Journal of King Saud University – Computer and Information Sciences 34 (2022) 6855–6871

Contents lists available at ScienceDirect

Journal of King Saud University – Computer and Information Sciences

journal homepage: www.sciencedirect.com

DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system voting system

Syada Tasmia Alvi [a,*], Mohammed Nasir Uddin [b], Linta Islam [b], Sajib Ahamed [b]

[a] Department of CSE, Daffodil International University, Bangladesh
[b] Department of CSE, Jagannath University, Bangladesh

ARTICLE INFO

Article history:
Received 14 October 2021
Revised 29 May 2022
Accepted 23 June 2022
Available online 1 July 2022

Keywords:
Voting
Blockchain
Ethereum
Smart Contracts

ABSTRACT

Voting is a fundamental democratic activity. Many experts believe that paper balloting is the only appropriate method to ensure everyone's right to vote. But this method is prone to errors and abuse. Many nations utilize digital voting methods to solve the difficulties of paper balloting. A single flaw in digital voting may lead to massive vote-rigging. Election voting methods must be legal, accurate, safe, and convenient. However, issues with digital voting methods may restrict acceptance. Due to its end-to-end verification capabilities, blockchain technology was developed to address these problems. To guarantee We have used blockchain technology anonymity, privacy, verifiability, mobility, integrity, security, and fairness in voting. By using blockchain our proposed system ensures security, privacy, and integrity. This system provides voter anonymity by keeping the voter information as a hash in the blockchain. It also provides fairness by keeping the casted vote encrypted till the ending time of the election. After ending time, the voter can verify their casted vote, ensuring verifiability. To test our protocol, we put it on Ethereum 2.0, a blockchain platform that uses Solidity as a programming language to create smart contracts. The adoption of smart contracts provides a safe means for performing voter verification, ensuring the correctness of voting results, making the counting system public, and protecting against fraudulent activities. We analyzed the system's performance based on security and gas costs. It improves in terms of security characteristics and the related cost for the necessary infrastructure.

1. Introduction

Democracy is defined as the right of people to choose their leaders. Voting is a critical process that enables people to elect their government leader. The electoral system should be democratic, independent, and impartial. As a result, it must be a transparent and secure procedure that allows everyone to share their viewpoint freely (Bosri et al., 2019). Many people in the world do not keep faith in the election system (Inzamam-Ul, YYYY). The Conventional voting is controlled and full of mediators (Asraful and Rashid, 2018). Furthermore, people are dealing with a variety of issues, such as booth capture (Inzamam-Ul, YYYY), dummy voting and the problem of proper monitoring (Rajendran, 2018), a massive line of people in front of the polling booths, false voting, pre-vote casting, redundant vote, lack of law enforcement and audits, political instability, lack of awareness, polling booths are located a long distance away from the house. Older people face significant challenges that lower the number of votes (Madhuri et al., 2017).

The Electronic Voting Machine(EVM) is the alternative to the issues with the old voting system. Nevertheless, because EVM(Electronic Voting Machine) does not fix any security concerns, it also suffers from universal approval problems. The main difficulty with EVM(Electronic Voting Machine) is that it is simple to inject any malware into the device that will mess with the server (Yi, 2019).

Another type of voting is Digital voting which utilizes automated tools to cast ballots, and there are two types of automatic voting: e-voting and I-voting. E-voting is whether electors use a voting machine, and I-vote is where they use an internet browser to do so. Digital voting systems empower electors to vote at any place in the world beyond location limitations that take into account flexibility, confidentiality, protection, and convenience in voting (Dogo et al., 2018). Various nations have begun using digital

* Corresponding author at: Department of CSE, Daffodil International University, Dhaka, Bangladesh.
E-mail address: syada.cse@diu.edu.bd (S.T. Alvi).
Peer review under responsibility of King Saud University.

Production and hosting by Elsevier

https://doi.org/10.1016/j.jksuci.2022.06.014

voting methods. Estonia was the very first country to establish a national Internet voting system. They allowed the citizens to cast their ballots from anywhere around the world through the internet (Hengavalli et al., 2019). Shortly after that, Switzerland adopted electronic voting for regional elections and Norway for local elections (Ayed, 2017).

Digital Voting also has certain drawbacks (Krishnamurthy et al., 2019). The secrecy of significant portions of the code is one of the main criticisms of electronic voting systems in Estonia and Norway. The format for the ballot on the Estonian I-Voting system is restricted due to various confidentiality concerns. The centralization of power of the IV thing enables DDOS attacks susceptible, which will allow electoral elections unavailable to voters (Ayed, 2017). People who vote could question the fairness and confidentiality of the voting process (Zhang et al., 2019). Police and security services have access to network traffic's variety and processing capacity to examine polling data for possible alterations. System attacks are still likely in all previous schemes, even though security is strengthened (Ayed, 2017). Some enhanced security schemes or processes must also ensure that voting or measuring procedures are reliable and the above listed issues are avoided (Krishnamurthy et al., 2019).

However, blockchain technology is a reliable method to overcome the problems above. With the development of blockchain, the central idea of decentralization has progressively gained more recognition (Hsiao et al., 2018). Blockchain is a decentralized network (Zhang et al., 2018) in which the node members exchange data, but each user maintains the identical data replication. Blockchain technology provides characteristics such as dissemination, privacy, and data accuracy (Fusco et al., 2018), etc (Asraful and Rashid, 2018). With the help of blockchain technology, it is possible to build a reliable and secure electronic voting system (Barnes and Perry, YYYY).

Bitcoin is the first application of blockchain technology for cryptocurrencies (Sun et al., 2018). Ethereum's price exceeds US$ 16 billion as of November 2019, making it the second-largest blockchain after Bitcoin (Seifelnasr et al., 2020). A distributed web application that executes on the Ethereum blockchain is referred to as a dApp. It contains capabilities like Smart Contracts and dApps that may be built and run without third-party abuse, falsification, or intervention. DApps may use smart contracts to communicate with Blockchain (Uddin, 2021). An Ethereum virtual machine (EVM) global device is recognized to be a means of carrying out smart contracts. Once an EVM (Ethereum virtual machine) is equipped with a smart contract, it becomes static, which means that the code can no longer be modified or fixed (Seifelnasr et al., 2020). Because of its particular-purpose virtual machine and specialized programming language, Ethereum has seen a significant increase in the number of decentralized and distributed apps. These traits have created the environment for a strong development community, constant advancements, and the introduction of new technical possibilities (Cortes-Goicoechea et al., 2021).

The network's continuous growth has unintentionally resulted in several limits for Ethereum. On the blockchain, transactions take long to execute, often encounter congestion, and incur high gas prices. Ethereum Layer 2 solutions came into play as a result of these constraints (Finextra, YYYY). Layer 2 refers to technologies that allow a program to grow by handling transactions outside of the Ethereum Mainnet (layer 1) while preserving the same protection and decentralization as the mainnet. Layer 2 approaches boost throughput (transaction speed) while also lowering gas costs (White-Gomez, YYYY). Ethereum is on the verge of a significant protocol upgrade that will boost its scalability by many orders of magnitude and create an architecture that can flexibly answer the demands of a continuously evolving industry (Cortes-Goicoechea et al., 2021). Ethereum 2 (also known as Ethereum 2.0) is the next iteration of the Ethereum blockchain system, representing a significant improvement. This means that the Ethereum blockchain will switch from proof-of-work to proof-of-stake for block validation (Bitcoin Suisse, YYYY). This improvement makes it possible to generate blocks in a more environmentally friendly manner, conserving power while developing a more comprehensive network architecture. The implementation of sharding in Eth2 has also been divided into parts due to the challenges of adding this consensus method. PoS is deployed on the Beacon Chain in the first stage, known as "Phase 0," and validators join as proposers and verification committees. The Beacon Chain ensures that validators are assigned to committees at random, laying the groundwork for the next stages (Cortes-Goicoechea et al., 2021). Due to its security, transparency, and flexibility, our purpose is to create a digital voting infrastructure based on the Ethereum blockchain with the addition of a smart contract to avoid and eliminate voting system defects and mitigate difficulties associated with the adoption of blockchain for voting. The main objectives of this paper are:

- To validate the system to ensure only the legitimate voters are allowed to cast their vote.
- To protect voter identity by providing unlinkability between voter and their casted vote.
- To reduce the transaction cost compared with the existing systems.

Since a voting system has to fulfill some security properties such as authentication, transparency, anonymity, integrity, security, privacy, mobility, fairness, and verifiability to achieve a fair and transparent result, the cost is a big issue in the case of implementation of Ethereum based application. So we have discussed the security properties which are satisfied by the proposed system. We have attempted to minimize the systems compute and storage costs while maintaining its essential security properties. We explain the implementation using Ganache, a local blockchain platform integrated into Truffle and analyze the costs associated with generic elections. We also compare the performance of the current proposal to that of prior proposals.

The remainder of the paper is organized as follows-Sections 2 and 3 overview the problem definition and the related works. Section 4 describes the details of the proposed blockchain-based Digital Voting System. Section 5 describes the implementation parts of the proposed system. Section 6 and 7 evaluate the security analysis approach and show the experiment results. Section 8 concludes the paper and highlights some future work.

2. Problem Definition

In the world, mainly democratic countries face many challenges that prevent country growth through various illegal activities such as corruption and violations of human rights, etc. Citizens are often unable to take part in elections because of the voting system (Krishnamurthy et al., 2019). Consequently, whenever it comes to voting, the typical person suffers very much in terms of clarification and protection. In a country like Bangladesh, traditional systems require hours of voting, while they have a lot of repetitive operations and many odd obstacles to elections: capturing polling stations, reinforcing ballots, separating poll agents from competitors, threatening voters to keep away from voting, sometimes polling officer have done bizarre behavior to take the side of particular candidates (theIndependent, YYYY). For these reasons, primarily senior citizens face difficulties casting their vote and avoiding it. In Bangladesh, 5.2 % of people are in the category of senior citizens of overall populations (Wikipedia, YYYY). In the case of voting, 5.2% means a lot as a number of votes can change the result. So the

absence of senior citizens in voting does not fulfill the true democracy. There are also circumstances in which unregistered voters engage in the political system as Dead Voters in the polling stations. Dishonest clerks and officers in the management of a polling station decide to modify the outcomes even after voting (Hjálmarsson et al., 2018). The authorities often order non-residents of an electoral district to leave the city, mobile telephone networks are often closed down, and a complete transport ban is enforced to ensure fair voting, all at people's harassment and misery. Let us think of a person who needs to go to the airport to catch a flight, who needs to see a doctor on an emergency basis. The electors may be on holiday, on business trips, or abroad for some other purpose, mostly for members of associations, which would prohibit the specific voter from voting and will decrease their general involvement in the election (theIndependent, YYYY). Protection, secrecy, accessibility, and anonymity questions have been posed by several citizens (theIndependent, YYYY). This cannot be good for a society in which citizens are wary of exercising their right to choose their leaders and have lost confidence in the administration's democratic process (Pankaj et al., 2017).

The digital method of voting will have greater protection and honesty than others (Patidar and Jain, 2019). Digital voting has a variety of problems (Krishnamurthy et al., 2019). One of the most serious criticisms leveled against both the Estonian and Norwegian electronic voting systems is their inability to keep key portions of the code secret. The content to submit the vote on the Estonian method of I-Voting is discarded due to the general secrecy problems. Voters may be concerned about the validity of the voting system and the lack of anonymity, as well as the possibility of fraud (Zhang et al., 2019). Authorities have access to a broad range of network activity and sufficient computing capabilities to estimate voting outcomes to alter them (Veldre and Andrews, 2014). Even with enhanced security in all prior systems, state-level attacks are still a possibility (Ayed, 2017). Major bugs were found in the software's programming language in Switzerland. Due to a lack of protection and voter trust, e-voting has also been rejected in some instances. This has occurred in Norway, Finland, Ireland, the Netherlands, and Germany, for example (Barnes and Perry, YYYY). When using a digital voting procedure, security is always the primary concern (Barnes and Perry, YYYY). Blockchain is now one of the emerging, rugged technologies that enable applications to obtain strong security mechanisms (Uddin et al., 2019). Blockchain technology may be used to create a reliable and secure automated voting system (Barnes and Perry, YYYY).

3. Related Works

In Khan et al. (2020) propose a way to eliminate the problematic aspects of conventional elections by using blockchain technology. This thesis aims to establish a decentralized e-voting methodology rather than a centralized one via blockchain technology and a readily available voting mechanism that guarantees the security of voters' identification and data transmission and verification. The proposed system uses several technologies, including ganache, truffle framework, and metamask. The limitations of this system are that the casted vote is visible during vote casting, and it does not provide anonymity to the voters.

Boshri et al. Suggested a blockchain-based democratic process based on the Ethereum network (Bosri et al., 2019). The electoral commission established an Ethereum account to hold voter data in this approach. Those voters who do not have access to smartphones may cast their ballots at a designated polling location. They will be required to complete a biometric verification procedure before casting their ballot. Though it uses blockchain technology, there are many involvements of third parties in this system. Only the casted vote is recorded in the chain, which is added by a third party (Kumari et al., 2020). In this case, the false vote is possible. Election administrators Manage the lifecycle of an election.

An electronic voting system is presented in Hjálmarsson et al. (2018) where blockchain is used as a service to create a distributed electronic voting system. This system has two types of nodes: district node and boot node. The district node indicates each voting district, and each district node is equipped with a software application that connects with the bootnode. A bootnode allows district nodes to identify and connect.This system can not protect voters' privacy very well (Qu et al., 2020; Tso et al., 2019; Roh and Lee, 2020) and it doesn't consider self tallying process (Fan et al., 2019).

In Jorge Lopes (2019), they propose a blockchain-based e-voting system using smart contracts. There are three categories of people who can communicate with the program, including the director, the developer, and the voter. Record, Creator, and Election are three contracts. Record contracts are responsible for storing voter registration information to verify authentication. After authentication, the API transfers a transfer of funds to the Creator Contract responsible for establishing a new Election Contract. An Election contract is created, and it sends its address to the Creator Contract for vote casting. Before being added to the blockchain, the ballot is encrypted via homomorphic encryption, which is a kind of symmetric encryption.

In Shahzad et al. (2019), the framework proposed an improved form of e-voting using blockchain. This proof of completeness algorithm deals with the development of blocks, the locking of blocks, the information management, and the design of a blockchain, especially for the voting machines network. In the case of the formation of a block, the presiding officer (PO) shall verify the elector's unique identification and biometric authentication. The voter casts his vote, and then the machine produces a hash using SHA-256 and sends the data to the presiding officer to produce a block. The key downside to this strategy is that it requires more security, privacy, and transparency before it can be considered a fully trustworthy voting method (Toapanta et al., 2019).

In Dagher et al. (2018) BroncoVote, a blockchain-based voting technology is developed to preserve voter anonymity and improve transparency while maintaining an open, safe, and cost-effective voting mechanism. BroncoVote introduces a voting system utilizing blockchain and smart contracts and Ethereum to obtain election administration and auditable election results for university environments. Three contracts are used in this system: Registrar, Creator, and Voting Contract. The limitations of this system is that it has a poorly protected method of registration and a weak voter authentication. Privacy concerns in the process are also present.

Li et al. (2021) created and built AMVchain, an efficient and scalable voting system that uses blockchain and smart contracts to provide transparent and decentralized voting. They begin by examining the flaws and problems of existing blockchain-based voting systems, then review vital research to address these issues. Based on the specifications for a reliable and efficient electronic voting system. Linkable ring signatures are used in the voting process to break the link between voters and votes and ensure voter anonymity.

Alvi et al. (2020) suggested a Digital Voting architecture that contains a smart contract to handle challenges like as authentication, transparency, anonymity, accuracy, and autonomy, as well as singularity, integrity, and mobility, that occur during the use of blockchain for voting. Based on the information supplied by the voters, a hash will be constructed and recorded in the chain in their system. Because the data is stored as a hash on the blockchain, voters will benefit from scalability and anonymity. Smart contracts on the blockchain ensure security and anonymity. A miner is approached by a smart contract to increase transaction speed. A lot of variables contributed to the nomination, including data transmission and energy utilization. Each block has its unique method of

counting votes. At the conclusion of voting, the total vote from the last block may be simply evaluated. It cuts down on counting time.

Uddin et al. (2021) presented a Blockchain-based E-voting system that uses Time Lock Encryption to provide integrity, authentication, and confidentiality. Authentication is accomplished through the use of a blind signature. They also used time lock encryption to ensure secrecy and protect the election from tampering. Only privileged people are allowed to join and vote for a certain political party. Due to the fact that blockchain technology is a decentralized technology, it may be used to overcome the centralized problem. In this article, time lock encryption is used to protect elections from fraud by preventing all parties involved from seeing the results until a specified, predetermined time.

4. Proposed Methodology

The architecture of the proposed methodology is shown in Fig. 1. We have used blockchain technology in our system. There are also some external entities. They are-

- Election commission(EC)- The election commission is in charge of overseeing the whole election process. Election commission is denoted as EC. EC initiates an election, activates it, and then closes it once a set time has passed. EC noticess entire voting process and publishes the result just after election has been over. Another key responsibility of the EC is to establish a voter list prior to the election by conducting a voter registration procedure.
- Voter- People who have the right to vote and are registered to vote in their local election district are called voters. Each voter is allowed to vote for one of the candidates.
- Crypto Server-It is essential to prohibit illegal access to the votes to maintain privacy. Each vote must be encrypted before being sent to the blockchain in order to do this. For this purpose a small node server named as crypto server is only used here for storing the public key and private key. It doesn't store any voting information and voters aren't able to access it.

Voters may use smart devices to cast their votes in the proposed Digital Voting System. Users without smartphones may still vote at a specified voting station. The voting process for both online and onsite voters is the same (see Fig. 2).

The Election commission (EC) is responsible for creating and closing the election by interacting with smart contracts in this

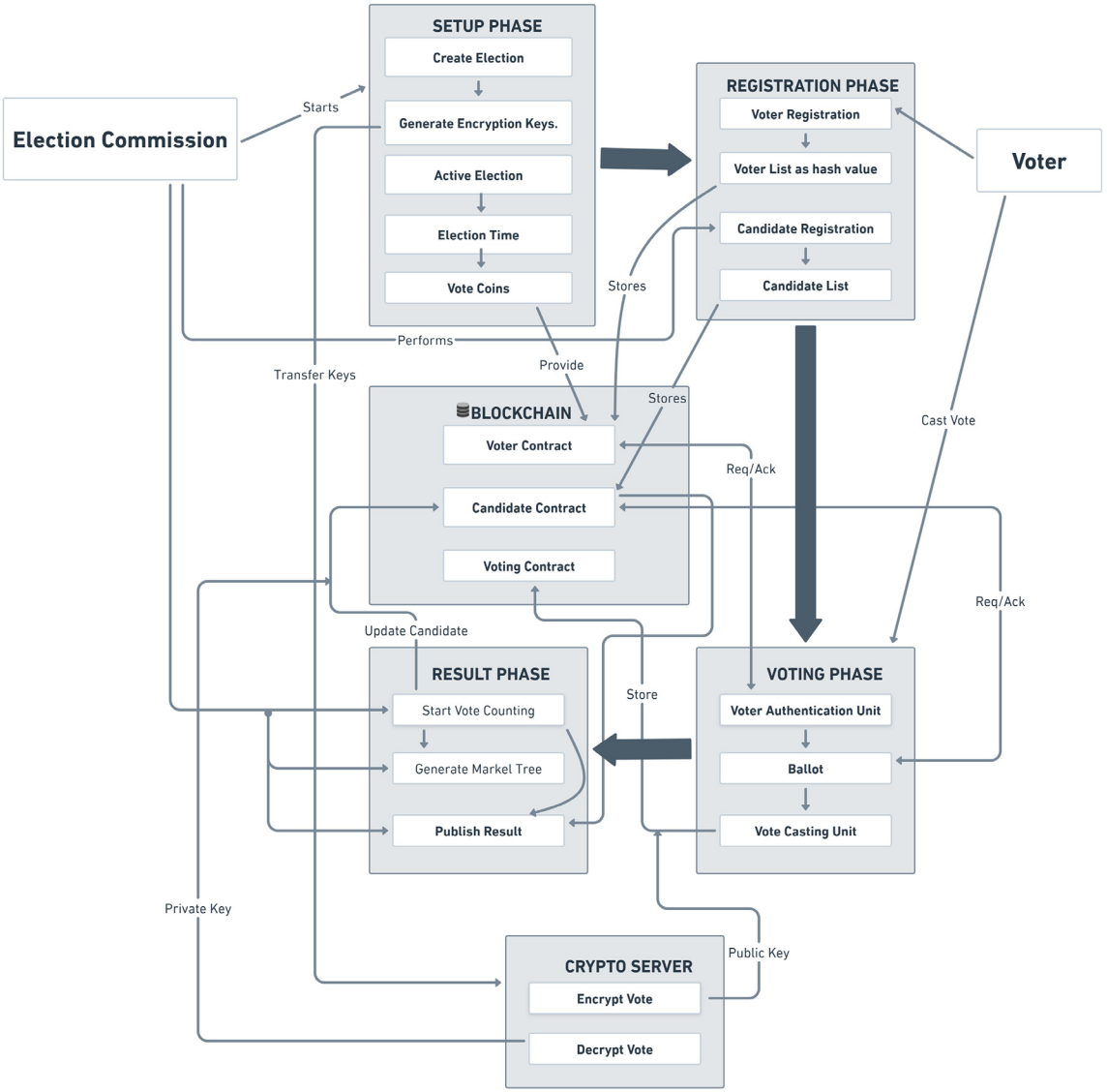

Fig. 1. Blockchain based Digital Voting using smart contracts.

proposed system. Smart contracts identify the responsibilities engaged in the election agreements and the numerous components and transactions that occur throughout the agreement's creation and execution. Three smart contracts are running in the proposed blockchain-based digital voting. They are voter contract, candidate contract, and voting contract. By using these three contracts, the voter's registration process, voter authentication, and voting are done directly between the voter and the blockchain. At first, the hash value of the voter's information is stored by the voter contract during the registration process to secure the voter information and provide anonymity to the voter. These hash values are also used to authenticate voters during vote casting. The candidate contract contains information for the candidates in the chain. After the election starts, voters perform the voter authentication process and then choose one of the candidates from the list of candidates provided by the candidate contract and cast a vote using a vote coin. Here, the vote coin represents the voting status of the voter. If the balance of the vote coin is 1, the voter doesn't cast his vote. If the balance of the vote coin is 0, that means the voter has already casted their vote. The casted vote is encrypted using a public key which Election Commission generates in a crypto server. The encrypted ballot is sent to the voting contract and added as a block in the chain.

For n votes, there will be n voting blocks in our system. After the ending time of the election, EC starts the counting process. In the counting process, the private key from the crypto server is used in the system to decrypt all the casted votes. The voting contract receives the whole of the decrypted vote. Then it sends the voter's vote coin to the chosen candidate's public key for counting without revealing the voter's identity. The candidate contract performs vote-counting operation by providing the candidate's account information and publishing the result.

The proposed voting mechanism includes four phases:

- First Phase: Registration Phase
- Second Phase: Voting Setup Phase
- Third Phase: Voting Phase
- Fourth Phase: Result Phase

The commonly used notations of this paper are presented in Table 1.

4.1. Registration Phase

The First phase of voting system consists of Registration unit which has two parts:

(i) Voters registration
(ii) Candidate Registration

4.1.1. Voter Registration

People who have the right to vote and are registered to vote in their local election district are called voters. The Election Commission provides and maintains an up-to-date list of registered voters. As a result, every eligible voter must visit their local voter registra-

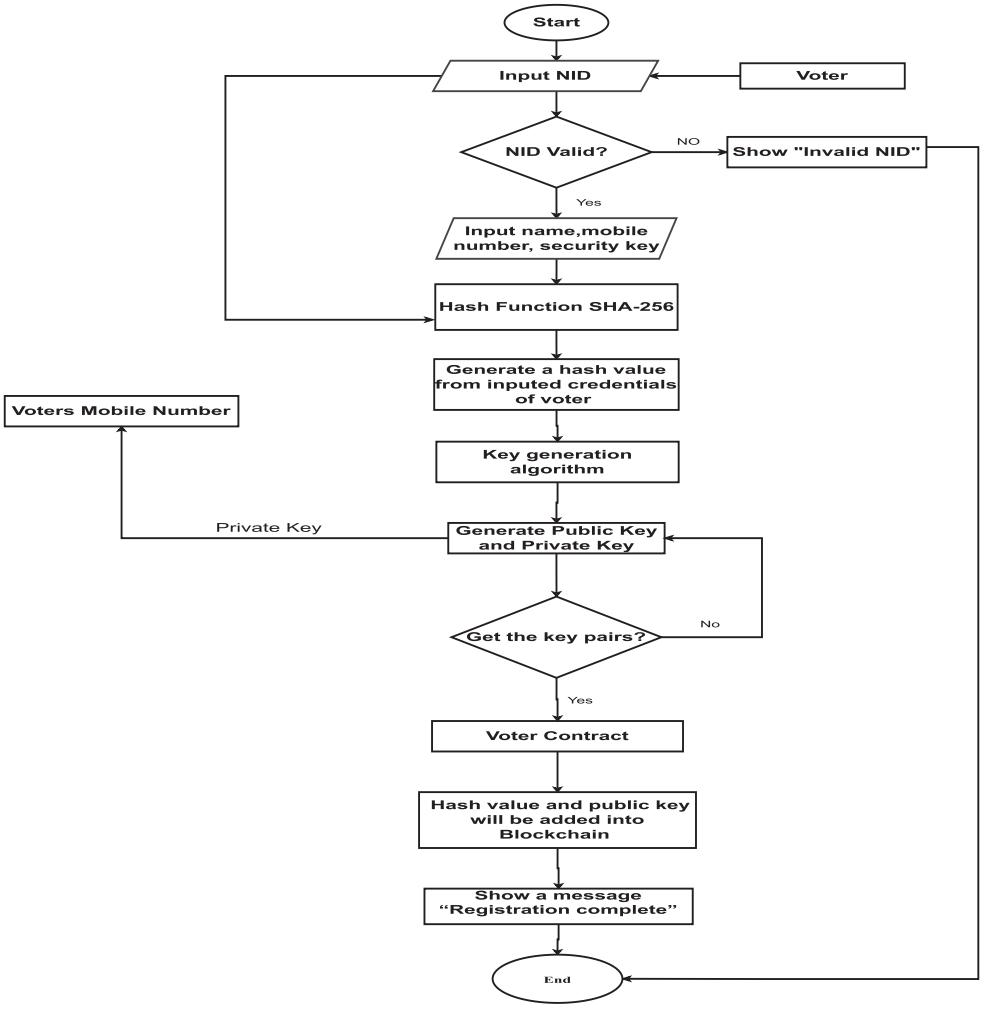

Fig. 2. Flow Chart of Voter Registration.

Table 1
Summary of notations.

Notation	Definition
id	National ID Card Number
nm_v	Voter name
Mb_v	Mobile Number of Voter
sk	Security Key
hv	256 bit fixed length hash value
pub_{kv}	Public key of voter
pv_{kv}	Private key of voter
KGA()	Key Generation Algorithm
OTP	One Time Password
SC_v	Smart Contract named Voter Contract
BC	BlockChain
rg	Region of the nominated candidate
sn	Seat number of region
ps	Party symbol number
SC_{cdt}	Smart Contract named Candidate Contract
pub_{kc}	Public key of Candidate
$info_{cj}$	Information of C_j Candidate where C_j (1 $\leqslant$ j$\leqslant$m)
$pub_{k_{Ec}}$	Public key of Election Commission
$pv_{k_{Ec}}$	Private key of Election Commission
vc	Vote Coin
CS	Crypto Server
s_t	Starting time of election
e_t	Ending time of election
B_i	Digital representation of Ballot form ($1 \leqslant i \leqslant n$),
EB_i	Encrypted Vote
SC_{vt}	Smart Contract named Voting Contract
V_{id}	Vote id
Cj_{ac}	Candidates account
w_c	Wining Candidate

tion center and provide the necessary information to be recognized as a genuine voter. It is the first stage in the system and is needed as part of the identity verification phase in keeping a track of which individuals have casted vote. It also serves as a control mechanism to prevent unregistered individuals from participating in the election by preventing them from casting a ballot.

Let V_i denotes the set of all the voter, $\forall$ voter $\in V_i, |V_i| \geqslant 1$ and there are n voters, $V_i (1 \leqslant i \leqslant n)$.

Algorithm 1: Voter Registration

Input: id, nm_v, Mb_v, sk
Output: hv, pub_{kv}, pv_{kv}

```
Input id
if IDValidation(id) then
    Input nm_v, Mb_v, sk
    hv = generateHash(id,nm_v, Mb_v, sk)
    goto step 8
else
    Return "Invalid NID".
OTP is sent to Mb_v
if (matchOTP (OTP)) then
    Generate pub_kv & pv_kv using KGA()
    Send pv_kv to the Mb_v
    if acknowledge(pv_kv) then
        hv & pub_kv is added in BC by SC_v
        Return Registration Complete Successfully
    else
        go to step 12
else
    go to step 8
```

Algorithm 1 illustrates the voter registration process. ID, voter name, security key, and voter's mobile number are the inputs of this algorithm. The outputs are the hash value of these inputs and two keys named public key and private key. validation() function is used to check the validation of NID at step 2. If the NID is not valid, then Invalid NID will be returned at step 7. If the validation of NID is true, then voters input their credentials in step 3. If all the inputs are taken correctly, then a hash value will generate using the generateHash() function in step 4, where the inputs are the parameters. An OTP will send to the voter's mobile at step 8. matchOTP() function is used to match the sent and input OTP at step 9. If both OTP matches, both public key and private key will generate using KGA() function at step 10. The private key is sent to the voter's mobile number. After getting the acknowledgment of voters getting the key using acknowledge() function at step 12, the hash value and public key of voters are added to the blockchain. At step 14, after performing all the processes, voters get a message Registration Complete Successfully. If the acknowledgment is not got, then go to step 12.

4.1.2. Candidate Registration

Since a candidate is also a voter, the candidate registration procedure is similar to voter registration. They must complete several additional steps following key generating in order to be considered a candidate. The full process of voter and candidate registration process is shown in Fig. 3.

Suppose there are m candidates C_j (1 $\leqslant$ j$\leqslant$m).

Algorithm 2 illustrates the candidate registration process. The candidate is also a voter, so if the candidate is a voter or not checked in step 1. If the candidate is not voter then *voterRegistration*(id, nm, Mb_v, sk) function is called at step 6 where the parameter is same as voter. Candidates must provide their region, party symbol, and seat number to complete the candidate registration procedure after finishing the voter registration process. Candidate contract adds the information of a candidate in the BlockChain, and Registration complete successfully message is returned at step 4 (see Fig. 4).

Algorithm 2: Candidate Registration

Input: id, nm, Mb_v,sk,rg,sn,ps
Output: Cj_{info}

```
if (IsVoter(id, nm, Mb_v,sk)) then
    Input rg,ps,sn
    SC_cdt add Cj_info in BC
    Return Registration Complete Successfully
else
    Call voterRegistration (id, nm, Mb_v,sk)
```

4.2. Voting Setup Phase

This phase is divided into three parts:

(i) Create Election
(ii) Active Election

4.2.1. Create Election

The election is created by EC. Algorithm 3 illustrates the election creation process by EC. EC joins Blockchain using a key pair of public keys and private keys. Then it sends a transaction to the registration contract with n vote coin, starting and ending time

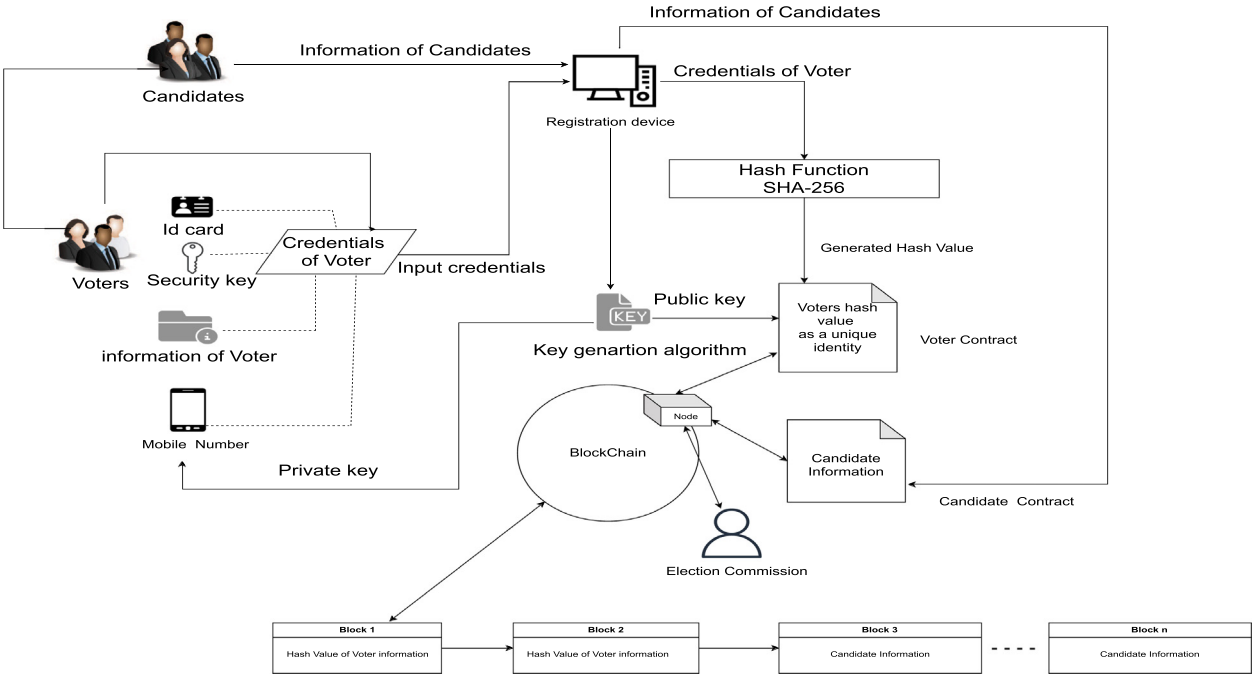

Fig. 3. Voter and Candidate Registration.

of election at step 2. Then transfer the keypair of public key and private key to the crypto server for vote encryption and decryption in step 3 (see Fig. 6–10).

Algorithm 3: Create Election

Input: vc, st, et
1 Join BC using $pub_{k_{Ec}}$ and $pv_{k_{Ec}}$
2 Send a tx =(vc_n, s_t, e_t) to SC_v
3 TransferKey($pub_{k_{Ec}}, pv_{k_{Ec}}$) to CS

4.2.2. Active Election

Algorithm 4 illustrates the election activation process where the inputs are: starting time, ending time,votecoin, and public key of voters. Voter contract sends a transaction of 1 vote coin, starting time, and ending time of election to each voter's public key. All the transactions are added to BlockChain. So the transactions of sending votecoin to the voters and voter's voting status are not hidden in this system.

Algorithm 4: Active Election

Input: st, et, vc, pub_{kv}
Output: vc
1 SC_v create a tx =($vc = 1$)
2 Send tx to V_i's pub_{kv}
3 tx's are added into BC

4.3. Voting Phase

This phase is divided into two parts:

(i) Voter Authentication
(ii) Vote Casting

4.3.1. Voter Authentication

The Voter contract is in charge of the voter authentication procedure. Voters must first sign into their wallets using the private key in order to complete the authentication procedure. After that, the voter must enter their credentials for authentication. In this case, the voter contract receives the credentials and generates a hash value from them in order to compare the hash value with other hash values already present in the blockchain. If both hash values are found equal, the voter is valid for voting.

Algorithm 5 illustrates the voter authentication process where the voter again submits the credentials for generating a hash value at step 1. If the hash value matches the hash value in the voter registration list, then return true at step 3. Otherwise, return false.

Algorithm 5: Voter Authentication

Input: id, nm, Mb_v,sk
Output: hv
1 hv = generateHash(id, nm, Mb_v,sk)
2 **if** *(Hashmatch(hv)* **then**
3 Return"True"
4 **else**
5 Return "False"

4.3.2. Vote Casting Unit

In many ways, the blockchain-based voting mechanism we're proposing is analogous to the concept of digital wallets. Each participant is given a digital wallet by the authority after the registration process, as we see in Section 4.1.1. In this system, voting is a transaction that contains a transaction index, timestamp, vote for the chosen candidate, and transaction hash. After performing the authentication process, the voter can cast a ballot.

Algorithm 6 illustrates the vote casting procedure. After the authentication procedure is completed in step 3, the voter receives a ballot containing a list of candidates with a party symbol. Voters

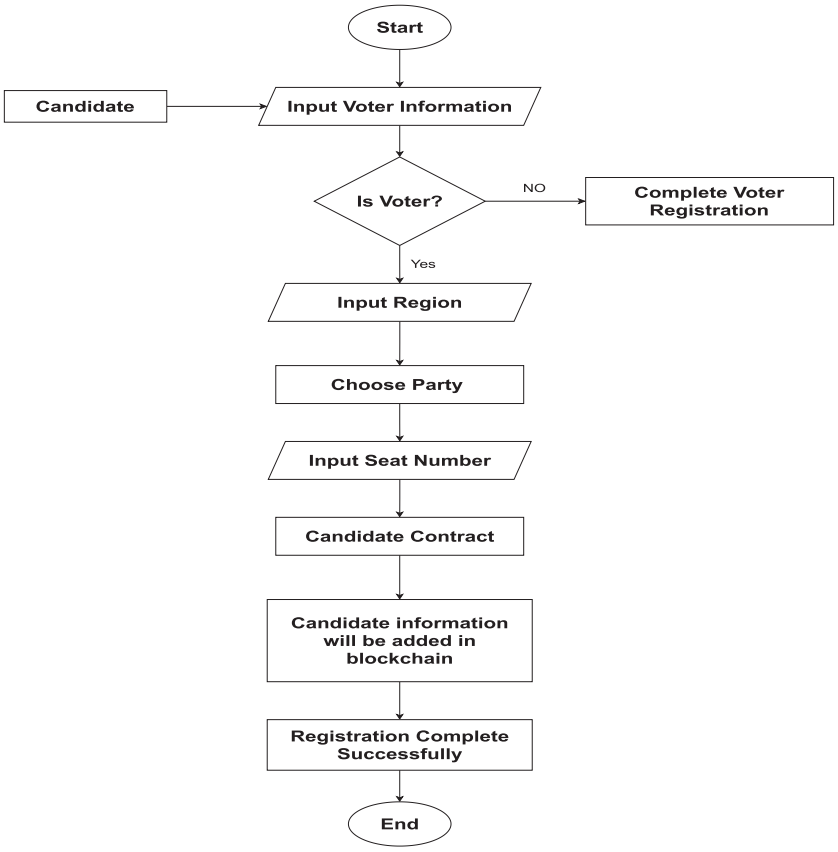

Fig. 4. Flow Chart of Candidate Registration.

can select candidates from the list of candidates and vote using the vote coin in steps 5 and 6. Then the voter will get the vote id at step 7. In steps 8 and 9, the casted vote is encrypted using the election commissioner's public key and saved on the blockchain.

Algorithm 6: Vote Casting

Input: pvk_v
Output: V_{id}
1 Login (pvk_v)
2 $Authentication$ = Voter Authentication (id, nm, Mb_v,sk)
3 **if** *(Authentication==True)* **then**
4 Get $B_i(1 \leq i \leq n)$, where $Cj_{info} \in$Bi
5 Choose C_j from C_{list}
6 Cast Vote to C_j using vc
7 Get V_{id}
8 EB_i = Encrypt(B_i, $pubk_{Ec}$)
9 SC_{vt} receive EB_i
10 **else**
11 "Reject"

4.4. Result Phase

This phase consists of:

(i) Vote Counting Unit
(ii) Publish Result

4.4.1. Vote Counting Unit

EC enters the private key into the system as part of the counting procedure. Each EB_i will be decrypted, and the voting contract will transfer the voting currency to the public key of each of the candidates who have been chosen. Through candidate contract, once the coin is delivered, the vote is tallied soon after receiving it. It is the same as determining the amount of money owned by a specific address. In the end, the number of coins in each candidate's wallet represents the number of votes cast on him.

Algorithm 7 illustrates the process of vote counting. All the encrypted vote is decrypted in step 1 by using the private key of the election commission. Then the voting contract sends a transaction of vote coin to each chosen candidate's public key. After checking the account balance of all the candidates, the winning candidate will be found.

Algorithm 7: Vote Counting

Input: EB_i, pvk_{Ec}
Output: C_{acj}
1 B_i = $decryptBallot(EB_i, pvk_{Ec})$
2 tvc = $sendVoteCoin(B_i, C_i)$
3 C_{acj} = $countVote(tvc)$

4.4.2. Publish Result

After voting, every vote will form a block and add it to the chain. The vote will be counted instantaneously after the vote is submitted, as there will be no risk of vote tampering and vote manipulation.

Algorithm 8 illustrates the result publishing process. The winner is found by checking the account of the candidates in step 1. Then a list is made in step 2, which contains a region, seat number, candidates obtained the vote, and winner of that region. The list is oriented in step 3.

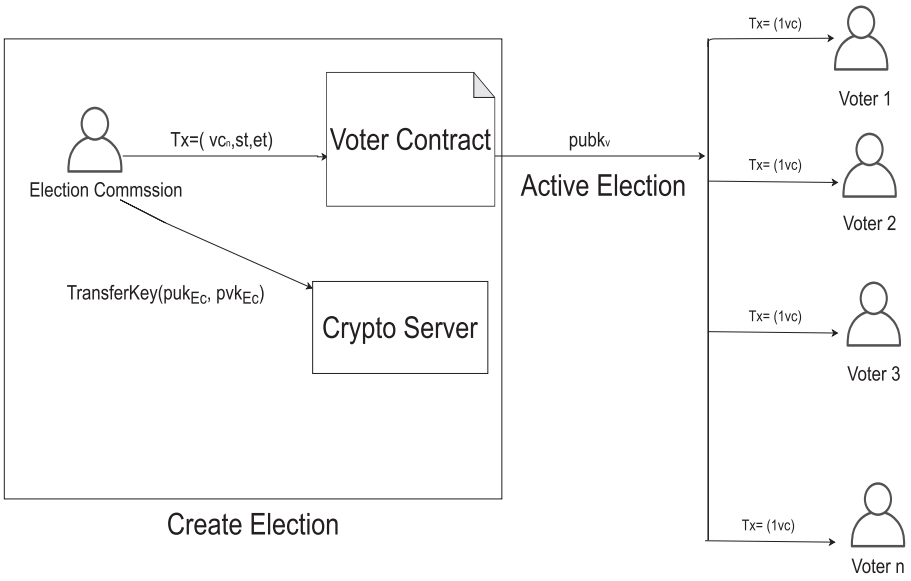

Fig. 5. Create Election and Active Election.

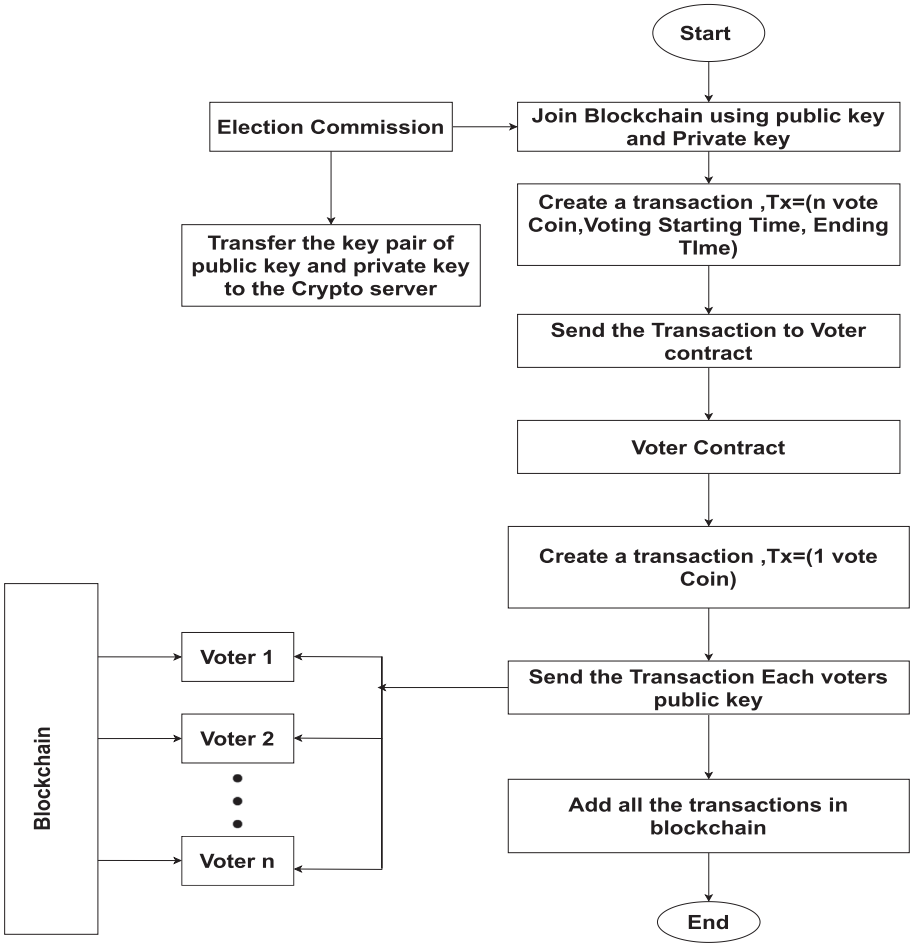

Fig. 6. Flow chart of create and active election.

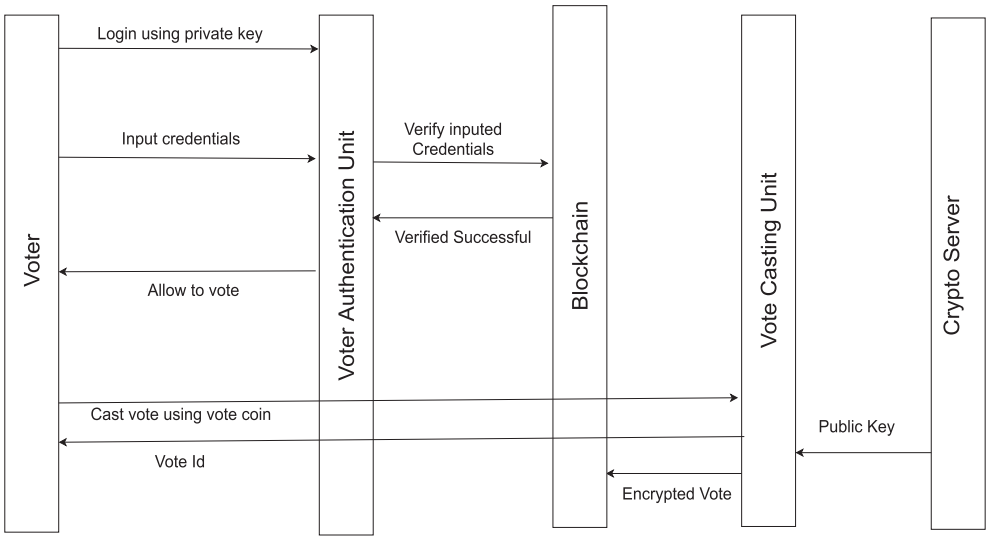

Fig. 7. Voter Authentication and Vote Casting.

Algorithm 8: Publishing Result

Input: C_{ac_j}
Output: w_c
1 w_c= findWinner(C_{ac_j})
2 vt_l = resultList(ps, sn, C_{ac_i}, w_c)
3 print(vt_l)

The result publishing process is shown in Table 2. In this table, the total votes of each candidate and the winning candidate are shown for different regions and seat numbers. Then the final result is published in the result panel.

5. Implementation

The Ethereum blockchain technology is a promising option for computerized voting applications. The Ethereum blockchain provides the ability to design smart contracts. The term "smart contract" refers to a computer program or transaction protocol designed to automatically perform appropriate activities according to the conditions of the agreement. Smart contracts have many objectives, including the elimination of trusted intermediaries, the reduction of arbitration and enforcement costs, the reduction of fraud losses, and the elimination of intentional and inadvertent exceptions. There are two kinds of accounts supported by Ethereum. An externally owned account (also known as a user-controlled account) is controlled by a user. These accounts are denoted by the letters EOA. A contract account is managed by the smart contract that is running on the computer. A contract account is denoted by the letter CA. Both kinds of accounts are capable of storing the Ethereum cryptocurrency, or ether. Ethereum does not execute operations (computations) in a smart contract without user input. As a result, before its functions may be performed, a CA must be enabled by an EOA. The EOA must buy 'gas' in order to carry out its operations, and this must be done using the ether currency (Rogers et al., 2007).

To develop a decentralized application that can effectively substitute a traditional voting system, a website is needed that provides the voting environment. Also, people who cannot go to their polling locations for various reasons may vote by visiting a user-friendly online website displaying their city's election ballot. First and foremost, to implement a blockchain-based voting system in Ethereum, we must first create the necessary environment. The

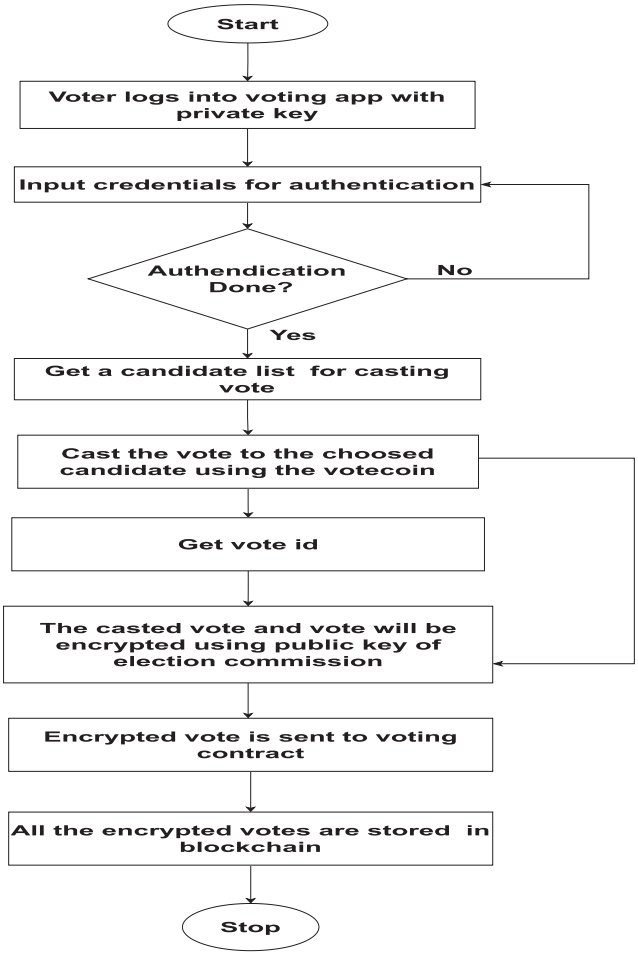

Fig. 8. Flow chart of Voter Authentication and Vote Casting.

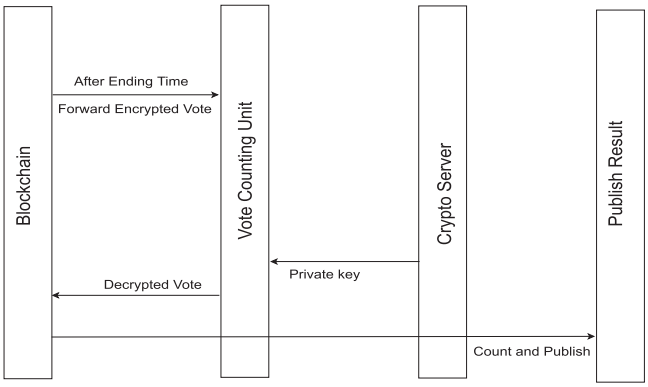

Fig. 9. Vote Counting.

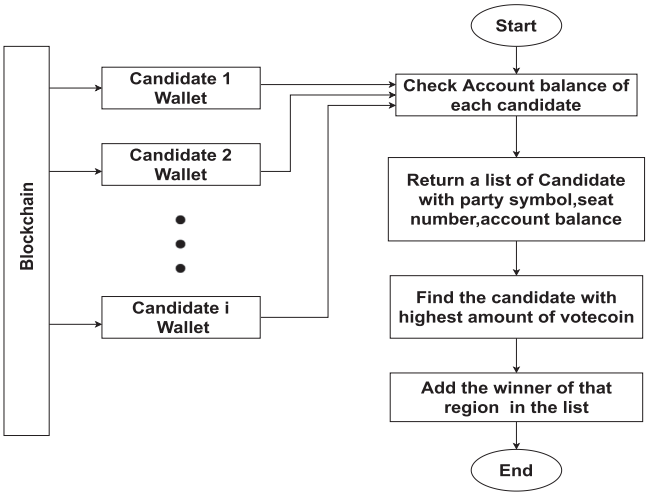

Fig. 10. Flow Chart of Vote Counting.

implementation details is shown in Fig. 11. The application is divided into basically two sides:

1. Server-side and
2. Client-side

5.1. Server-side

On the server side, there is running a blockchain network. The server-side components are:

1. Truffle
2. Solidity
3. Ganache
4. Node Server

5.1.1. Truffle

Truffle is a solidity programming language-based tool for developing ethereum blockchains. Truffle also includes features like as automation testing, client-side development, network management, and smart contract administration (Shakya et al., 2022). The proposed system uses Truffle to manage the network. Truffle is mainly responsible for compiling smart contracts written by solidity, performing migration on various contracts, and generating ABI (Application Binary Interface).

5.1.2. Solidity

Solidity is a contract-oriented, high-level programming language (Khalid et al., 2020) that is used to create smart contracts in our system. It is comparable to JavaScript in its functionality (Kudva et al., 2020).Contracts are organized similarly to classes in object-oriented programming languages when utilizing Solidity for contract development. Like in traditional programming language, contract code is made up of variables and functions (Wohrer and Zdun, 2018). Solidity is compiled into bytecode that can be run on the EVM (Ethereum virtual machine) via the EVM (Ethereum virtual machine) compiler (Khalid et al., 2020).

5.1.3. Ganache

Another tool called ganache is used for managing and testing the application at the local machine. Ganache is a specific RPC-Server that can be checked and built for Truffle, which is accessible as a mobile and commands line application (Khan et al., 2020). Ganache may be used at any point in the development process, allowing you to update, reuse, and test your dApp in a safe and secure manner. It is a tool that allows to run Blockchain locally and perform tests, issue commands, and observe the status of the Blockchain. It's a blockchain simulator that's been installed locally. Ganache uses a graphical interface to simulate Blockchain networks and Live-test Smart Contracts without the use of virtual test networks or a remote network (Gautam et al., 2021). It offers ten previously funded accounts of 100 Ether and a 12-word seeds term for the regeneration of such accounts (Khan et al., 2020).

5.1.4. Node Server

A small node server is used in our system. It acts as a cryptographic server which is named as a crypto server. This server is used for storing the public & private keys for encryption and decryption, respectively, as shown in Fig. 11. EC(Election Commission) generates the keys in this server, which are used to encrypt the casted votes and decrypt them at the counting time.

5.2. Client-side

A client-side user interface has been developed in order to allow people to vote using Ethereum accounts through any computer or mobile device. On the client-side, several tools are used to manage the User Interface (UI). There is CSS for enhancing the design and React JS for handling the client-side data. HTML is also used as the markups. A JavaScript library called web3.js is used for com-

Table 2
Result Publication.

Region (Rg)	Seat Number (Sn)	Candidate of Party1	Candidate of Party2	Candidate of Party3	Winner
X1	1	2000	3000	1000	Party2
X1	2	1000	4000	3000	Party2
X1	3	5000	4000	1000	Party1
X2	4	2000	3000	1000	Party2
X2	5	5000	500	6000	Party3
		Winner		Candidate of Party2	

munication between client and server. Web3.js is a collection of libraries that provides API for interacting with blockchain networks using HTTP, IPC, or WebSocket.

Metamask is a secured crypto wallet and maintains an Ethereum wallet that stores Ethers (or money) and enables users to send and receive Ethers through a dApp of their choice. Meta Mask seems to be a lightweight browser plugin that works with a wide variety of browsers such as Chrome, Firefox, Opera, and Brave (Bhavani et al., YYYY).

Metamask primarily maintains the public and private keys, and the private key is used to sign and confirm transactions (The Defiant, YYYY). The encrypted keys are stored in the browser. Metamask has proved to be very healthy, and no successful hack attempts have resulted in currency loss. It is responsible for managing the user account information such as balance, public and private keys. It is called the bridge between the browser and the blockchain network. It takes requests from the web3 and sends them to the server (Sourav Rajeev et al., 2019).

6. Security Property Analysis

The most fundamental challenges with electronic voting systems are security and confidence (Taş et al., 2021). In order to prevent any enemies or self-interested parties from being able to alter the results and ensure election integrity, we considered that blockchain had enhanced several areas of security and privacy. However, there is still a lot that can be done better. We also want to ensure that the votes that have been tallied are genuine. To ensure a fair and democratic conclusion, the voting process must be fair and transparent. Therefore, ensuring maximum security properties like anonymity, security, privacy, integrity, and verifiability in a voting system is necessary. How the proposed system fulfills all the properties are described below:

6.1. Anonymity

A voter's identity cannot be traced back to a vote they have made. This secures voters by enabling them to express their preferred viewpoints openly. To protect voters' anonymity, adversaries should be unable to associate any vote with a particular voter (Zaghloul et al., 2021). Blockchain ensures anonymity since the public key serves as the voter's identification in the network. In addition to this, the researcher employs a variety of additional methods to conceal the user's identity since maintaining anonymity in an account-model-based system may be difficult (Xin et al., 2019).

This is because every transaction in the system unavoidably updates the account balance of both the transaction sender and the transaction recipient. Even when the privacy of a blockchain system is well-protected, however, legislation becomes a new obstacle to overcome for this system to gain widespread acceptance (Syed et al., 2018). When working in specific blockchain environments, anonymity cannot be ensured (NYCC, YYYY). Since the hash function may offer anonymity (Uddin et al., 2018), the proposed method allows voters to enter their information into the blockchain in an anonymous way. Each voter information is stored as a hash in this system that ensures robust features of privacy preservation and authentication. It allows users to prove their authentication without disclosing their real identities. In the blockchain network, the public key represents the voter's identity, while the hash value represents the voter's data. The casted vote is encrypted to ensure that the voter's votes cannot be linked together in this method. After decrypting all votes, the smart contract sends the vote coin to the candidate without disclosing the voter's identity, preserving the voter's anonymity, as shown in Fig. 12.

6.2. Integrity

Votes should not be modified, forged, or deleted without detection (Shahzad et al., 2019). During the voting process, the integrity of the outcome is a fundamental concept. The Merkle tree is a feature of blockchain technology that guarantees data integrity (Mykletun et al., 2003). Each block in the blockchain comprises a fixed number of transactions. Whenever transactions happen on the blockchain, they are recorded in a data structure known as the Merkle tree. The Merkel tree is built from the bottom up, as seen in Fig. 13. A transaction's hash is calculated and placed in the Merkel tree, which seems to be the tree's lowest tier, as soon as it arrives (leaf nodes). The pairwise hash is then computed by concatenating these hashes into pairs. This procedure is carried out till the Merkel root is established. The hash of each block is produced in this manner. The Merkel tree eliminates the need for nodes to wait for all transactions to be completed before forming a block, increasing the blockchain's security (Sumit Kumar et al., 2019). The Merkle tree ensures the integrity of the proposed digital voting system. In Fig. 14, merkle tree for 8 vote of proposed system is shown.

6.3. Fairness

There should be no early results collected since they may have an impact on the vote of the remaining voters (Dimitriou, 2020). The Fairness process ensures that the results are kept secret throughout the voting phase, ensuring that no voters are manipulated. This is accomplished by employing a digital commitment method and separating the voting and counting stages (Hardwick et al., 2018).

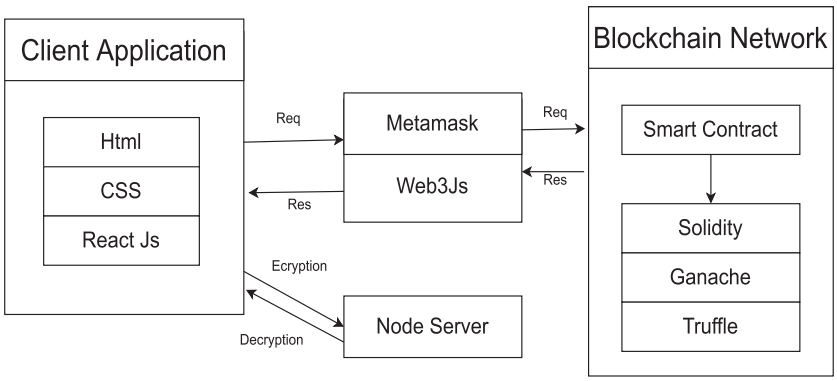

Fig. 11. Flow of implementation.

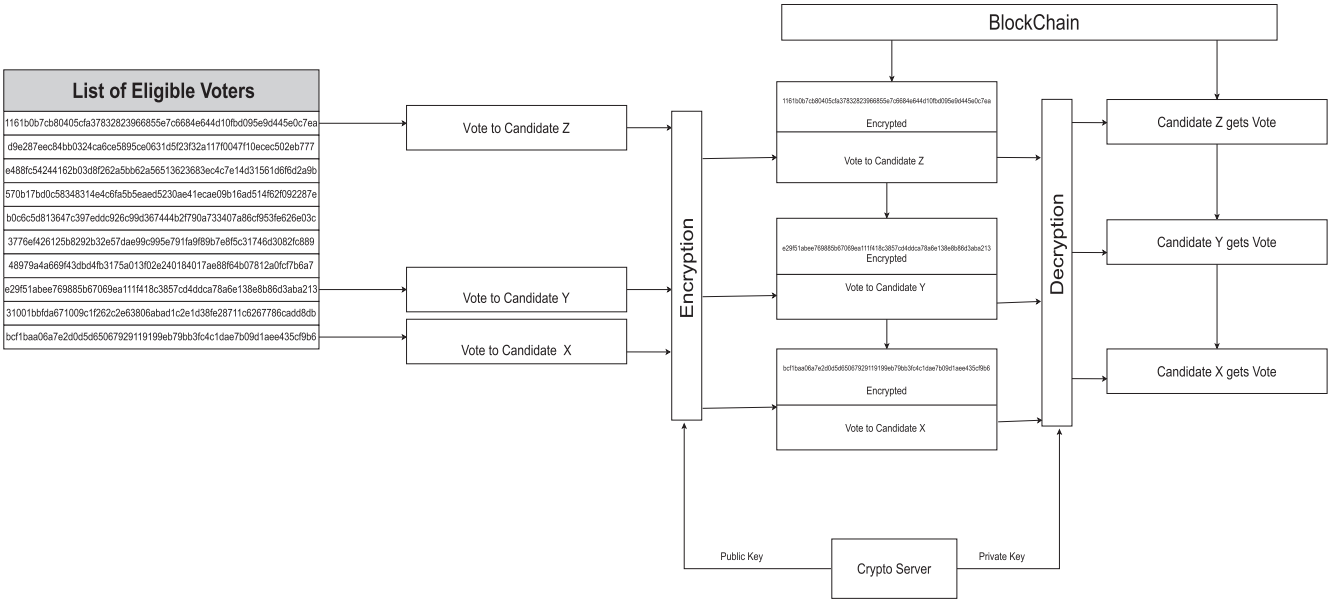

Fig. 12. Anonymity of voter.

To ensure fairness, all votes are encrypted from the moment they are cast until the time the election terminates, as shown in Fig. 15. Votes are encrypted before being cast, so we can not get partial results. After the ending time of the election, all the casted votes are decrypted for counting, which we can see in Fig. 12. From this figure, we can see that the voting stage is separated from the counting stage.

6.4. Verifiability

The capacity of a voter to confirm that his or her ballot has been tallied is referred to as verifiability (Hsiao et al., 2017). Verifiability can be categorized into two: universal and individual verifiability.

- Universal Verifiability: Anyone may clarify that the election result is the same one published, according to universal verifiability.
- Individual Verifiability: Individual verifiability gives an individual voter the ability to verify that one's vote has been counted (Sheer Hardwick et al., 2018).

DVTChain uses blockchain technology. Blockchain technology ensures that every transaction is transparent and verifiable by the whole network. Voters may examine the account details of candidates to see whether the counting procedure has been completed correctly and thus offers universal verifiability. Voters get a VID (vote id) at the moment of voting in the proposed system, as shown in Fig. 16, which is designed to offer individual verifiability.

6.5. Security

By shielding votes from unwanted entry and coercion, the proposed system gives protection. Because of the unchanging feature of the BC, the knowledge (votes) documented on the BC can not be manipulated. When anyone changes a transaction, all the data blocks from that block must be re-mined before the new block. The hash function and the hash function of the previous block are used in a block. Since the data of a block will be manipulated,

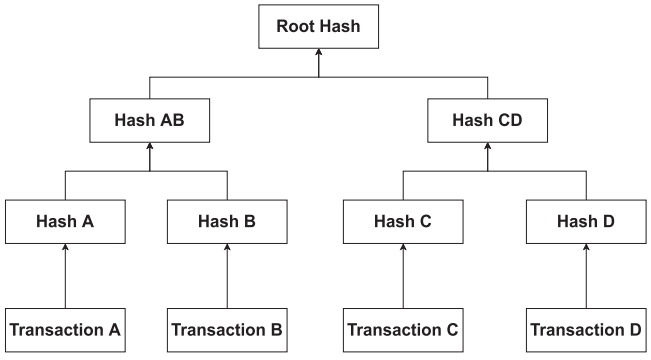

Fig. 13. Merkle Tree.

this adjustment will lead to the differential hash value. The new hash value would clash with the next block value. Therefore, the next block must be re-mined too. For any block in the chain, the same re-mining method is necessary. If the miner operates on the remaining old blocks, new blocks will be recorded on the blockchain, which makes it incredibly difficult to exploit a single block of data. The calculation capability required for this is immense and, in real life, virtually impossible. It makes blockchain secure for us; ballots are a piece of faulty evidence, and the votes in the system cannot be abused at all (Bosri et al., 2019).

6.6. Privacy

An individual voter's voting method should not be disclosed to anybody else. This characteristic is maintained in non-electronic voting systems by physically shielding the voter from prying (Chaieb et al., 2019). Privacy is ensured by preserving the anonymity of voter identities. In order to protect the secrecy of each voter, no specific vote can be traced back to the voter since voter information is recorded in the blockchain as a hash, which is the unique identity of a voter.

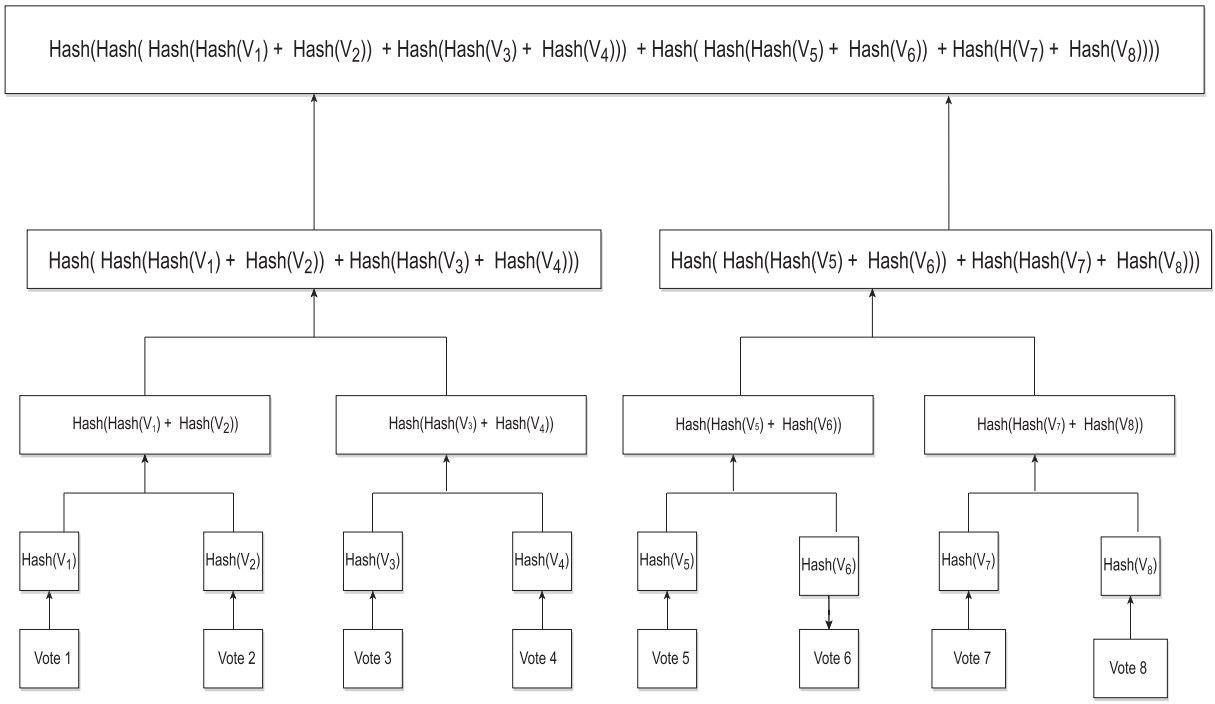

Fig. 14. Merkle Tree for eight vote.

Fig. 15. Block structure during vote casting and after ending time of election.

The privacy in our system derives from (a) the hash value of voter information makes it impossible to link a voter's identity with his/her messages on the blockchain (b) all casted votes of the voters remain encrypted during vote casting (d) after the ending time of the election, only the casted vote will be decrypted, as shown in Fig. 14.

6.7. Uncoercability

In order to ensure that voters do not feel pressured or forced to vote, the system should enable them to do so. Only a voter can decide his intention (Ghavamipoor et al., 2013). During the vote casting, all casted votes are encrypted, as shown in Fig. 14. The system is not insensitive to coercion since a legitimate cast vote cannot be altered by the voter.

6.8. Mobility

Mobility means the voter has the facility to cast their vote from anywhere (Jorge Lopes, 2019). Voting systems should be readily accessible at voting time. The location of the vote should not be limited in voting systems (Jafar et al., 2021). The proposed method requires just a device with internet connectivity and a blockchain address to access the voting network. Thus no additional infrastructure or voting equipment is needed.

6.9. Uniqueness

Uniqueness means a voter should be allowed to cast just one vote that is included in the final vote. The voter will have no permission to vote more if he wants to cast votes (Alvi et al., 2021).

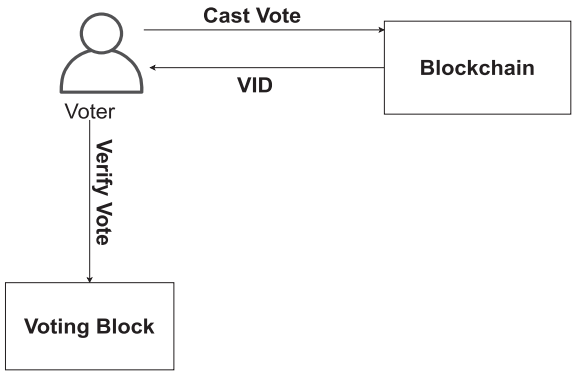

Fig. 16. Verifiability.

Table 3
Gas costs for initial contract deployment

Contract	Gas Used	Actual Cost(Ether)
Voter Contract	614032	0.01228064
Candidate Contract	579917	0.01159834
Voting Contract	734353	0.01468706

Table 4
Gas costs for different operation.

Operation	Gas Used	Actual Cost(Ether)
Voter Registration	114234	0.0022847
Candidate Registration	136934	0.0027387
Store encrypted vote	382606	0.0076521
Send decrypted vote to candidate	14447	0.0002889

In the proposed system, there is a smart-contract named as a voter contract used for voters which are used to notify the voters that the election process is activated, as shown in Fig. 5. This contract can also monitor the voting status of a voter by maintaining a list of the voter as a hash with the balance of the vote coin. At the beginning of the election, the balance of vote coin of all the voters will be one in this list. Whenever the voter casts his/her vote, the balance of the vote coin will become zero. As a result, a voter is unable to cast another legal vote. This is how the system is able to satisfy the uniqueness property by using the vote coin.

7. Analysis of Cost of the Proposed system

The currency in the Ethereum system is known as Ether (ETH). Computation is repaid in ETH inside the blockchain and EVM (Ethereum virtual machine), whereas the implementation fee is measured in gas. Practically, one gas unit corresponds to the efficiency of a single computing step and gas. ETH is purposefully separated in just such a way that global business forces cause ETH price volatility, and the cost of gas is closely related to the cost of computing. The Ethereum contract defines the details validated by the exchange-initiating group and contains a notification transmitted to any other blockchain user from the client. In the case of function calls for each contract, contracts can also transmit data among all other contracts in this manner. Throughout a transaction, there might be a *gasPrice* section representing the sender's gas payment. The performance of a contract is triggered by a receipt or other transaction. On each network node, each instruction will be conducted. There is a defined cost within each operation carried out, represented in multiple gas units, and each transfer has a fixed ether cost identical to gasLimit * gasPrice (Braghin et al., 2019).

In Table 3, we have shown the gas costs for the initial deployment of three smart contracts. Typically, the price of gas is roughly 0.00000002 Ether, or 20 Gwei (Alrebdi et al., 2022). It is the standard value (CryptoVantage, YYYY).

Table 4 shows the gas costs for different operations of the proposed digital voting. Voter registration and candidate registration cost can vary depending on the size of the information of voters and candidates. Other costs are fixed.

Table 5 demonstrates the contrast between the related work and the proposed system based on the used gas, provided property, and the operations performed in the blockchain.

Figs. 17 and 18 show the comparison of existing and proposed systems based on contract deployment cost and provided security properties. We can see that the cost of Khan et al. (2020) and Hjálmarsson et al. (2018) is less than the proposed system in Fig. 16 because the provided property of these two systems are less than others which can be easily understood from Fig. 17.

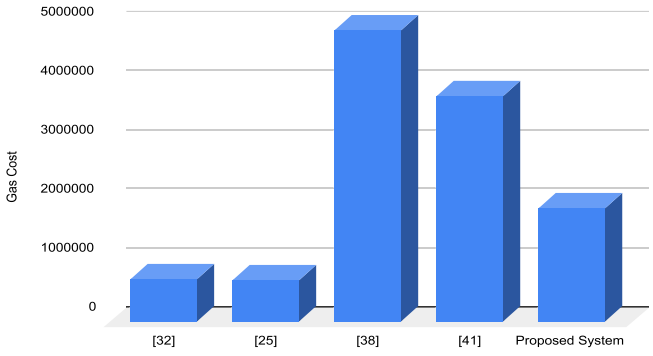

Fig. 17. Comparison of Contract deployment Cost.

Table 5
Comparison of Contract Deployment.

Contract	Gas Used	Provided Property	Operation
Khan et al. (2020)	726774	Integrity, Security, Verifiability	Vote Casting
Hjálmarsson et al. (2018)	701538	Integrity,Security, Fairness	Vote Casting, Vote Counting
Jorge Lopes (2019)	4935530	Anonymity, Privacy, Security, Fairness, Mobility, Uncoercability	Voter Registration, Ballot Creation, Vote Casting, Vote Counting
Dagher et al. (2018)	3817723	Anonymity, Integrity, Privacy, Security, Fairness, Mobility, Uncoercability	Voter Registration, Ballot Creation, Vote Casting, Vote Counting
Proposed System	1928302	Anonymity, Integrity Privacy, Security, Fairness, Mobility, Uncoercability	Voter Registration, Candidate Registration, Vote Casting, Vote Counting

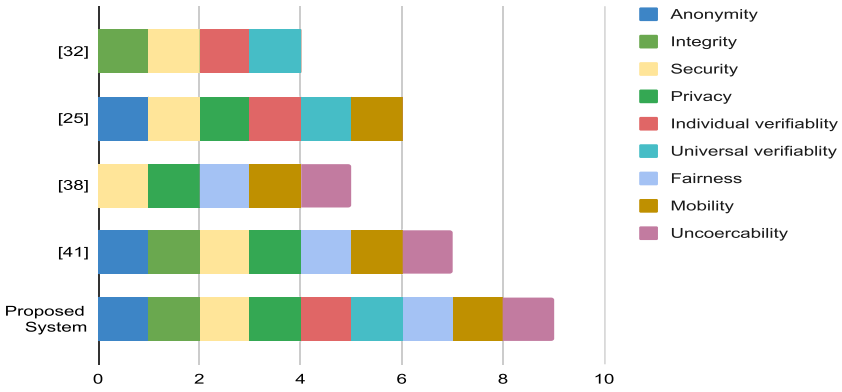

Fig. 18. Comparison of Security Properties.

8. Conclusions and Future Works

This part analyzes and finalizes the research study provided in this work with a few guidelines for future practice. However, the limitations exist that can be overcome in the following implementations of this work and improvement ideas to be executed.

8.1. Summary of the Proposed Mechanism

In the voting system, several countries face crucial uncertainties in ensuring stability. Ensuring the engagement and credibility of the electorate, the fairness of the polling data, and the non-manipulative vote counting, we developed a blockchain-based digital voting system using smart contracts. In this mechanism, three smart contracts are performed various operations of the full election process. So the involvement of the third part is less than other existing systems. The casted votes are kept encrypted until the ending time of the election. So no one can find the link between vote and voter. We have stored the voter's information as a hash so that no one can identify the voter in the network. Here, the data is preserved as a hash instead of full information, so cost is also reduced. After the ending time o the election, voters can also verify their vote by using a vote id which they will get at the time of vote casting. This process facilitates voters to vote for their candidate via smart devices from everywhere in the world. This would help to increase the number of voters in order to attain democracy in every region. So, in conclusion, we can say that our method can be successfully used in the election process as it provides maximum security properties such as anonymity, integrity, security, privacy, fairness, verifiability, and mobility.

8.2. Limitations

The limitation of this system is that we do not implement the OTP (One Time Password)option in our registration process. Another limitation is that we have stored the encrypted vote in the blockchain during vote casting. This data will not be used after the end of the election. For storing these data, the cost has increased.

8.3. Future Research Directions

The limitations that have been mentioned formerly are going to be part of future work. Therefore, we target to use of sidechains in our proposed method as using duplicate currency, and sidechains expand the capabilities of blockchains by executing some activity outside them and returning the outcome to the mainchain for usage. So we can store the encrypted vote in the sidechain and can use the decrypted result in the mainchain, which will reduce the cost.

Funding

This research received no specific funding from public, commercial, or not-for-profit funding agencies.

Declaration of Competing Interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

References

Alrebdi, Norah, Alabdulatif, Abdulatif, Iwendi, Celestine, Lian, Zhuotao, 2022. Svbe: searchable and verifiable blockchain-based electronic medical records system. Scientific Reports 12 (1), 1–11.

Alvi, Syada Tasmia, Uddin, Mohammed Nasir, Islam, Linta, 2020. Digital voting: A blockchain-based e-voting system using biohash and smart contract. In: 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT), pp. 228–233.

Alvi, Syada Tasmia, Islam, Linta, Rashme, Tamanna Yesmin, Uddin, Mohammed Nasir, 2021. Bsevoting: A conceptual framework to develop electronic voting system using sidechain. In: 2021 8th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI), pp. 10–15.

Asraful Alam, S.M., Rashid, Zia Ur, 2018. Md Salam, and Ariful Islam. Towards blockchain-based e-voting system. 10.

Christopher Brake Andrew Barnes and Thomas Perry. Digital voting with the use of blockchain technology, a. https://www.economist.com/sites/default/files/plymouth.pdf.

Christopher Brake Andrew Barnes and Thomas Perry. Digital voting with the use of blockchain technology, b. https://www.economist.com/sites/default/files/plymouth.pdf.

Ben Ayed, Ahmed, 2017. A conceptual secure blockchain based electronic voting system. International Journal of Network Security & Its Applications 9, 01–09.

VV Bhavani, K Saisri, K Naveen, and M Lalitha. Personalised secure e-identity card.

Bitcoin Suisse. Frequently asked questions about ethereum 2. https://www.bitcoinsuisse.com/eth-2-faq.

Bosri, R., Uzzal, A.R., Omar, A.A., Hasan, A.S.M.T., Bhuiyan, M.Z.A., 2019. Towards a privacy-preserving voting system through blockchain technologies. In: 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech), pp. 602–608.

Chiara Braghin, Stelvio Cimato, Simone Cominesi, Ernesto Damiani, and Lara Mauri. Towards Blockchain-Based E-Voting Systems, pages 274–286. 12 2019. ISBN 978-3-030-36690-2.

Chaieb, Marwa, Koscina, Mirko, Yousfi, Souheib, Lafourcade, Pascal, Robbana, Riadh, 2019. Dabsters: A privacy preserving e-voting protocol for permissioned blockchain. In: International Colloquium on Theoretical Aspects of Computing. Springer, pp. 292–312.

Cortes-Goicoechea, Mikel, Franceschini, Luca, Bautista-Gomez, Leonardo, 2021. Resource analysis of ethereum 2.0 clients. In: 2021 3rd Conference on Blockchain Research Applications for Innovative Networks and Services (BRAINS), pp. 1–8.

CryptoVantage. Everything you need to know about ethereum gas fees. https://www.cryptovantage.com/guides/what-are-ethereum-gas-fees/.
Gaby Dagher, Praneeth Marella, Matea Milojkovic, and Jordan Mohler. Broncovote: Secure voting system using ethereum's blockchain. pages 96–107, 01 2018.
Dimitriou, Tassos, 2020. Efficient, coercion-free and universally verifiable blockchain-based voting. Computer Networks 174, 107234.
Eustace Dogo, N Nwulu, Olaniyi Olayemi Mikail, Clinton Aigbavboa, and Thembinkosi Nkonyana. Blockchain 3.0: Towards a secure ballotcoin democracy through a digitized public ledger in developing countries. 09 2018.
Fan, Xuepeng, Li, Peng, Zeng, Yulong, Zhou, Xiaoping, 2019. Implement liquid democracy on ethereum: A fast algorithm for realtime self-tally voting system, p. 11.
Finextra. Top ethereum layer 2 networks. https://www.finextra.com/blogposting/21237/top-ethereum-layer-2-networks.
Francesco Fusco, Maria Ilaria Lunesu, Filippo Pani, and Andrea Pinna. Crypto-voting, a blockchain based e-voting system. pages 223–227, 01 2018.
Gautam, Mehul, Akthar, Shoaib, Basha, Aktar, Dilip, Golda, 2021. Blockchain for secure and proper management of medical data and records. In: 2021 5th International Conference on Electronics, Communication and Aerospace Technology (ICECA), pp. 671–678.
Ghavamipoor, Hoda, Shahpasand, Maryam, 2013. An anonymous and efficient e-voting scheme. In: 7th International Conference on e-Commerce in Developing Countries:with focus on e-Security, pp. 1–13.
Hardwick, Freya Sheer, Gioulis, Apostolos, Akram, Raja Naeem, Markantonakis, Konstantinos, 2018. E-voting with blockchain: An e-voting protocol with decentralisation and voter privacy. In: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), IEEE, pp. 1561–1567.
Hengavalli, Pranith, Manoj, M.V., Bs, Prashanth, Thomas, Likewin, Srinivasa Murthy, Y.V., 2019. End-to-end verifiable electronic voting system using delegated proof of stake on blockchain. SSRN Electronic Journal 01.
F. p. Hjálmarsson, G.K. Hreiðarsson, M. Hamdaqa, and G. Hjálmtýsson. Blockchain-based e-voting system. In 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), pages 983–986, 2018.
Hsiao, Tsung-Chih, Zhen-Yu, Wu., Liu, Chia-Hui, Chung, Yu-Fang, 2017. Electronic voting systems for defending free will and resisting bribery and coercion based on ring anonymous signcryption scheme. Advances in Mechanical Engineering 9. 168781401668719.
Jen-Ho Hsiao, Raylin Tso, Chien-Ming Chen, and mu-en wu. Decentralized E-Voting Systems Based on the Blockchain Technology, pages 305–309. 01 2018. ISBN 978-981-10-7604-6.
Md. Inzamam-Ul Haque 3 Mohammed Golam Sarwar Bhuyan4 Md. Shahriare Arnob1, Niloy Sarker2. Blockchain-based secured e-voting system to remove the opacity and ensure the clarity of election of developing countries. In International Research Journal of Engineering and Technology (IRJET), volume 7.
Jafar, Uzma, Aziz, Mohd Juzaiddin Ab, Shukur, Zarina, 2021. Blockchain for electronic voting system–review and open research challenges. Sensors 21 (17), 5874.
José Luís Pereira Jorge Lopes. Blockchain based e-voting system: A proposal. In Twenty-fifth Americas Conference on Information Systems, Cancun, 2019, 2019.
Umair Khalid, Muhammad Asim, Thar Baker, Patrick Hung, Muhammad Adnan Tariq, and Laura Rafferty. A decentralized lightweight blockchain-based authentication mechanism for iot systems. Cluster Computing, 23, 09 2020.
Saad Moin Khan, Aansa Arshad, Gazala Mushtaq, Aqeel Khalique, and Tarek Husein. Implementation of decentralized blockchain e-voting. EAI Endorsed Transactions on Smart Cities, 4 (10), 6 2020.
Krishnamurthy, R., Rathee, Geetanjali, Jaglan, Naveen, 2019. An enhanced security mechanism through blockchain for e-polling/counting process using iot devices. Wireless Networks 08.
Sowmya Kudva, Renat Norderhaug, Shahriar Badsha, Shamik Sengupta, and A.S.M. Kayes. Pebers: Practical ethereum blockchain based efficient ride hailing service. 01 2020.
Kumari, Pooja, Sheri, Bhagia, Siddiqui, Isma, Khatri, Khubaib, 2020. Conventional vs blockchain-based e-vote system.
Chenchen Li, Jiang Xiao, Xiaohai Dai, and Hai Jin. Amvchain: authority management mechanism on blockchain-based voting systems. Peer-to-peer Networking and Applications, pages 1–12, 2021.
Madhuri, B., Adarsha, M.G., Pradhyumna, K.R., Prajwal, B.M., 2017. Secured smart voting system using aadhar. In: 2017 2nd International Conference On Emerging Computation and Information Technologies (ICECIT), pp. 1–3.
Mykletun, Einar, Narasimha, Maithili, Tsudik, Gene, 2003. Providing authentication and integrity in outsourced databases using merkle hash trees. UCI-SCONCE Technical Report.
NYCC. Benefits and challenges of blockchain technology. https://www.nycg.global/benefits-and-challenges-of-blockchain-technology/.
Mr. Pankaj Sharma Neha Saini, Himani Verma. An analytical study of e-voting system. volume 04, 2017.
Patidar, K., Jain, S., 2019. Decentralized e-voting portal using blockchain. In: 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), pp. 1–4.
Wenlei Qu, Lei Wu, Wei Wang, Zhaoman Liu, and Hao Wang. A electronic voting protocol based on blockchain and homomorphic signcryption: Na. Concurrency and Computation: Practice and Experience, page e5817, 06 2020.
Rajendran Anandha Jothi. Confidential e-voting system using face detection and recognition. 3, 06 2018.
B. Rogers, S. Chhabra, M. Prvulovic, and Y. Solihin. Using address independent seed encryption and bonsai merkle trees to make secure processors os- and performance-friendly. In 40th Annual IEEE/ACM International Symposium on Microarchitecture (MICRO 2007), pages 183–196, 2007.
Chang-Hyun Roh* and Im-Yeong Lee**. A study on electronic voting system using private blockchain. JOURNAL OF INFORMATION PROCESSING SYSTEMS, 16, 04 2020.
Seifelnasr, Mohamed, Galal, Hisham S., Youssef, Amr M., 2020. Scalable open-vote network on ethereum. IACR Cryptology ePrint Archive 2020, 33.
Shahzad, B., Crowcroft, J., 2019. Trustworthy electronic voting using adjusted blockchain technology. IEEE Access 7, 24477–24488.
Samarth Shakya and Vivek Kapoor. A decentralized polling system using ethereum technology. Journal of Information Technology Management, 14 (Security and Resource Management challenges for Internet of Things): 1–8, 2022.
Sheer Hardwick, F., Gioulis, A., Naeem Akram, R., Markantonakis, K., 2018. E-voting with blockchain: An e-voting protocol with decentralisation and voter privacy. In: 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), pp. 1561–1567.
Sourav Rajeev Rohan Varghese Mathew V. Arun, Aditya Dutta. E-voting using a decentralized ethereum application. 04 2019.
Sudhanshu Saxena Dr. Hemavathi P Ananya Sumit Kumar, Darshini N. Voteeth: An e-voting system using blockchain. In International Research Journal of Computer Science (IRJCS), volume 5, 2019.
Sun, Xin, Wang, Quanlong, Kulicki, Piotr, Sopek, Mirek, 2018. A simple voting protocol on quantum blockchain. International Journal of Theoretical Physics 10.
Syed, Shahram Najam, Shaikh, Aamir, Naqvi, Shabbar, 2018. A novel hybrid biometric electronic voting system: Integrating finger print and face recognition. Mehran University Research Journal of Engineering and Technology 37, 01.
Ruhi Taş and Ömer Özgür Tanrıöver. A manipulation prevention model for blockchain-based e-voting systems. Security and Communication Networks, 2021, 2021.
The defiant. What is metamask? https://thedefiant.io/what-is-metamask/.
theIndependent. Blockchain could be the answer to fair voting in bangladesh, a. http://www.theindependentbd.com/post/234648.
theIndependent. Significance of electronic voting machine in bangladesh, b. http://www.theindependentbd.com/printversion/details/204166.
S.M.T. Toapanta, Marjorie Isanoa Sinche, and L. Gallegos. A cyber environment approach to mitigate vulnerabilities and threats in an electoral process in ecuador. In ICETM 2019, 2019.
Tso, Raylin, 2019. Zi-Yuan Liu, and Jen-Ho Hsiao. Distributed e-voting and e-bidding systems based on smart contract. Electronics 8, 422.
Md Ashraf Uddin. Lecture note on introduction to blockchain technology. 2021.
Md Ashraf Uddin, Andrew Stranieri, Iqbal Gondal, and Venki Balasubramanian. A patient agent to manage blockchains for remote patient monitoring. 10 2018.
Uddin, M.A., Stranieri, A., Gondal, I., Balasubramanian, V., 2019. A decentralized patient agent controlled blockchain for remote patient monitoring. In: 2019 International Conference on Wireless and Mobile Computing, Networking and Communications (WiMob), pp. 1–8.
Mohammed Nasir Uddin, Sadman Ahmmed, Imtiaz Ahmed Riton, and Linta Islam. An blockchain-based e-voting system applying time lock encryption. In 2021 International Conference on Intelligent Technologies (CONIT), pages 1–6, 2021.
Veldre, Aaron, Andrews, Sally, 2014. Lexical quality and eye movements: Individual differences in the perceptual span of skilled adult readers. The Quarterly Journal of Experimental Psychology 67, 703–727.
Alex White-Gomez. What are layer 2 solutions and why are they important? https://www.one37pm.com/nft/tech/what-are-layer-2-solutions-and-why-are-they-important#::text=Layer%202%20is%20a%20term, speed)%20and%20reduce%20gas%20fees.
Wikipedia. Demographics of bangladesh. https://en.wikipedia.org/wiki/Demographics of Bangladesh.
Wohrer, Maximilian, Zdun, Uwe, 2018. Smart contracts: security patterns in the ethereum ecosystem and solidity. In: 2018 International Workshop on Blockchain Oriented Software Engineering (IWBOSE). IEEE, pp. 2–8.
J. Xin, Pei Huang, L. Chen, Xin Lai, X. Zhang, W. Li, and Yongcan Wang. Watercarver: Anonymous confidential blockchain system based on account model. IACR Cryptol. ePrint Arch., 2019: 1265, 2019.
Yi, Haibo, 2019. Securing e-voting based on blockchain in p2p network. EURASIP Journal on Wireless Communications and Networking 1–9, 2019.
Zaghloul, Ehab, Li, Tongtong, Ren, Jian, 2021. d-bame: Distributed blockchain-based anonymous mobile electronic voting. IEEE Internet of Things Journal.
Zhang, W., Yuan, Y., Hu, Y., Huang, S., Cao, S., Chopra, A., Huang, S., 2018. A privacy-preserving voting protocol on blockchain. In: 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), pp. 401–408.
Qixuan Zhang, Bowen Xu, Haotian Jing, and Zeyu Zheng. Ques-chain: an ethereum based e-voting system. ArXiv, abs/1905.05041, 2019.