_id$)[0].candidates* **then**
    $person\_id \leftarrow$ IdentifiedFaces($face\_id$, $person\_group\_id$)[0].candidates[0].person_id
    FaceAttributes($face\_id$) $\leftarrow$ get_face_attributes($face\_id$)
    Print("Face detected and identified as Person ID: ", $person\_id$)
    Print("Age: ", FaceAttributes($face\_id$).age)
    Print("Gender: ", FaceAttributes($face\_id$).gender)
    Print("Emotion: ", FaceAttributes($face\_id$).emotion)
  end
  else
    Print("Face detected but not recognized.")
  end
end
return

$$KYC\_verification = \begin{cases} \text{True} & \text{if } Admin\_verification(Voter_{\text{info}}) \\ \text{False} & \text{otherwise} \end{cases} \tag{3}$$

Elaborate logs, denoted as $Logs$, are meticulously maintained throughout this verification process. Once the administrator successfully validates the voter's information, the $isValid$ status is elevated to True, denoted as $isValid = True$ as shown in Algorithm 3, thereby granting the voter access to the subsequent phase, guaranteeing a highly secure and verified voter constituency.

Algorithm 2 Onboard Voter (Voter Registration Process)

Input: name, aadhaar_card, constituency, photo
Output: QR code
Step 1: Enter name, aadhar_card, constituency
Step 2: Click face photo
Step 3: photo_identifier_string $\leftarrow$ AZURE_FACE_API(photo)
Step 4: Store <name, aadhar_card, constituency, photo_identifier_string, *isValid* = *False*, *hasVoted* = *False*> to election DB
Step 5: **if** *isValid* == *False* **then**
  user_qr_code $\leftarrow$ generate_qr_code(name, aadhar_card, constituency, photo_identifier_string)
  return Download user_qr_code to user phone
else
  return QR code generation skipped (already onboarded)

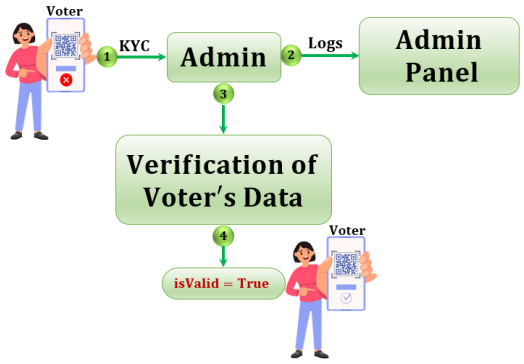

Fig. 6: Admin-Controlled KYC Verification Process

Algorithm 3 Validate Voter

Input: Aadhaar Card
Output: Validation Status
Step 1: Admin logs in using admin_username and admin_password
Step 2: Voter physically goes for KYC and submits Aadhar card
Step 3: Admin authenticates voter using Aadhar card
if *voter details exist in election DB* **then**
  if *isValid* == *False* **then**
    if *Aadhar card details are correctly verified and photo matches* **then**
      go to **Step 4**
    else
      return Authentication failure
  else
    Ask voter to Onboard first
    return Authentication failure
Step 4: Admin authorizes voter
  if *current_year - birth_year* $\geq$ *18* **then**
    isValid = True
    Update voter info in election DB
else
  return Authorization failure

3) Transparent Voter Authentication for Candidate Access: Upon completing the KYC verification process, voters are prompted to upload their QR code and undergo a subsequent image capture. Let V represent the voter, QR represent the QR code, and I represent the captured image, and let A be the Azure API call, and D denote the stored image in the Azure database during the voter's registration process. The image authentication process can be represented as follows:

$$A(V, QR, I, D) = \begin{cases} \text{True} & \text{if } I = D \text{ and} \\ & V \text{ is authorized by } QR, \\ \text{False} & \text{otherwise} \end{cases} \tag{4}$$

If $A(V, QR, I, D) = True$, it indicates that the voter's captured image matches the stored image, and the QR code is valid, ensuring a secure authentication. Once the image authentication is successfully validated, voters access a comprehensive list of constituent candidates, as shown in Fig. 7. This rigorous authentication ensures a transparent

and secure electoral experience, empowering voters to make well-informed decisions during the voting process. The combination of KYC verification, QR code validation, and image authentication forms a robust system (S) for maintaining the integrity and security of the electoral process:

$$S(V, QR, I, D) = \begin{cases} True & \text{if } A(V, QR, I, D) = 1 \\ False & \text{otherwise} \end{cases} \quad (5)$$

This system S is designed to ensure the transparency and security of voter authentication for accessing the electoral candidate lists, promoting a reliable electoral experience.

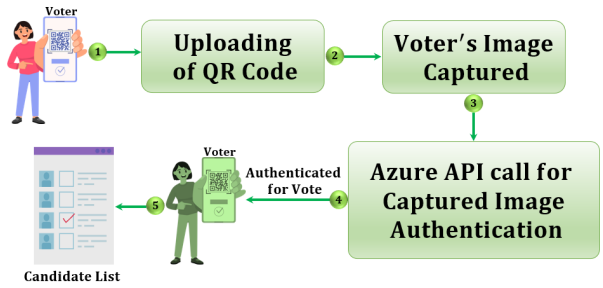

Fig. 7: Accessing Electoral Candidate Lists After Secure Authentication

4) Candidate list Verification: The validation of a candidate, as depicted in Algorithm 4, involves checking the authenticity and eligibility of a candidate, typically by comparing their provided information or identifier against a predefined set of valid candidates.

Algorithm 4 Validate Candidate

Input: Candidate identifier (candidate_id $\in C$), candidate_list (C)
Output: Validation Result $\in$ {True, False}
Initialize $i = 0$
while $i < |C|$ **do**
  if *candidate_list*$[i]$ = *candidate_id* **then**
    return Validation Result = True
  $i \leftarrow i + 1$
return Validation Result = False

If the candidate is found in the list of valid candidates, the validation process returns *True*, indicating that the candidate is legitimate. If not, it returns *False*, signifying that the candidate is not authorized or eligible for the process. This validation step is essential for maintaining the security and integrity of systems and ensuring that only valid participants are allowed to proceed, enhancing the reliability and trustworthiness of the system. Let C be the set of valid candidates, C_i be the candidate identifier for the i-th candidate in C, and c_{check} be the candidate identifier to be validated. The validation process can be expressed as:

$$c_{\text{check}} \in C \Rightarrow \text{Validation} = \text{True} \quad (6)$$

$$c_{\text{check}} \notin C \Rightarrow \text{Validation} = \text{False} \quad (7)$$

Where, $c_{\text{check}} \in C$ signifies that the candidate identifier c_{check} belongs to the set of valid candidates C, leading to a "True" validation outcome, while $c_{\text{check}} \notin C$ indicates that the candidate identifier c_{check} is not within C, resulting in a "False" validation.

5) Voting Verification and Election Outcomes with the Blockchain-Enhanced Voting Process: In the voting process, a voter receives a list of candidates (C) and selects their preferred choice. This initiates a transaction (T), where the voter's choice is formally recorded. The voter's selection can be represented as:

$$\textit{preferred\_candidate} \in C \quad (8)$$

The smart contract (SC) processes the transaction and employs a secure vote validation using Algorithm 5 to verify the legitimacy of the chosen candidate. The validation algorithm ensures that the selected candidate is a valid member of the candidate set C.

$$\text{Validation}(\textit{preferred\_candidate}, C) = \{\text{True}\} \quad (9)$$

Upon successful validation, the transaction is permanently recorded on a blockchain (B), resulting in a ledger of transactions. As a crucial indicator of successful participation, the *hasVoted* condition variable is *true*, preventing multiple votes from the same voter and confirming their engagement in the election.

$$B = \{T_1, T_2, \ldots, T_n\} \quad (10)$$

The election result is then determined through a mathematical function aggregating and counting the valid votes, providing a clear and verifiable outcome. This can be expressed as:

$$Result = \text{Count\_Valid\_Votes}(B, C) \quad (11)$$

The combination of mathematical verification, secure blockchain technology (BC), and transparent result computation enhances the overall integrity and accountability of the electoral process, ensuring that the election outcomes accurately reflect the will of the voters. The election result becomes accessible on the result panel, as shown in Fig. 8, offering a comprehensive and easily interpretable display of the outcome. This intricate, technology-driven procedure merges the convenience of *DemocracyGuard* with the robust security and transparency of blockchain technology, enhancing the overall integrity and accountability of the electoral process.

V. Results and Findings

DemocracyGuard, the innovative blockchain-based voting framework designed for digital democracy, has undergone rigorous case studies and simulations to evaluate its efficacy and potential impact on modern democratic processes. These assessments provide valuable insights into the strengths and potential challenges associated with implementing *DemocracyGuard* compared to traditional voting systems.

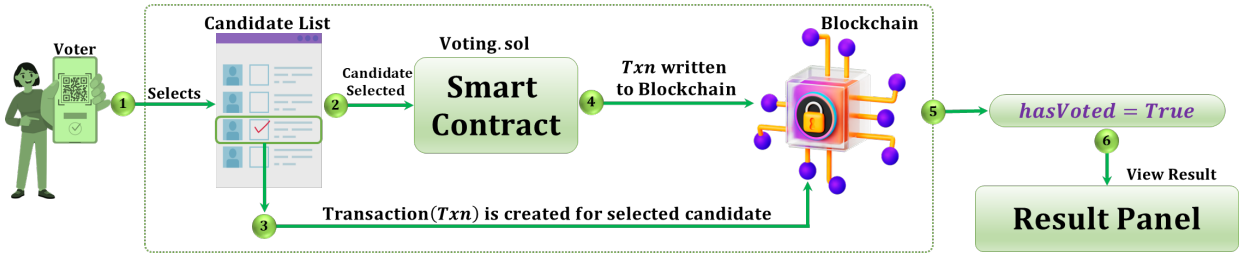

Fig. 8: Blockchain-Enhanced Voting Process Unveils Election Outcomes

Algorithm 5 Secure Vote Verification Algorithm

Input: QR_code, live_photo
Output: Validation Error, Vote For Candidate
Step 1: On Voting day, submit QR_code on the application
Step 2: voter_details ← scan(QR_code)
Step 3: Query election DB using voter_details
if *hasVoted* == *False* **then**
  if *isValid* == *True* **then**
    Step 4: Click a live_photo
    isCorrectPhoto ← AZURE_FACE_API(live_photo, voter_details.photo_identifier_string)
    if *isCorrectPhoto* == *True* **then**
      Step 5: Display list of candidates for voter_details.constituency
      candidate ← select single preferred candidate
      isValidCandidate ← ValidateCandidate(candidate)
      if *isValidCandidate* == *True* **then**
        Step 6: UpdateVotesFor(candidate)
      else
        return Error("Candidate not found")
    else
      return ValidationError("Photo mismatch")
  else
    return ValidationError("Ineligible to vote")
else
  return ValidationError("Already Voted")

A. Case Studies and Implementation

The case studies involved simulated elections across diverse scenarios, considering factors such as voter turnout, system resilience to cyber threats, and overall user experience. In each instance, *DemocracyGuard* demonstrated robust performance, ensuring the integrity and security of the voting process. Simulations revealed that the decentralized nature of the blockchain infrastructure significantly reduced the risk of tampering or unauthorized access. In Fig. 9, DemocracyGuard, a blockchain-based voting framework for digital democracy, is depicted, capturing the essence of democracy through a snapshot from the voters' registration process. This image highlights the initial stages of civic engagement within the innovative and secure platform. Following successful registration, Fig. 10 displays a welcome message within DemocracyGuard, greeting voters and emphasizing the user-centric approach of the digital democracy system. Fig. 11 then reveals a greeting along with the effortless QR code submission procedure, showcasing the cutting-edge technology integrated into DemocracyGuard for casting votes efficiently and securely. Fig. 12 provides a comprehensive visualization during the Cast Your Vote phase, presenting voter details and candidate choices to empower users in making informed decisions. In Fig. 13, the administrative panel of DemocracyGuard is featured, unveiling voter and candidate details for rigorous verification, underlining the system's commitment to ensuring the integrity of electoral processes. Fig. 14 showcases DemocracyGuard's transparency by revealing election poll results in the Result Section, solidifying its role as a pioneering blockchain-based voting framework for advancing digital democracy.

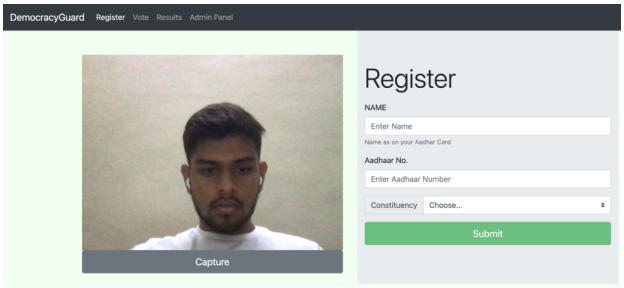

Fig. 9: Capturing the Essence of Democracy: A Snapshot from the Voters Registration Process in DemocracyGuard

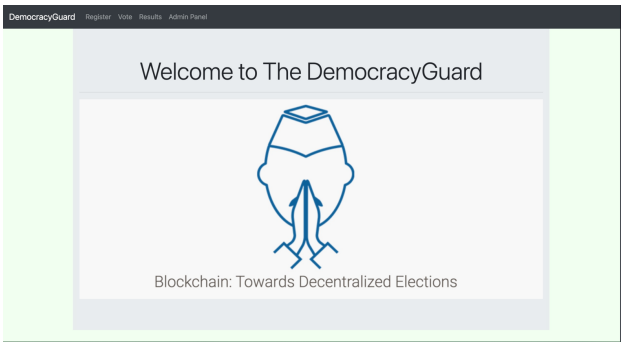

Fig. 10: Welcome Message Greets Voters Upon Successful Registration in DemocracyGuard

B. Analysis of the Data

In-depth analysis of the data generated during the case studies highlighted several key findings. The transparency inherent in blockchain technology allowed for real-time tracking of votes, providing a verifiable and immutable record of the electoral process. Moreover, smart contracts in *DemocracyGuard* streamlined the voting process, minimizing errors and ensuring adherence to predefined rules. Fig. 15 shows the Smart Contract Creation within *DemocracyGuard*. This pivotal snapshot encapsulates the intricate steps in transforming predefined rules and conditions into

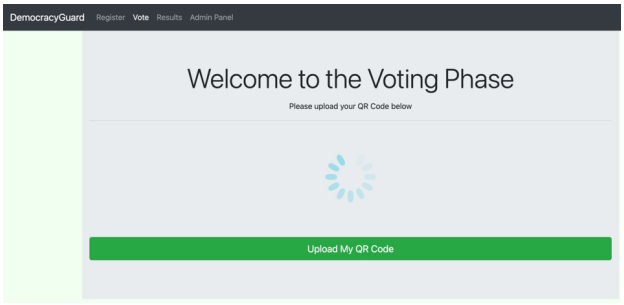

Fig. 11: Revealing a Greeting and the Effortless QR Code Submission Procedure for Casting Votes in DemocracyGuard

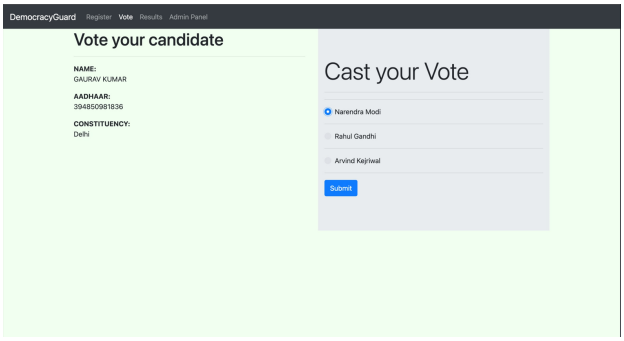

Fig. 12: A Comprehensive Visualization of Voter Details and Candidate Choices for Informed Decision-Making during Cast Your Vote phase

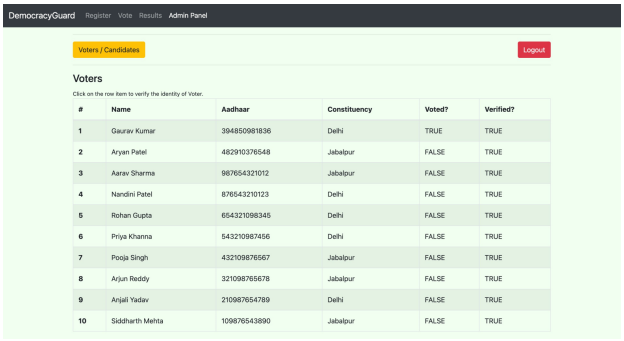

Fig. 13: Admin Panel, Revealing Voter and Candidate Details for Rigorous Verification in Electoral Processes

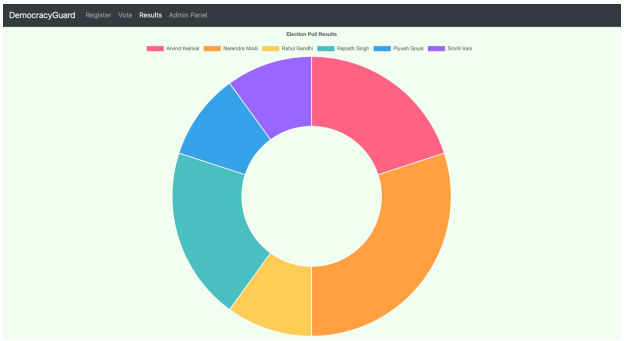

Fig. 14: DemocracyGuard Reveals Election Poll Results in the Result Section

self-executing contracts on a blockchain. As the digital landscape evolves, this visual glimpse into the creation of smart contracts underscores the fusion of technology and governance, ushering in a new era of decentralized and automated decision-making within the *DemocracyGuard* platform. Fig. 16 illustrates the cumulative operation time required for casting the vote, offering valuable insights into the efficiency and duration of the voting procedure.

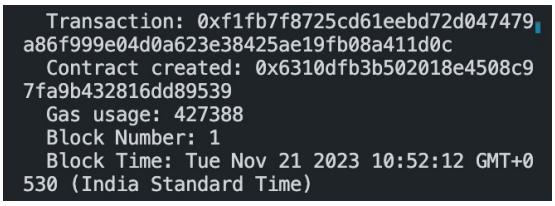

Fig. 15: Smart Contract creation process in DemocracyGuard

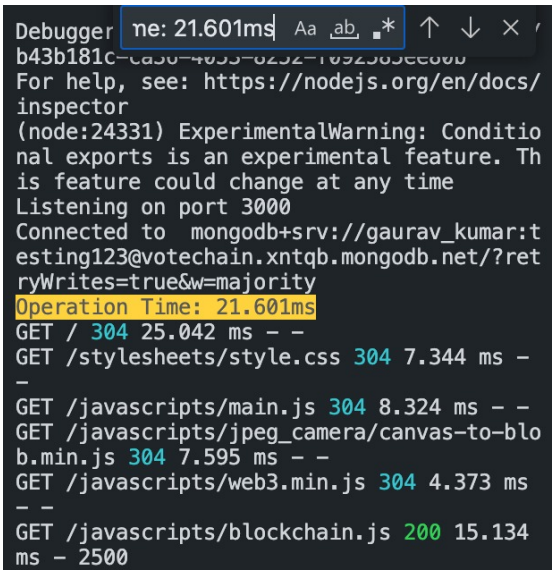

Fig. 16: Total Operation time for casting the vote in DemocracyGuard

C. Comparison with Traditional Voting Systems

A comparative analysis between *DemocracyGuard* and traditional voting systems revealed distinct advantages for the blockchain-based framework. Traditional systems often face challenges related to centralized vulnerabilities, susceptibility to manipulation, and logistical issues. *DemocracyGuard*, on the other hand, demonstrated superior resilience to tampering, increased accessibility, and a reduced likelihood of errors or disputes. TABLE V reveals key insights into the features of various blockchain-based voting frameworks, with a particular focus on *DemocracyGuard*. Among the evaluated frameworks, *DemocracyGuard* scores consistently high, receiving a positive mark (✓) in every analyzed category. Specifically, *DemocracyGuard* excels in providing cost-free voting, biometric verification, a robust blockchain infrastructure, efficient smart contract implementation, enhanced voter turnout mechanisms, secure transaction

TABLE V: Comparative analysis of features in Blockchain-based Voting Framework

Paper Title	Cost-free Voting	Biometric Verification	Blockchain Infrastructure	Smart Contract Efficiency	Voter Turnout Enhancement	Transaction Verification	Admin Verified KYC	Azure Face API
S Wolchok et al. [57]	✓	✗	✗	✗	✗	✗	✗	✗
FÞ Hjálmarsson et al. [52]	✓	✗	✓	✓	✓	✓	✗	✗
W Zhang et al. [2]	✓	✗	✓	✓	✗	✓	✗	✗
B Wang et al. [3]	✗	✗	✓	✗	✗	✓	✗	✗
A Pandey et al. [58]	✓	✗	✓	✗	✗	✓	✗	✗
H Patil et al. [59]	✗	✗	✓	✓	✗	✓	✗	✗
H Yi et al. [53]	✓	✗	✗	✓	✗	✗	✗	✗
KM Khan et al. [60]	✗	✗	✓	✗	✗	✓	✗	✗
M Kamil et al. [54]	✓	✗	✓	✗	✗	✓	✗	✗
U Jafar et al. [12]	✓	✗	✓	✗	✓	✓	✗	✗
R Taş et al. [61]	✓	✗	✓	✓	✗	✓	✗	✗
ST Alvi et al. [15]	✓	✗	✓	✓	✗	✓	✗	✗
MS Farooq et al. [55]	✗	✗	✓	✓	✗	✓	✗	✗
RS Bhadoria et al. [18]	✓	✗	✓	✓	✗	✓	✗	✗
Y Wahab et al. [17]	✓	✗	✓	✓	✗	✓	✗	✗
MN Neloy et al. [56]	✓	✓	✓	✓	✓	✓	✗	✗
MV Vladucu et al. [16]	✓	✗	✓	✓	✗	✓	✗	✗
DemocracyGuard	✓	✓	✓	✓	✓	✓	✓	✓

verification, and an administrator-verified KYC process. This comprehensive approach signifies *DemocracyGuard's* commitment to addressing multiple facets of secure and transparent voting systems.

VI. Conclusion and Future Work

Incorporating blockchain technology into online voting systems holds great potential for addressing the pressing security concerns associated with electronic voting. The decentralized architecture, transparency features, and non-repudiation capabilities inherent in blockchain offer a robust foundation for establishing a trustworthy and resilient electoral process. The proposed DemocracyGuard platform, built on the Ethereum blockchain and complemented by facial recognition technology, represents a significant stride in fortifying voter authentication and enhancing the overall security of online voting. Implementing blockchain in online voting systems requires ongoing attention to various challenges and considerations. Future work should include comprehensive security audits to identify and mitigate potential vulnerabilities, ensuring the platform's resistance to manipulation and unauthorized access. Efforts should be directed towards refining the user experience, making the platform more intuitive and accessible to a diverse range of voters. Scalability remains a critical aspect, and further research should be conducted to optimize the performance of blockchain-based online voting systems, especially as they handle an increasing number of transactions during elections. The DemocracyGuard platform stands as a testament to the potential of blockchain in revolutionizing the electoral landscape. Still, a sustained commitment to improvement and adaptation will be crucial for its long-term success.

References

[1] K. M. AboSamra, A. A. AbdelHafez, G. M. Assassa, and M. F. Mursi, "A practical, secure, and auditable e-voting system," *Journal of information security and applications*, vol. 36, pp. 69–89, 2017.

[2] W. Zhang, Y. Yuan, Y. Hu, S. Huang, S. Cao, A. Chopra, and S. Huang, "A privacy-preserving voting protocol on blockchain," in *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*. IEEE, 2018, pp. 401–408.

[3] B. Wang, J. Sun, Y. He, D. Pang, and N. Lu, "Large-scale election based on blockchain," *Procedia Computer Science*, vol. 129, pp. 234–237, 2018.

[4] A. Sharma, T. Singh, T. Aggarwal, D. Jain, P. Singh *et al.*, "Blockchain based e-voting," in *2022 4th International Conference on Advances in Computing, Communication Control and Networking (ICAC3N)*. IEEE, 2022, pp. 2054–2058.

[5] A. Benny, "Blockchain based e-voting system," *Available at SSRN 3648870*, 2020.

[6] D. A. Kumar and T. U. S. Begum, "A comparative study on fingerprint matching algorithms for evm," *Journal of Computer Sciences and Applications*, vol. 1, no. 4, pp. 55–60, 2013.

[7] R. M. Prasad, P. Bojja, and M. Nakirekanti, "Aadhar based electronic voting machine using arduino," *International Journal of Computer Applications*, vol. 145, no. 12, pp. 39–42, 2016.

[8] "Vvpat | district doda | india," https://doda.nic.in/vvpat/, (Accessed on 09/25/2023).

[9] V. N. R. B, S. Akshay, M. Arun, and I. K. M. A, "Decentralized E-Voting System," pp. 8040–8050, 2019.

[10] 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, 2020.

[11] D. Weiss, J. Wolmer, and A. Vatsa, "Blockchain-based electronic voting system for modern democracy: A review," in *2022 IEEE Integrated STEM Education Conference (ISEC)*. IEEE, 2022, pp. 162–166.

[12] 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, 2021.

[13] R. Cooley, S. Wolf, and M. Borowczak, "Blockchain-based election infrastructures," in *2018 IEEE international smart cities conference (ISC2)*. IEEE, 2018, pp. 1–4.

[14] Y.-X. Kho, S.-H. Heng, and J.-J. Chin, "A review of cryptographic electronic voting," *Symmetry*, vol. 14, no. 5, p. 858, 2022.

[15] S. T. Alvi, M. N. Uddin, L. Islam, and S. Ahamed, "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*, vol. 34, no. 9, pp. 6855–6871, 2022.

[16] M.-V. Vladucu, Z. Dong, J. Medina, and R. Rojas-Cessa, "E-voting meets blockchain: A survey," *IEEE Access*, vol. 11, pp. 23 293–23 308, 2023.

[17] Y. Wahab, A. Ghazi, A. Al-Dawoodi, M. Alisawi, S. Abdullah, L. Hammood, and A. Nawaf, "A framework for blockchain based e-voting system for iraq," *International Journal of Interactive Mobile Technologies*, vol. 16, no. 10, 2022.

[18] R. S. Bhadoria, A. P. Das, A. Bashar, and M. Zikria, "Implementing blockchain-based traceable certificates as sustainable technology in democratic elections," *Electronics*, vol. 11, no. 20, p. 3359, 2022.

[19] P. S. Herrnson, M. J. Hanmer, and R. G. Niemi, "The impact of ballot type on voter errors," *American Journal of Political Science*, vol. 56, no. 3, pp. 716–730, 2012.

[20] L. Leemann and D. Bochsler, "A systematic approach to study electoral fraud," *Electoral studies*, vol. 35, pp. 33–47, 2014.

[21] R. Oppliger, "How to address the secure platform problem for remote

internet voting," *Sis*, vol. 2, pp. 153–173, 2002.
[22] J. Shi, J. Wang, and F. Fu, "Fast and robust vanishing point detection for unstructured road following," *IEEE Transactions on Intelligent Transportation Systems*, vol. 17, no. 4, pp. 970–979, 2015.
[23] D. S. Wallach, "On the security of ballot marking devices," *Ohio St. Tech. LJ*, vol. 16, p. 558, 2020.
[24] A. Riera and P. Brown, "Bringing confidence to electronic voting," *Electronic Journal of e-Government*, vol. 1, no. 1, pp. pp14–21, 2003.
[25] D. Kasdan, *State restrictions on voter registration drives*. New York: Brennan Center for Justice, 2013.
[26] T. S. Roberts, "Enhanced disclosure as a response to increasing out-of-state spending in state and local elections," *Colum. JL & Soc. Probs.*, vol. 50, p. 137, 2016.
[27] F. Hao and P. Y. Ryan, *Real-world electronic voting: Design, analysis and deployment*. CRC Press, 2016.
[28] O. He and Z. Su, *A new practical secure e-voting scheme*. na, 1998.
[29] Y. Yang, Z. Guan, Z. Wan, J. Weng, H. H. Pang, and R. H. Deng, "Priscore: blockchain-based self-tallying election system supporting score voting," *IEEE Transactions on Information Forensics and Security*, vol. 16, pp. 4705–4720, 2021.
[30] L. Vo-Cao-Thuy, K. Cao-Minh, C. Dang-Le-Bao, and T. A. Nguyen, "Votereum: An ethereum-based e-voting system," in *2019 IEEE-RIVF International Conference on Computing and Communication Technologies (RIVF)*. IEEE, 2019, pp. 1–6.
[31] P. P. Mukherjee, A. A. Boshra, M. M. Ashraf, and M. Biswas, "A hyper-ledger fabric framework as a service for improved quality e-voting system," in *2020 IEEE Region 10 Symposium (TENSYMP)*. IEEE, 2020, pp. 394–397.
[32] S. Vivek, R. Yashank, Y. Prashanth, N. Yashas, and M. Namratha, "E-voting system using hyperledger sawtooth," in *2020 International Conference on Advances in Computing, Communication & Materials (ICACCM)*. IEEE, 2020, pp. 29–35.
[33] M. Benji and M. Sindhu, "A study on the corda and ripple blockchain platforms," in *Advances in Big Data and Cloud Computing: Proceedings of ICBDCC18*. Springer, 2019, pp. 179–187.
[34] S. Jani, "Smart contracts: Building blocks for digital transformation," *Indira Gandhi National Open University*, 2020.
[35] V. Cortier, P. Gaudry, and S. Glondu, "Possible evolutions of the voting system in tezos," 2021.
[36] E. Amoah and J.-Y. Oh, "Blockchain adoption in project management," *Issues in Information Systems*, vol. 22, no. 4, pp. 143–156, 2021.
[37] S. Barański, J. Szymański, A. Sobecki, D. Gil, and H. Mora, "Practical i-voting on stellar blockchain," *Applied Sciences*, vol. 10, no. 21, p. 7606, 2020.
[38] I. Coelho, V. Coelho, P. Lin, and E. Zhang, "Community yellow paper: A technical specification for neo blockchain," *NeoResearch, March*, 2019.
[39] J. S. Yadav, N. S. Yadav, and A. K. Sharma, "A qualitative and quantitative parametric estimation of the ethereum and tron blockchain networks," in *2021 9th International Conference on Reliability, Infocom Technologies and Optimization (Trends and Future Directions)(ICRITO)*. IEEE, 2021, pp. 1–5.
[40] C. Esposito and C. Choi, "Design and implementation of a blockchain-based e-voting system by using the algorand platform," in *Proceedings of the 38th ACM/SIGAPP Symposium on Applied Computing*, 2023, pp. 715–723.
[41] F. SAPÁK, "Security and performance analysis of avalanche distributed consensus protocol."
[42] R. K. Mutuku, "Modernizing the kenyan electoral system through polkadot blockchain network," *East African Journal of Information Technology*, vol. 6, no. 1, pp. 77–90, 2023.
[43] P. Lamela Seijas, A. Nemish, D. Smith, and S. Thompson, "Marlowe: implementing and analysing financial contracts on blockchain," in *Financial Cryptography and Data Security: FC 2020 International Workshops, AsiaUSEC, CoDeFi, VOTING, and WTSC, Kota Kinabalu, Malaysia, February 14, 2020, Revised Selected Papers 24*. Springer, 2020, pp. 496–511.
[44] M. Duguleană and F. Gîrbacia, "Augmented reality meets non-fungible tokens: Insights towards preserving property rights," in *2021 IEEE International Symposium on Mixed and Augmented Reality Adjunct (ISMAR-Adjunct)*. IEEE, 2021, pp. 359–361.
[45] A. Yakovenko, "Solana: A new architecture for a high performance blockchain v0. 8.13," *Whitepaper*, 2018.
[46] "Technical paper," https://flow.com/technical-paper, (Accessed on 10/19/2023).
[47] H. Vranken, "Sustainability of bitcoin and blockchains," *Current opinion in environmental sustainability*, vol. 28, pp. 1–9, 2017.
[48] Y. Yanovich, I. Ivashchenko, A. Ostrovsky, A. Shevchenko, and A. Sidorov, "Exonum: Byzantine fault tolerant protocol for blockchains," *bitfury. com*, pp. 1–36, 2018.
[49] A. Baliga, I. Subhod, P. Kamat, and S. Chatterjee, "Performance evaluation of the quorum blockchain platform," *arXiv preprint arXiv:1809.03421*, 2018.
[50] C. G. Akcora, Y. R. Gel, and M. Kantarcioglu, "Blockchain networks: Data structures of bitcoin, monero, zcash, ethereum, ripple, and iota," *Wiley Interdisciplinary Reviews: Data Mining and Knowledge Discovery*, vol. 12, no. 1, p. e1436, 2022.
[51] D. Ashok Kumar and T. Ummal Sariba Begum, "A Comparative Study on Fingerprint Matching Algorithms for EVM," *Journal of Computer Sciences and Applications*, vol. 1, pp. 55–60, 2013.
[52] F. Þ. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa, and G. Hjálmtỳsson, "Blockchain-based e-voting system," in *2018 IEEE 11th international conference on cloud computing (CLOUD)*. IEEE, 2018, pp. 983–986.
[53] H. Yi, "Securing e-voting based on blockchain in p2p network," *EURASIP Journal on Wireless Communications and Networking*, vol. 2019, no. 1, pp. 1–9, 2019.
[54] M. Kamil, A. S. Bist, U. Rahardja, N. P. L. Santoso, and M. Iqbal, "Covid-19: Implementation e-voting blockchain concept," *International Journal of Artificial Intelligence Research*, vol. 5, no. 1, pp. 25–34, 2021.
[55] M. S. Farooq, U. Iftikhar, and A. Khelifi, "A framework to make voting system transparent using blockchain technology," *IEEE Access*, vol. 10, pp. 59 959–59 969, 2022.
[56] M. N. Neloy, M. A. Wahab, S. Wasif, A. All Noman, M. Rahaman, T. H. Pranto, A. B. Haque, and R. M. Rahman, "A remote and cost-optimized voting system using blockchain and smart contract," *IET Blockchain*, vol. 3, no. 1, pp. 1–17, 2023.
[57] S. Wolchok, E. Wustrow, J. A. Halderman, H. K. Prasad, A. Kankipati, S. K. Sakhamuri, V. Yagati, and R. Gonggrijp, "Security analysis of india's electronic voting machines," in *Proceedings of the 17th ACM conference on Computer and communications security*, 2010, pp. 1–14.
[58] A. Pandey, M. Bhasi, and K. Chandrasekaran, "Votechain: A blockchain based e-voting system," in *2019 Global Conference for Advancement in Technology (GCAT)*. IEEE, 2019, pp. 1–4.
[59] H. Patil, P. Ladkat, A. Jituri, R. Desai, and D. S. Shinde, "Blockchain based e-voting system," in *Proceedings of International Conference on Communication and Information Processing (ICCIP)*, 2019.
[60] K. M. Khan, J. Arshad, and M. M. Khan, "Secure digital voting system based on blockchain technology," *International Journal of Electronic Government Research (IJEGR)*, vol. 14, no. 1, pp. 53–62, 2018.
[61] R. Taş and Ö. Ö. Tanrıöver, "A manipulation prevention model for blockchain-based e-voting systems," *Security and communication networks*, vol. 2021, pp. 1–16, 2021.