International Journal of Environmental Sciences
ISSN: 2229-7359
Vol. 11 No. 13s,2025
https://theaspd.com/index.php

Electwithme: A Secure-Balloting, Coercion-Resistant, Scalable, And Optimized E-Voting System Using Blockchain Technology

Urmila Devi[1], **Shweta Bansal**[2]

[1]*PhD Scholar, Computer Science and Engineering Department, K.R. Mangalam University, Gurugram, Haryana, India, urmilabibyan@gmail.com*

[2]*Associate Professor, Computer Science and Engineering Department, K.R. Mangalam University, Gurugram, Haryana, India, shweta.bansal@krmangalam.edu.in*

Abstract. *In every democracy, voting is an essential and fundamental activity. The wrong candidate may be chosen to lead the nation if this process is botched or doesn't go as planned. Traditional voting systems have many loopholes where voting turnout becomes very low. For several reasons, individuals prefer not to wait in extensive lines on election day or to have to travel through hilly or terrorist-prone areas. The blockchain-based online voting system can significantly address all voting challenges to make the election process more comfortable and secure, which needs to be considered in designing a robust system. This paper presents a novel approach to building a safe and robust e-voting system using the two-layered EVM machine called zkEVM (Zero Knowledge Ethereum Virtual Machine) and a newly designed and optimized smart contract. The proposed architecture is made to reduce the total gas cost of the smart contract while offering security, coercion resistance, reliability, anonymity, authenticity with OTP validation, and receipt-freeness. The suggested smart contract gas cost is lowered by up to 11% compared to earlier works. The system smart contract is also analyzed with different blockchain testnets and provides a graphical representation. Nearly all of the e-voting requirements are met by the suggested system, and a comparative study is also given in the latter part of the paper.*

Keywords: *E-voting, Blockchain, Smart Contract, Ballot, Ethereum, Coercion Resistant, Sharding, Zero Knowledge Proofs.*

1. INTRODUCTION

In a democracy, the people can voice their opinions through the election system, which determines the leaders and the future direction of their society. Even after years of evaluation, voter turnout has not increased with today's voting systems. One possible reason for the low voter participation may be the lack of an available and easy-to-use internet voting technology. The traditional ballot method, which involves bringing a ballot paper to the polls, and digital voting via the electronic voting system (EVS) are currently the two most popular voting methods. Blockchain-based electronic voting platforms are an excellent way to offer a reliable system that will boost the voting process's throughput. In Fig. 1 the traditional voting approach shows where there are methods to vote in person or through mail-in adverse conditions.

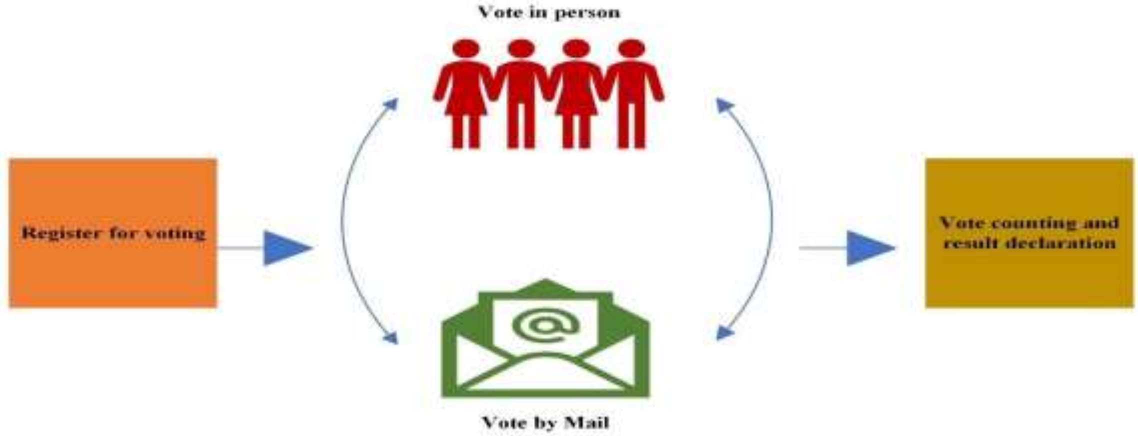


Fig. 1 Traditional Voting System

Electronic voting often appears as an approach to increase public trust in the electoral process and make elections more effective. The E-voting process can be mainly divided into three categories–

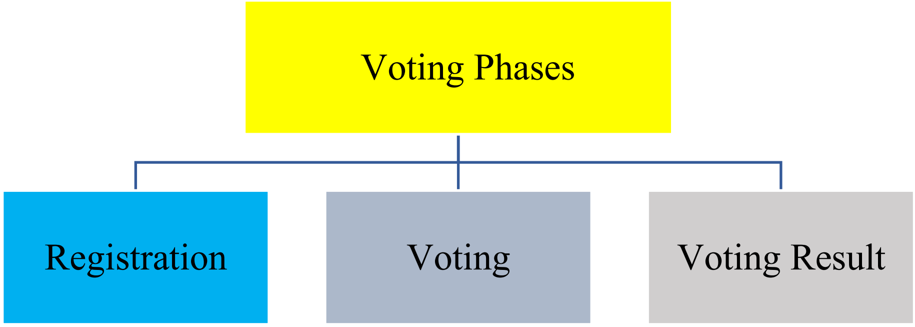


Fig. 2 Phases in the E-voting process

In the registration Phase, candidates and voters for the Elections will be registered with valid ID proofs. The voting phase describes the voting process for the designated places in the elections. In the last phase, the voting results will be declared based on the cast votes.

In this paper, we have proposed a secure and optimized smart contract-based e-voting architecture. Based on the literature survey, the problem with the existing work and the research gaps are found. Many more e-voting requirements are not in their consideration. Overall, the research contribution can be summarized as given below:

- A new voting blockchain-based architecture is being proposed.
- A secure and optimized smart contract is designed along with the sharding concept.
- Gas cost for the proposed smart contract is optimized by using the essential variables and functions in terms of memory usage.
- Deployment Gas cost for the smart contract is being tested with multiple blockchain testnets like - Sepolia testnet, Polygon-based zkEVM (Zero Knowledge Ethereum Virtual Machine), and on local blockchain named Ganache.
- In the proposed system, a verified voter can only cast the vote once. Once it is cast vote cannot be changed at any cost.
- Voter authentication is done based on the OTP Validation with Aadhar ID verification.
- The vote can be verified by the legitimate voter whether their vote is being counted or not for the elections.
- Anonymity of the voter is maintained by using the OTP validation and region code which will be provided to the voter at the time of registration.
- The solution is also provided for the tie-up of the voting result.
- Almost all e-voting requirements are met with the proposed system like - security, anonymity, integrity, coercion resistance, authentication, etc.
- The gas cost for the suggested smart contract is reduced by up to 11% as compared to the previous work [11].
- A graphical representation is shown for the e-voting requirements and deployment gas between the different blockchain test environments.

2. PROBLEM STATEMENT

To select the best candidate for any democratic nation, elections are an extremely significant and vital occurrence. The wrong person can be chosen if this process is rigged or fails. They should feel safe and transparent in this process to freely express their opinions. However, there are numerous locations in India, such as remote, hilly, or terrorist-prone areas, where voters do not travel to cast their ballots. Voter turnout declines, which may result in the wrong candidate being chosen. In Traditional Voting, the paper ballots were counted and the election results were announced. Due to a lack of transparency, there were numerous gaps in that process. Because of their hectic schedules or for other reasons, everyone wants everything these days in the palm of their hands. ordering takeout, shopping, or even selecting a life mate via the internet. So why are we unable to cast our votes online? One excellent way to handle all the problems is to implement an online voting system. Every security and functional concern can be resolved by the blockchain-based electronic voting system.

3. REVIEW OF RELATED LITERATURE

The papers studied from the range of the past 10 years from existing databases like – Google Scholar, Web of Science, Scopus and SCI Indexed Journal, and Conferences. But here are a few latest five-year reviews of related literature that are closely related to my problem statement.

Table (1): Review of Related Literature

Reference Papers	Year	Review of related literature
[1]	2014	The authors studied the secure online voting system and focused on the security and feasibility of the voting system. They proposed a voting system by using the twofold system which consists of SMS-based voting and Website-based voting. However, there are a few limitations or research gaps in the proposed model as SMS-based voting is cell phone-based which is very much prone to any malware.
[2]	2022	The authors studied blockchain-based system papers from 2010 to 2021 and did a comprehensive survey based on the phase of the e-voting system. Authors have given detailed tabular data based on the Voter Authentication, encryption, and hashing techniques, which papers are resistant to attacks, and a detailed tabular view of paper based on the security properties of the online voting system.
[3]	2021	The authors studied online voting systems and proposed an e-voting system named" EVO". They used the Ethereum-based blockchain using the smart contract using the SMS gateway for voter authentication. They proposed only a single person can vote from a valid Mobile no. There is a limitation in the proposed scheme as a member can be registered with a different mobile no and can try to vote again and a smart contract can also be optimized.
[4]	2020	The authors studied e-voting systems and provided a web-based e-voting system using a smart contract on the Ethereum blockchain. They suggested providing transparency to the system. The proposed system can be improved by providing more user interaction pages. The authors also did not discuss and compare the proposed model with the existing models.
[5]	2020	The authors) studied the e-voting process and proposed a model based on the private and public blockchain. They also mentioned intrusion detection to detect the DDOS (Distributed Denial of Service) attack in their proposed model but there are no countermeasures proposed to tackle the attack. The architecture needs more improvements in terms of security measures.
[6]	2021	The authors have studied online voting systems and proposed a system based on the OTP (One Time Authentication Password) and ODP (One Day Password Verification) and verified by a fingerprint hardware machine. They suggested the proposed model can be used in Government and non-government organizations. However, there is a limitation as they did not discuss the online voting requirements in terms of security and functionality.
[7]	2023	The authors proposed a privacy-preserving e-voting system using the Score-based voting

		process using blockchain technology with the Zero-knowledge proofs technique. In this scheme, there is an issue in maintaining the security of the ballots. They just focused on the privacy of the voters where other requirements needed to be taken care of.
[8]	2022	The authors studied e-voting systems and proposed a system using blockchain technology and ensured to provide a transparent system. They did not focus on the coercion and all other requirements of the voting system which needs to be taken care of in further research.
[9]	2022	The authors studied the online voting process in India and proposed a model for a two-phase authentication process using the OTP (One Time Password). The voter will get the OTP on their mobile phone to cast the vote. As per the model, voters can only vote if they have mobile phones. In this approach, there are security concerns as mobile phones can be hacked by illegitimate nodes.
[10]	2016	In this book chapter, the author has discussed possible methods for authentication like knowledge-based, token-based, and biometric-based authentication. In this paper, they focused on the authentication mechanism's advantages and disadvantages. They also suggested the online voting process can be improved if more secure authentication methods.
[11]	2022	The authors studied the online voting system and proposed a new model for the voting process. They also discussed the security measures of the system. They suggested and compared the Gas cost for the smart contract with the existing architectures. But for future work gas cost has to be reduced more along with the functionality given in smart contracts.
[12]	2022	The authors studied the online voting process and provided a solution using the RSA Key Encapsulation method to encrypt and decrypt the voter's credentials and the ballots. They suggested that the blockchain can be used to avoid possible attacks on ballots.
[13]	2022	The authors studied online voting systems and gave a review of all the possible solutions that are based on the blockchain.
[14]	2020	The authors studied the online voting process and tried to understand the potential risks and challenges in the process by using the ATAM (Architecture trade-off analysis method). They also suggested using the blockchain to prevent security attacks and promote transparency.
[15]	2020	The authors proposed a new voting model based on the blockchain and used the homomorphic technique to provide encryption to the system. They also suggested a solution to verify the proofs of the ballots. But the provided system is very complex which will cost so for better system implementation gas cost should be kept in consideration.
[16]	2020	The authors studied an online voting system based on blockchain and provided a hybrid architecture to run a smart contract. They also discussed the evaluation parameters based on the Gas cost, average time, and transactions per block.
[17]	2021	The authors studied and proposed verify-your-vote as an online voting system using cryptographic techniques like Elliptic curve cryptography and blockchain as public bulletin boards. But in their proposed model coercion resistance is not there which can be considered as a future scope for the researchers.
[18]	2019	The authors studied an online system and tried to provide a distributed e-voting system and e-bidding system for the online process. They used Python to implement the cryptographic techniques. However, they did not focus more on the security and coercion of the ballots. They suggested if blockchain can be used with the cryptographic technique then a robust system can be made.
[19]	2022	The authors used blockchain technology to propose an online voting system. They developed a smart contract-based architecture with the voter's authentication and

		security measures. But in their system, they showed access to the Government database by the third entity in the system which can cause an issue in terms of security.
[20]	2022	(Umar et al., 2022) proposed an online voting system using the Paillier cryptosystem to provide the voter's privacy and tried to resolve security-related issues like the integrity of the system. They suggested using the blockchain for a better online voting process.
[21]	2020	The authors studied and proposed an online voting system by using the Ethereum blockchain along with the Metamask wallet concept. In this paper, they showed the comparison between the gas cost for the applicable functions of the voting process. They suggested gas costs should be minimized for the optimization of the smart contracts.
[22]	2020	In this paper, authors have discussed and proposed an online voting system using the hybrid consensus model which is a combination of the Proof of Credibility and Proof of Stake that work mutually to address the problems of secure e-voting systems.
[23]	2022	The authors have done a Systematic Literature review based on the blockchain-based voting system. They also provide a comparison of the different approaches used in previous literature.
[24]	2021	The authors have studied and proposed blockchain-based e-voting systems. They mentioned the hardware and software requirements of the system. But they did not provide the gas cost evaluation which has to be done for a better understanding of the system evaluation.
[25]	2020	The authors studied and proposed blockchain-based e-voting systems and used the .Net framework to implement the system. However, they did not mention any kind of blockchain implementation in terms of gas cost. They did not discuss e-voting system requirements.
[26]	2020	The authors studied the blockchain thoroughly and gave an analysis of computational energy in blockchain-based applications. However, they did not talk much about the security of the e-voting system.
[27]	2020	The authors presented an e-voting system based on blockchain technology that enables users to vote online. They made a front-end application connected with Metamask to make transactions. However, they did not focus on Gas cost optimization and other security requirements.
[28]	2023	An extensive survey is being done including blockchain terminologies and cryptographic techniques. They suggested blockchain will be a great solution for the e-voting process.
[29]	2021	The authors analyzed existing blockchain-based e-voting systems and proposed a three-layered architecture that can AVL Chain for an e-voting system. They focused on cryptography but many other security requirements are discussed in their architecture.
[30]	2022	In this paper, the author discussed the complete details related to Ethereum Network. Blockchain technology is being used with the Ethereum network to execute any type of decentralization.
[31]	2020	The author has done an empirical analysis based on online voting requirements and proposed a model to secure voter privacy using the IPFS decentralized file-sharing system. However, this paper did not talk about other security and functional requirements.

4. PROPOSED METHODOLOGY

To propose a secure and efficient e-voting system, we have used blockchain technology. A smart contract is being designed with the required voting operations.

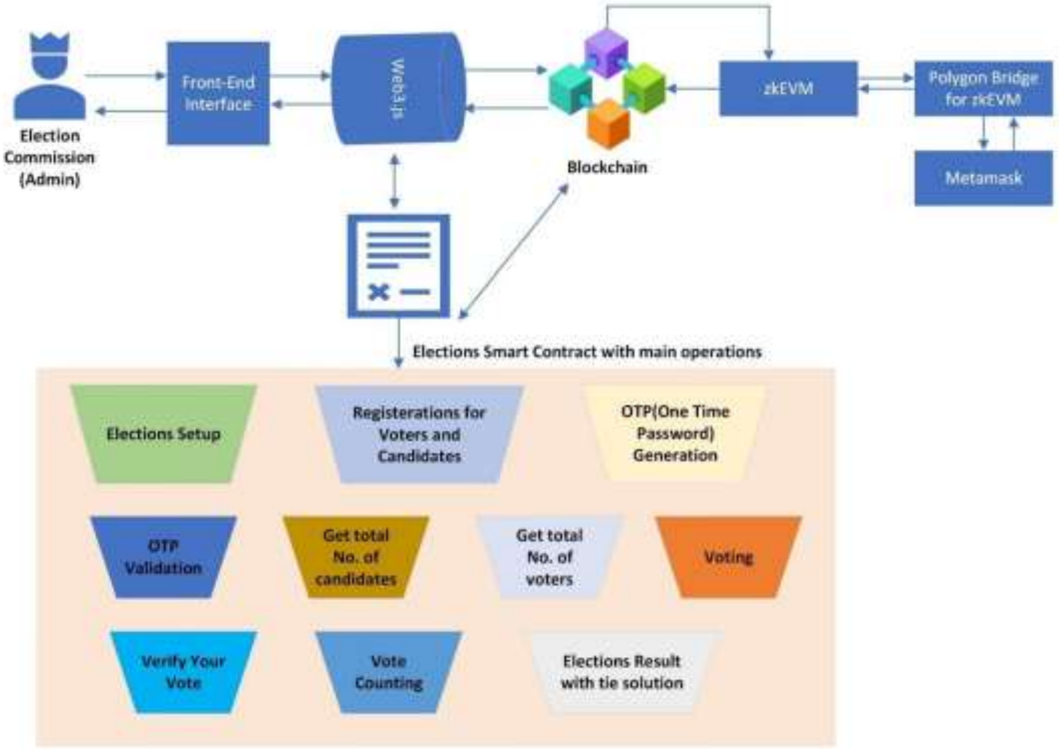

Election Commission (Admin)
Front-End Interface
Web3.js
Blockchain
zkEVM
Polygon Bridge for zkEVM
Metamask
Elections Smart Contract with main operations
Elections Setup
Registerations for Voters and Candidates
OTP(One Time Password) Generation
OTP Validation
Get total No. of candidates
Get total No. of voters
Voting
Verify Your Vote
Vote Counting
Elections Result with tie solution

Fig. 3 Proposed Solution Architecture

As shown in Fig. 3 the proposed architecture can be described as - the Election Commission(admin) will be the admin of the electoral process to keep a check on the overall voting process. The admin can only interact with the designed system with the provided front-end. There will be some gas cost for any transaction that is being done on any blockchain-based application. So, in the given architecture, the gas cost is being reduced by identifying the latest version of the EVM (Ethereum Virtual Machine) named "zkEVM (Zero Knowledge Ethereum Virtual Machine)". The zkEVM will be connected to the blockchain wallet named Metamask to add the blockchain ethers to support the transaction on the blockchain environment. All the instructions will be written in the smart contract. In the proposed smart contract, there are almost eleven voting operations that are being designed and implemented to provide a robust voting system. However, we can say the architecture of the proposed methodology is the main three entities – Election Commission, Voters, and Candidates.

Sharding – Sharding is a process where a main blockchain can be divided into multiple off-blockchains to improve the scalability of the system. In the proposed solution, a sharding technique is being suggested where the main blockchain can be divided into two shards as shown in Fig.4.

Shard1 can be used for the registration of voters and candidates. Shard 2 can be used to store votes. So that at the time of result, the declaration main blockchain can fetch results from shard 2 and publish them on the election Bulletin board.

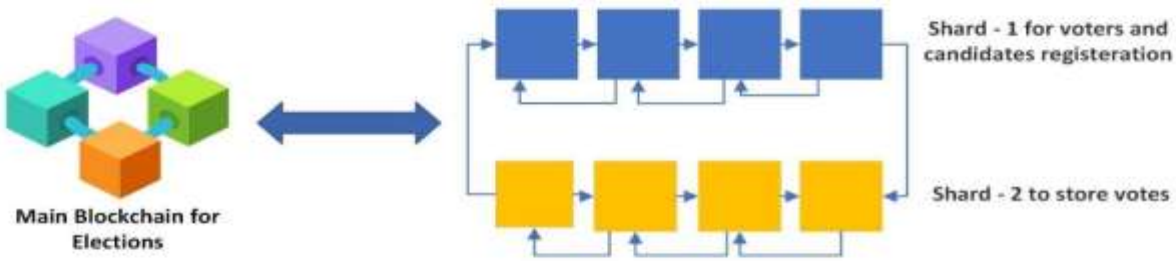

Main Blockchain for Elections
Shard - 1 for voters and candidates registeration
Shard - 2 to store votes

Fig. 4 Proposed Sharding Process for Proposed Solution

Smart Contract Execution with zkEVM

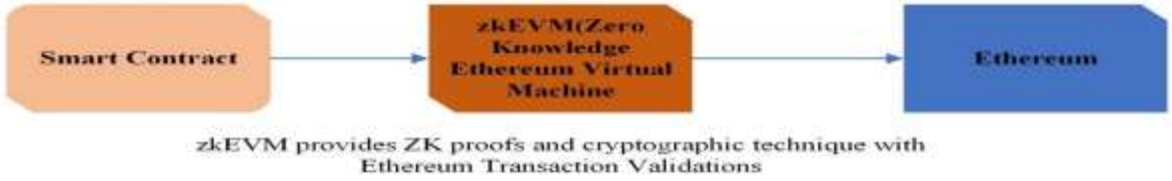

Smart Contract
zkEVM(Zero Knowledge Ethereum Virtual Machine
Ethereum
zkEVM provides ZK proofs and cryptographic technique with Ethereum Transaction Validations

Fig. 5 Smart Contract Execution with zkEVM

This Fig. 5 shows the working of a smart contract with zkEVM. The zkEVM works with EVM and then provides the cryptographic solution for the deployed contract. In Fig. 6 below, elections will be initiated by the Election Commission for a specific Time slot. Registrations for the voters and candidates will be done with some set of validations. Once registration is done the voting phase will start where a validated voter will cast the vote. Three main conditions will be checked - Are elections still going on? Is the voter and candidate region code the same? Is it already voted? Is One Time Password (OTP) valid? The vote-casting will be completed once all validations are passed. Once the Elections are over the result will be declared.

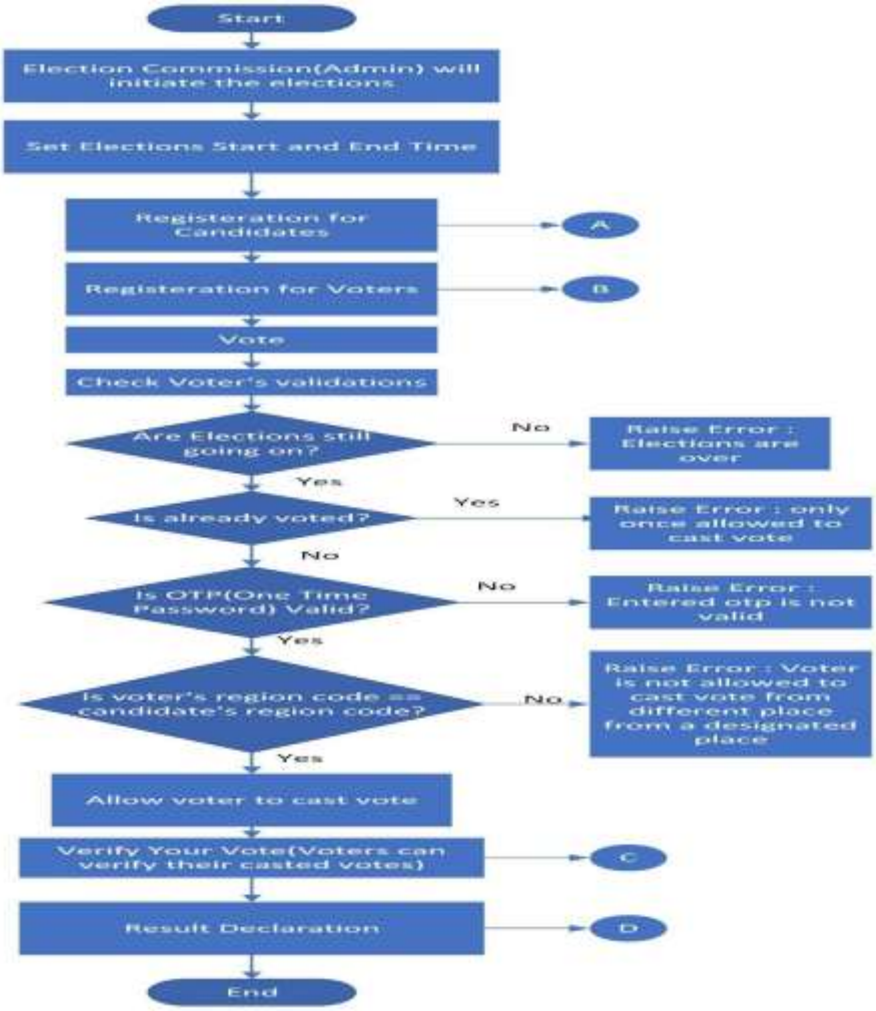

Start
Election Commission(Admin) will initiate the elections
Set Elections Start and End Time
Registeration for Candidates
A
Registeration for Voters
B
Vote
Check Voter's validations
Are Elections still going on?
No
Raise Error : Elections are over
Yes
Is already voted?
Yes
Raise Error : only once allowed to cast vote
No
Is OTP(One Time Password) Valid?
No
Raise Error : Entered otp is not valid
Yes
Is voter's region code == candidate's region code?
No
Raise Error : Voter is not allowed to cast vote from different place from a designated place
Yes
Allow voter to cast vote
Verify Your Vote(Voters can verify their casted votes)
C
Result Declaration
D
End

Fig. 6 Flow chart for the proposed solution

5. PROPOSED SOLUTION

A smart contract is being designed and implemented with multiple voting operations. The smart contract is connected with the Blockchain environment which will work as a system backend. A Web3.js library is being used to connect the smart contract with the front end. A Metamask wallet can be connected to the smart contract to approve the transaction on the blockchain environment. Each person on the system has to accomplish several steps. The initialization, registration, and voting are the three primary phases that everyone must go through. At last, the voting result phase is required to publish the voting results. Each phase is explained in detail below:

5.1 Initialization Phase

The proposed smart contract is written in the solidity programming language. The contract is developed and tested using the Remix IDE online with the different blockchain testnets. In this phase to deploy the smart election start date and end date are needed.

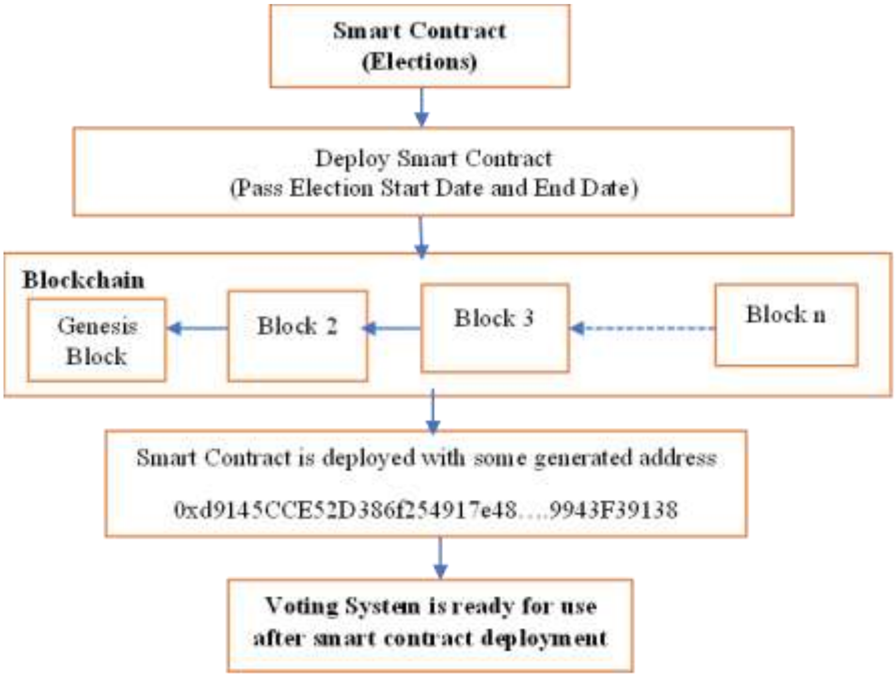

Smart Contract (Elections)
Deploy Smart Contract
(Pass Election Start Date and End Date)
Blockchain
Genesis Block
Block 2
Block 3
Block n
Smart Contract is deployed with some generated address
0xd9145CCE52D386f254917e48….9943F39138
Voting System is ready for use after smart contract deployment

Fig. 7 Deployment of smart contract

After the successful deployment of the smart contract, the system will be ready for use.

5.2 Registration Phase

The registration process begins with the addition of required details. This process differs for the candidate and voters in terms of mandatory details records. At the time of candidate registration, the candidate's name, Aadhar ID, party name, and region code are required. The region code will be used to identify the place of the candidate electoral places. For voter registration, voter account address (blockchain node address), Aadhar ID, age, isVoterAlive, and the region code are needed. An OTP is also being generated against that voter address which will be used at the time of voting. If the valid OTP is not provided at the time of vote casting, then that system will raise an error and not allow that person to vote.

5.3 Voting Phase

In this phase, the legitimate registered voter will be allowed to vote. During the voting phase, the voter will provide the OTP, and vote for the registered candidate. Once the vote is recorded then it cannot be changed in the systems. In the proposed system a facility is also provided where a voter can verify their vote cast with the correct OTP-based login in the system. A voter can only vote until the elections are alive.

5.4 Voting Result Phase

In this phase, voting results will be announced when the election time is over. The winner's candidate name will be announced with the total number of voters. A voting result tie solution is also provided in the proposed smart contract. As in the traditional voting system, if there is any situation where there is a tie-in between the winning candidates then the winner's name used to be announced based on the lottery system. Based on the same concept, the solution is provided.

6. IMPLEMENTATION

6.1 EVM Component Stack

In the proposed solution, EVM (Ethereum Virtual Machine) is being used to develop, deploy, and test the solidity of the e-voting system. The below Table 2, shows the components stack that will work with the EVM.

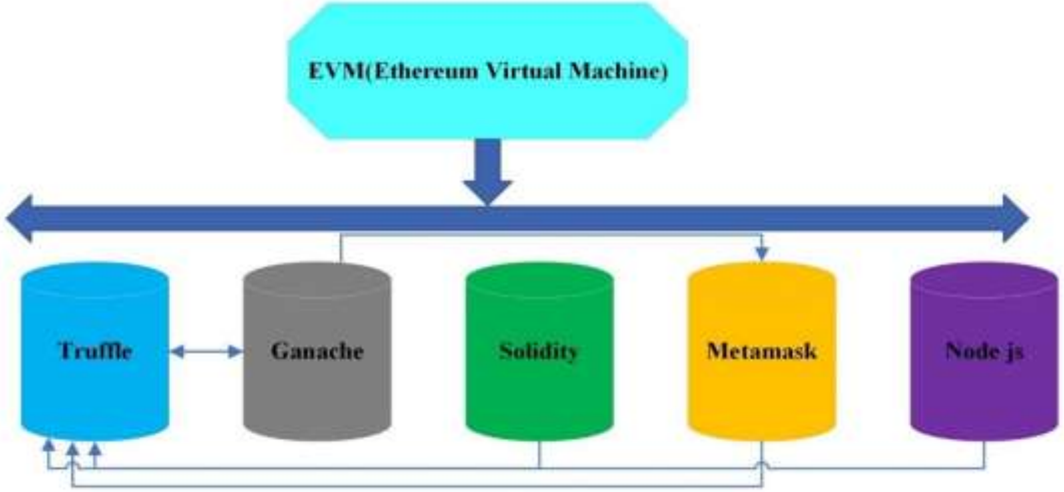


Fig.8 EVM components stack

Table (2): EVM component stack

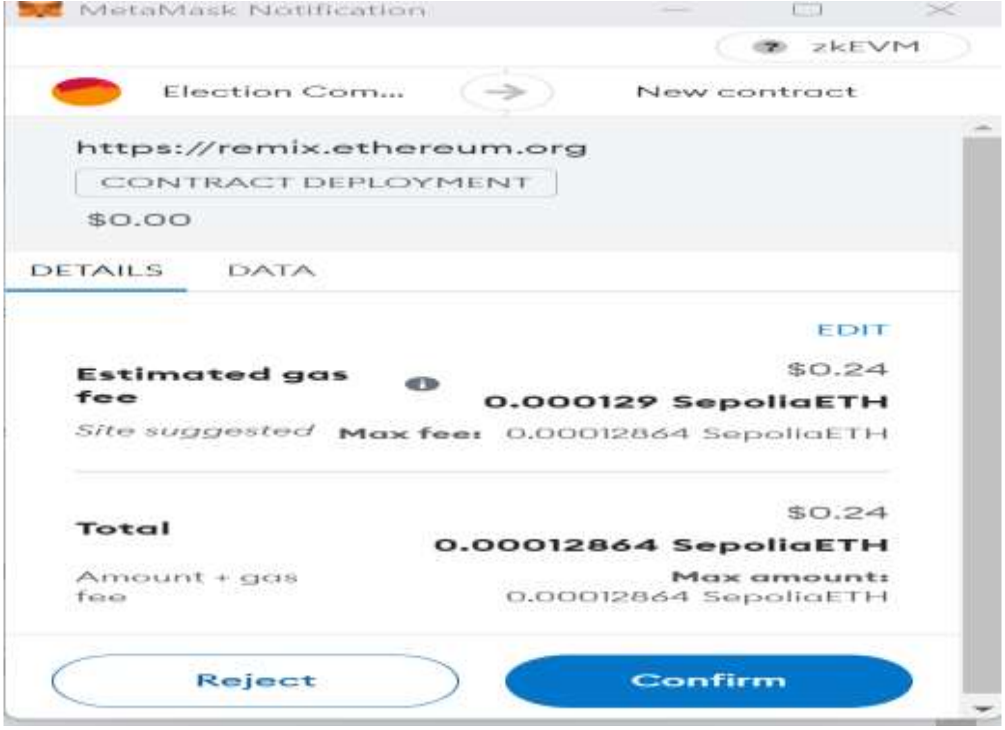
Components	Functions in EVM Stack	Remarks
Truffle	Framework as a development environment	A framework that facilitates the execution of smart contracts.
Ganache [44]	Local Blockchain	It is a local blockchain to run, execute, or test the smart contract executions.
Solidity	Programming Language	It is used to develop decentralized applications in blockchain environments.
Metamask	Ether Wallet	It is like other online wallets. It holds ethers that can be used to make transactions on blockchain-enabled applications.
Node.js/NPM	Server	It provides server-side scripting to run decentralized applications.

6.2 Deployment of proposed smart contract in different blockchain testnet environments for deployment gas difference

The screenshots for the smart contract deployment in different environments are given below to elaborate the process.

6.2.1 zkEVM Testnet – Zero Knowledge Ethereum Virtual Machine

zkEVM is a layer 2 Ethereum virtual machine to provide more security in the environment. It uses zero-knowledge proofs to provide authenticity. In Fig. 9 and Fig. 10 the deployment of the smart contract by using the zkEVM polygon for testing purposes.



https://remix.ethereum.org
CONTRACT DEPLOYMENT
$0.00

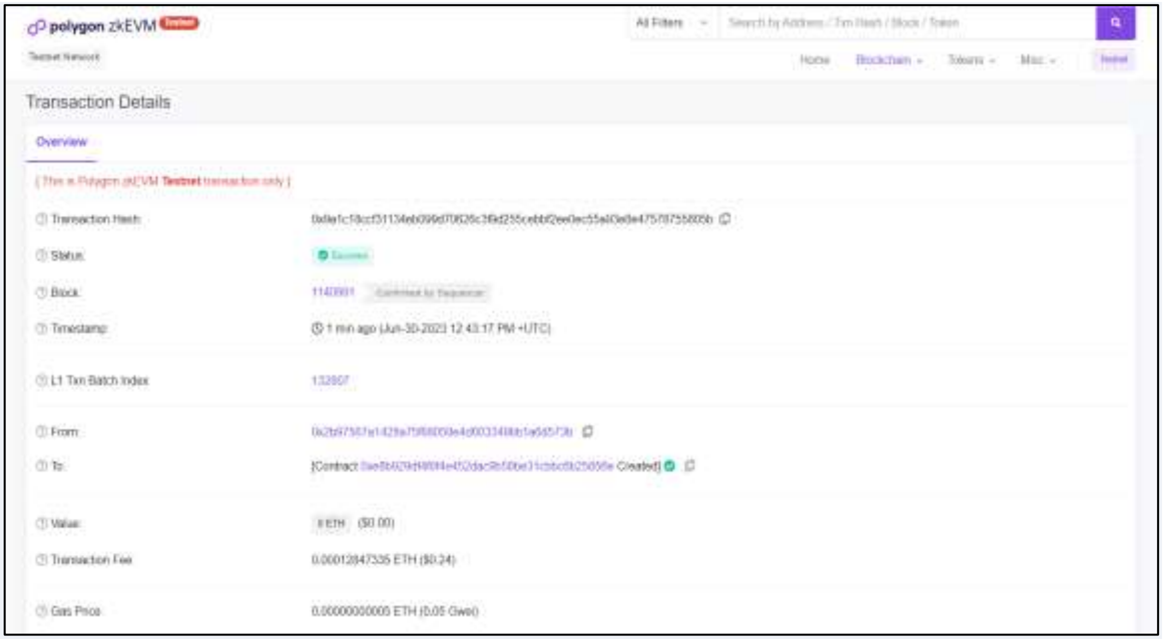
DETAILS DATA

EDIT

Estimated gas fee — $0.24 — 0.000129 SepoliaETH
Site suggested — Max fee: 0.00012864 SepoliaETH

Total — $0.24 — 0.00012864 SepoliaETH
Amount + gas fee — Max amount: 0.00012864 SepoliaETH

Fig. 9 Contract Deployment Confirmation Screen Shot with zkEVM TestNet Metamask Wallet



Transaction Details

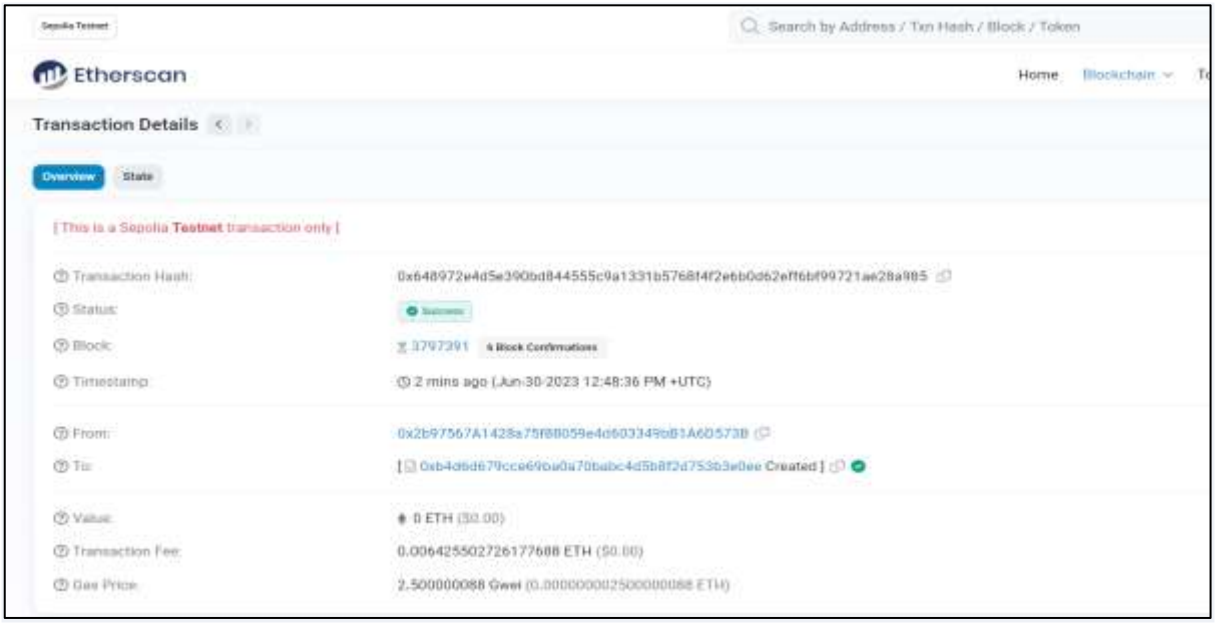
[This is Polygon zkEVM Testnet transaction only]

Transaction Hash:	0x8e1c18ccf31134eb099d70626c3f6d255cebbf2ee0ec55a60e0e47578755805b
Status:	Success
Block:	1140881 Confirmed by Sequencer
Timestamp:	1 min ago (Jun-30-2023 12:43:17 PM +UTC)
L1 Txn Batch Index:	132807
From:	0x2b97587e1429a75f68059e4d003348bb1a5d573b
To:	[Contract 0xe8b629d48084e452dac9b50be31cbbc6b25d56e Created]
Value:	0 ETH ($0.00)
Transaction Fee:	0.00012847335 ETH ($0.24)
Gas Price:	0.00000000005 ETH (0.05 Gwei)

Fig. 10 Screen Shot from Ether Scan for a Contract Deployment on zkEVM

6.2.2 Sepolia Testnet –

Sepolia is a Testnet to test the smart contract deployment with the test ethers which are provided to the developers to test their contracts. In Fig. 11 Contract deployment gas cost is shown which is self-described.



Transaction Details

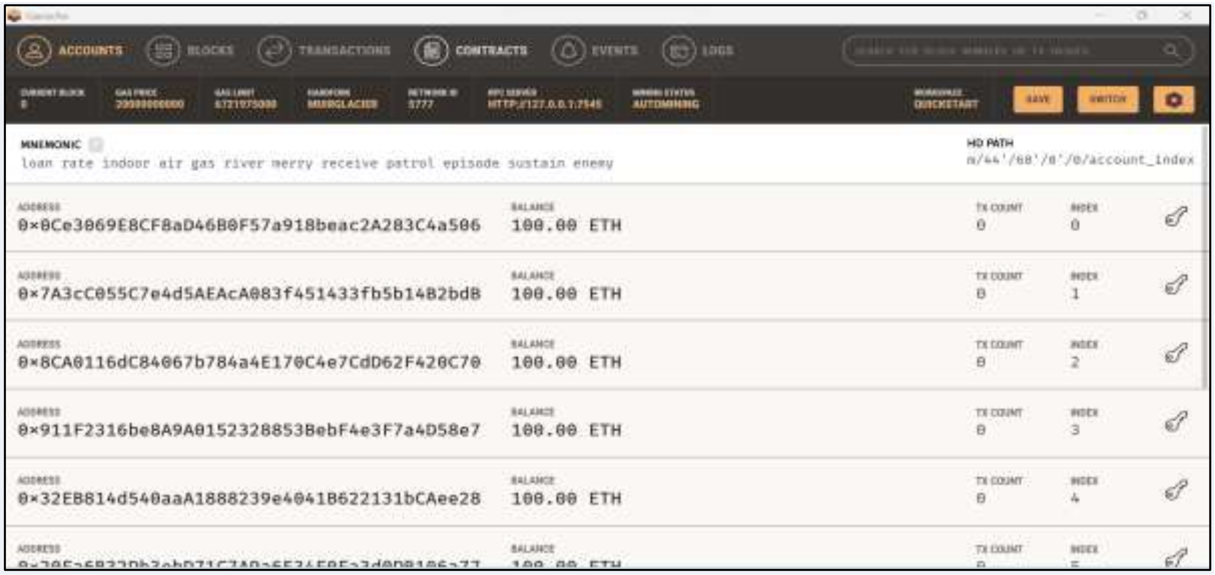
[This is a Sepolia **Testnet** transaction only]

Transaction Hash:	0x648972e4d5e390bd844555c9a1331b5768f4f2ebb0d62eff6bf99721ae28a985
Status:	Success
Block:	3797391 4 Block Confirmations
Timestamp:	2 mins ago (Jun-30-2023 12:48:36 PM +UTC)
From:	0x2b97567A1428a75f88059e4d603349bB1A6D573B
To:	[0xb4d6d679cce69ba0a70babc4d5b8f2d753b3e0ee Created]
Value:	0 ETH ($0.00)
Transaction Fee:	0.006425502726177688 ETH ($0.00)
Gas Price:	2.500000088 Gwei (0.000000002500000088 ETH)

Fig. 11 Transaction on Etherscan for Sepolia TestNet Contract Deployment

6.2.3 Ganache (Local Blockchain) –

Ganache is a local blockchain to executes the smart contracts to build the distributed application. The proposed smart is being deployed on the Ganache. Below figures for deployment and gas costs are shown.



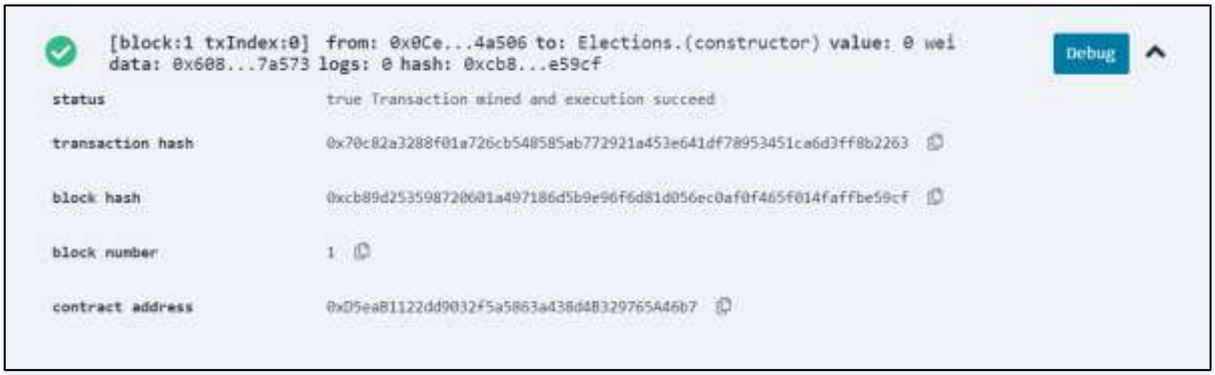
CURRENT BLOCK	GAS PRICE	GAS LIMIT	HARDFORK	NETWORK ID	RPC SERVER	MINING STATUS	WORKSPACE
0	20000000000	6721975000	MUIRGLACIER	5777	HTTP://127.0.0.1:7545	AUTOMINING	QUICKSTART

MNEMONIC
loan rate indoor air gas river merry receive patrol episode sustain enemy

HD PATH
m/44'/60'/0'/0/account_index

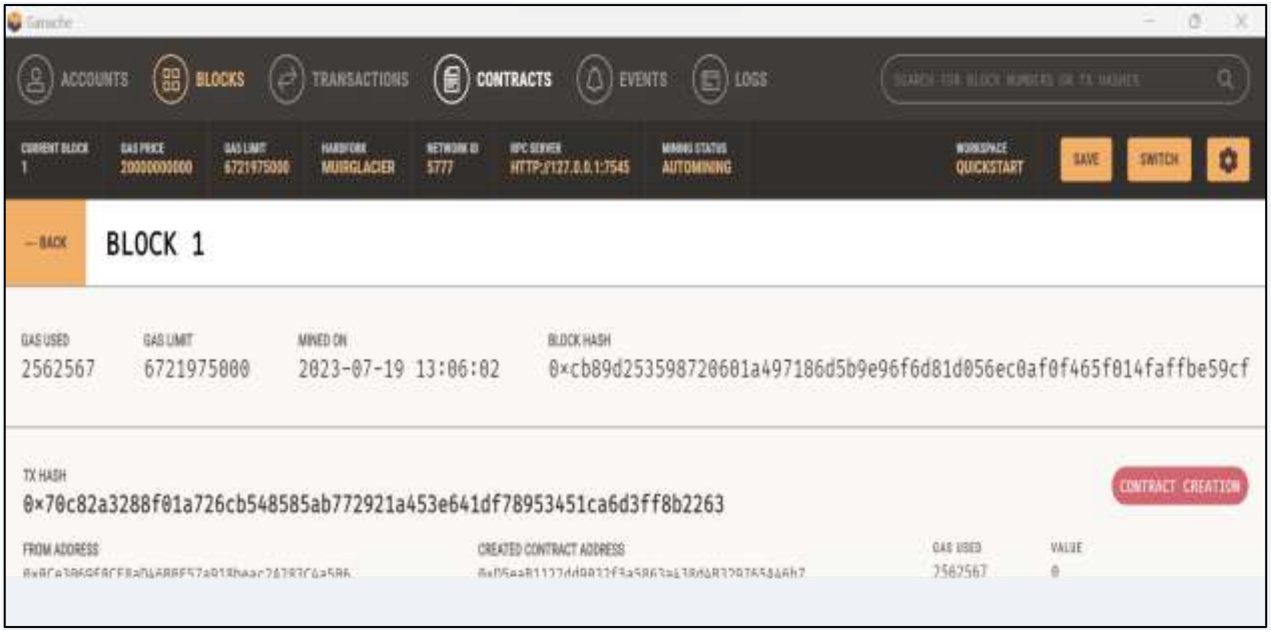
ADDRESS	BALANCE	TX COUNT	INDEX
0×0Ce3069E8CF8aD46B0F57a918beac2A283C4a506	100.00 ETH	0	0
0×7A3cC055C7e4d5AEAcA083f451433fb5b1482bdB	100.00 ETH	0	1
0×8CA0116dC84067b784a4E170C4e7CdD62F420C70	100.00 ETH	0	2
0×911F2316be8A9A0152328853BebF4e3F7a4D58e7	100.00 ETH	0	3
0×32EB814d540aaA1888239e4041B622131bCAee28	100.00 ETH	0	4

Fig. 12 Ganache Blockchain Dashboard



```
[block:1 txIndex:0]  from: 0x0Ce...4a506 to: Elections.(constructor) value: 0 wei
data: 0x608...7a573 logs: 0 hash: 0xcb8...e59cf
status                 true Transaction mined and execution succeed
transaction hash       0x70c82a3288f01a726cb548585ab772921a453e641df78953451ca6d3ff8b2263
block hash             0xcb89d253598720601a497186d5b9e96f6d81d056ec0af0f465f014faffbe59cf
block number           1
contract address       0xD5eaB1122dd9032f5a5863a438d4B329765A46b7
```

Fig. 13 Contact deployed on Ganache Blockchain



```
CURRENT BLOCK  GAS PRICE    GAS LIMIT   HARDFORK     NETWORK ID  RPC SERVER              MINING STATUS   WORKSPACE
1              20000000000  6721975000  MUIRGLACIER  5777        HTTP://127.0.0.1:7545   AUTOMINING      QUICKSTART

BLOCK 1

GAS USED   GAS LIMIT    MINED ON             BLOCK HASH
2562567    6721975000   2023-07-19 13:06:02  0×cb89d253598720601a497186d5b9e96f6d81d056ec0af0f465f014faffbe59cf

TX HASH
0×70c82a3288f01a726cb548585ab772921a453e641df78953451ca6d3ff8b2263

FROM ADDRESS                                   CREATED CONTRACT ADDRESS                       GAS USED   VALUE
0x0Ce3069F8CFE8aD4688F57a018beac24283C4a506    0xD5eaB1122dd9032f5a5863a438d4B329765A46b7    2562567    0
```

Fig. 14 Block1 Contract Deployment Description along with Gas Used

7. RESULT DISCUSSION

7.1 Evaluation of Proposed Solution Based on Gas Cost

7.1.1 Discussion on Gas Cost

Gas Cost [42] is a Computational Cost which is the overall cost required to complete a transaction in the blockchain. A Gas Cost can be divided into two types – Transaction Cost and Execution Cost.

Execution Cost [43] - The execution cost is the cost of performing the computational processes, whereas the transaction cost is the cost of sending the code to the blockchain.

7.1.2 Comparison Table for Deployment Gas Cost with Previous Work

Below is given table that explains the comparisons between the proposed solution with the previous work. As we found many of the papers only implemented 1 to 4 operations for e-voting systems where we have developed a solution with almost 11 operations with less Gas Cost. As shown in the below table our proposed solution with only four operations, Gas cost is very less than the previous work. In that manner we can say, we have optimized the Gas cost at a certain level with the more e-voting system property. In Fig.16 the graphical representation of the same is also shown.

Table (3): Comparison of Deployment Gas Cost with previous work

Contract	Gas used	Provided Property	Operations
Khan et al. (2020) as cited in [11]	726774	Integrity, Security, Verifiability	Vote Casting
Hjálmarsson et al. (2018) as cited in [11]	701538	Integrity, Security, Fairness	Vote Casting, Vote Counting
Jorge Lopes (2019) as cited in [11]	4935530	Anonymity, Privacy, Security, Fairness, Mobility, Uncoercability	Voter Registration, Ballot Creation, Vote Casting, Vote Counting
Dagher et al. (2018) as cited in [11]	3817723	Anonymity, Integrity, Privacy, Security, Fairness, Mobility, Uncoercability	Voter Registration, Ballot Creation, Vote Casting, Vote Counting
Shyda Alvi (2022) as cited in [11]	1928302	Anonymity, Integrity Privacy, Security, Fairness, Mobility, Uncoercability	Voter Registration, Candidate Registration, Vote Casting, Vote Counting
Proposed System (With four operations)	1739552	Anonymity, Integrity Privacy, Security, Fairness, Mobility, Uncoercability, Reliability, Availability, ballot Secrecy, receipt freeness	Voter Registration, Candidate Registration, Vote Casting, Vote Counting
Proposed System (with eleven operations)	2569467	Voter Authenticity, Voter Anonymity, Data Integrity, Privacy, No Vote-Selling/ Coercion Resistance, Reliability, Availability, Ballot secrecy, Receipt-Freeness	Election Setup, Voter Registrations, Candidate registrations, OTP generations for validation, OTP validation, get Total No. of candidates, get total no. of voters, Voting, verify your vote, vote counting, Elections Result with tie Solution

7.1.3 Graphical Representation for Deployment Gas Cost

As we can see the proposed work reduced gas cost by almost 11% from the previous paper for the four operations. Even with the eleven operations the cost is not much increased. This is the main finding of the research.

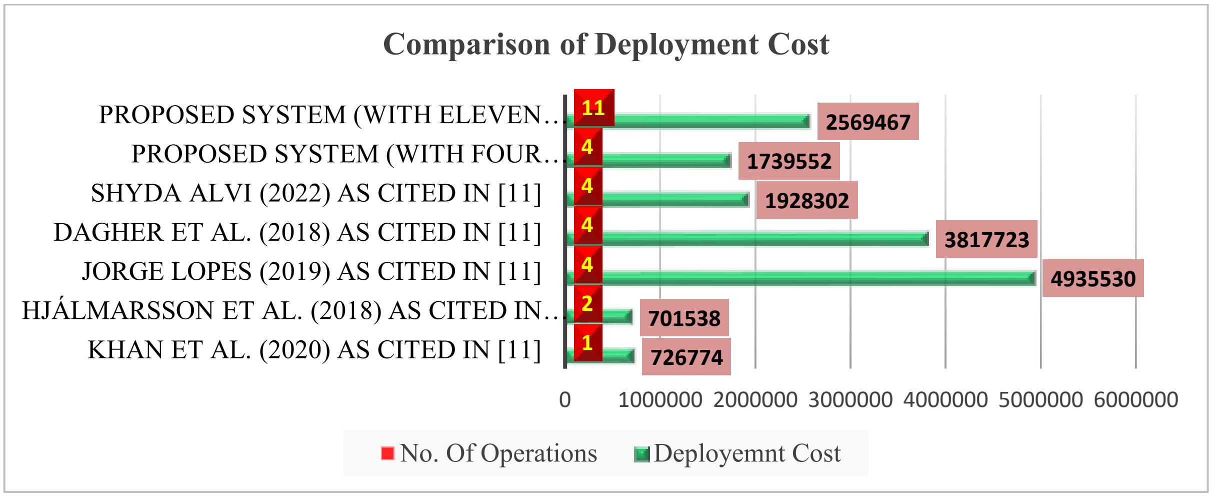


Fig. 15 Comparison of Deployment Cost

7.1.4 Comparison Table for Proposed Solution based on Different Blockchain Deployment Environments

Table (4): Gas Cost for Proposed Solution with Different Environments

S. No	Platform (Deployed on)	Deployment Gas Cost	Ether's cost
1.	Remix IDE with Virtual machine	2570201	0.05 Test Ethers
2.	Sepolia TestNet	2570201	0.006426 SepoliaETH
3	zkEVM TestNet	2569467	0.000129 Sepolia ETH
4	Ganache (Local Blockchain)	2562567	0.05 Test Ethers

The above Table 4. Explained the Deployment Gas cost which is observed at the time of the proposed smart contract deployment. We found zkEVM is much better than other Ethereum Testnets like - Sepolia Testnet.

7.1.5 Graphical Representation for Proposed Solution Based on Different Blockchain Deployment Environments

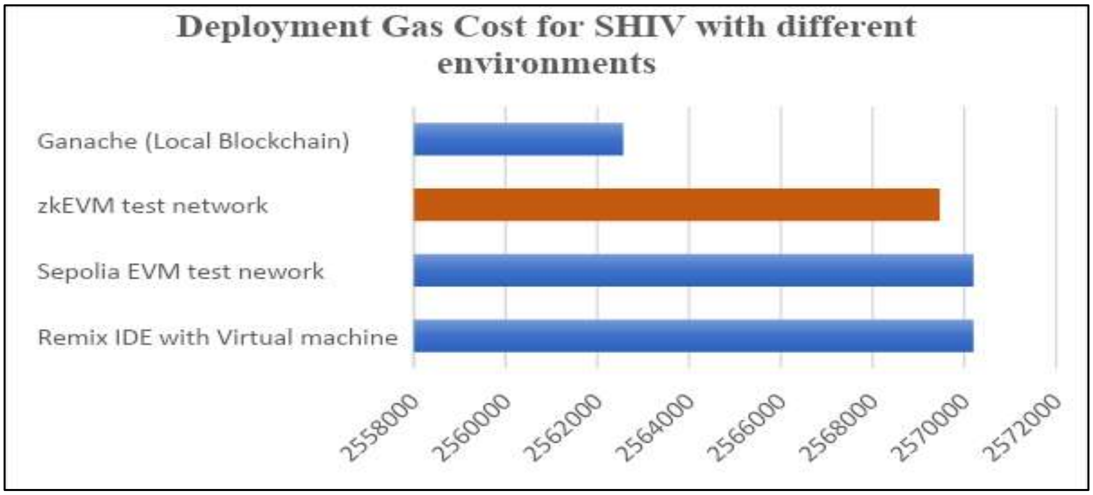


Fig. 16 Graph Representation of Deployment Gas Cost for Proposed Solution with Different Environments

7.2 Result Discussion Based on E-voting Security and Functional Requirements

The proposed solution fulfills the all-online voting requirements, where below is a comparison table shown based on previous work.

Table (5): Comparison table based on requirements

Year	Reference Papers	Voter Authenticity	Voter Anonymity	Data Integrity	Privacy	No Vote-Selling/ Coercion	Reliability	Availability	Ballot secrecy	Receipt-Freeness
2020	[32]	Yes	No	Yes	Yes	No	No	Yes	No	No
2021	[33]	Yes	No	No	Yes	No	No	Yes	No	No
2021	[34]	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	No
2021	[35]	Yes	Yes	Yes	Yes	Yes	Yes	No	No	No
2021	[36]	Yes	Yes	Yes	Yes	Yes	No	Yes	No	No
2021	[37]	Yes	No	Yes	Yes	Yes	Yes	Yes	Yes	No
2021	[38]	Yes	Yes	Yes	Yes	No	Yes	Yes	No	No
2021	[39]	Yes	Yes	Yes	Yes	No	No	No	No	No
2021	[40]	Yes	No	Yes	Yes	No	No	No	Yes	No
2021	[41]	Yes	Yes	Yes	Yes	Yes	No	No	Yes	No
2022	[12]	Yes	No	Yes	Yes	No	No	No	Yes	Yes
2023	Proposed Architecture - (Smart Contract using zkEVM Blockchain environment with Sharding)	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes

7.3 Graph Representation for Requirement Analysis

The proposed system has fulfilled the requirements of an e-voting system through its graphical representation.

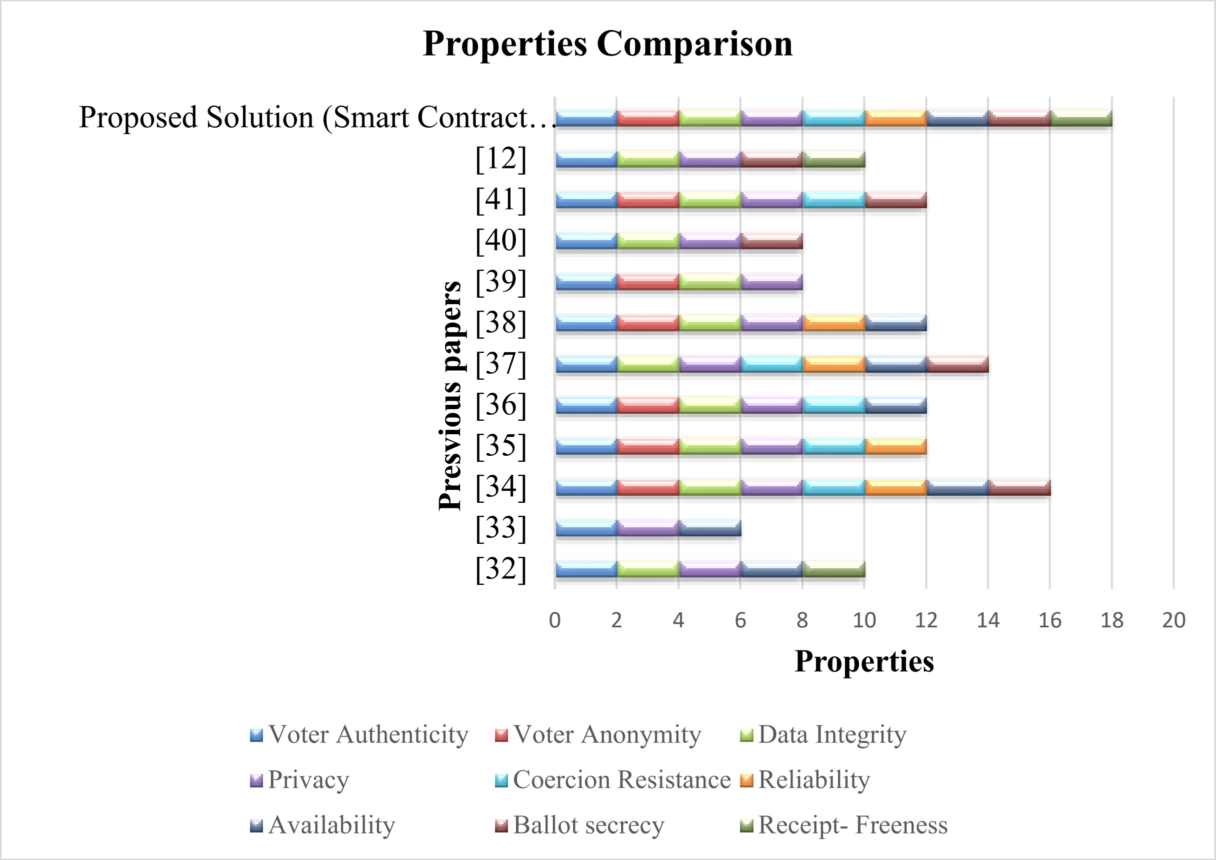


Fig. 17 E-voting properties comparison with previous work

8. CONCLUSION

Blockchain technology is used to implement the e-voting system. Solidity is used to develop and design a smart contract with optimized deployment gas costs. Different Blockchain EVM-based testnet environments, such as Sepolia and zkEVM, are being used to test the smart contract. Because of its inherited features, zkEVM is a highly recommended EVM platform for any kind of decentralized application. Scalability, security, and privacy concerns can be resolved by implementing zkEVM. The proposed solution also suggests sharding as a way to address the scalability problems with blockchain networks. Comparing the proposed smart contract gas cost to the previously discussed work, an 11% reduction is possible. For a clearer understanding of the outcome, graphical representations of each comparison were also provided. In the end, we discovered that the gas cost and e-voting requirements of our suggested system are significantly better. The system can be combined with machine learning methods in the future to improve voting environment predictions.

REFERENCES

[1] Nadaph, A., Katiyar, A., Naidu, T., Bondre, R., & Kumari Goswami, D. (2014). An Analysis of Secure Online Voting System. In International Journal of Innovative Research in Computer Science & Technology (IJIRCST) (Issue 2).
[2] Benabdallah, A., Audras, A., Coudert, L., El Madhoun, N., & Badra, M. (2022). Analysis of Blockchain Solutions for E-Voting: A Systematic Literature Review. IEEE Access, 10(July), 70746–70759. https://doi.org/10.1109/ACCESS.2022.3187688
[3] Dath, D. (2021). *EVO : An E-Voting System using Blockchain*. *9*(13), 174–178.
[4] Susanto, A. (2020). Implementation of Smart Contracts Ethereum Blockchain in Web-Based Electronic Voting (e-voting). *Jurnal Transformatika*, *18*(1), 56. https://doi.org/10.26623/transformatika.v18i1.1779
[5] Cheema, M. A., Ashraf, N., Aftab, A., Qureshi, H. K., Kazim, M., & Azar, A. T. (2020). Machine Learning with Blockchain for Secure E-voting System. *Proceedings - 2020 1st International Conference of Smart Systems and Emerging Technologies, SMART-TECH 2020*, *December 2021*, 177–182. https://doi.org/10.1109/SMART-TECH49988.2020.00050
[6] Othman, A. A. H., Muhammed, E. A. A., Mujahid, H. K. M., Muhammed, H. A. A., & Mosleh, M. A. A. (2021, March 22). Online

Voting System Based on IoT and Ethereum Blockchain. *2021 International Conference of Technology, Science and Administration, ICTSA 2021*. https://doi.org/10.1109/ICTSA52017.2021.9406528

[7] Alshehri, A., Baza, M., Srivastava, G., Rajeh, W., Alrowaily, M., & Almusali, M. (2023). Privacy-Preserving E-Voting System Supporting Score Voting Using Blockchain. *Applied Sciences (Switzerland)*, *13*(2). https://doi.org/10.3390/app13021096

[8] V.Anitha, Orlando, R. S. (2022). Transparent voting system using blockchain. *Measurement: Sensors*.

[9] Rathore, M. (2022). *A Two-Phase Authentication Mechanism for E-voting in*. *10*(4), 26–31.

[10] Abu-Shanab, E., Khasawneh, R., & Alsmadi, I. (2013). Authentication mechanisms for e-voting. *Human-Centered System Design for Electronic Governance*, *January 2016*, 71–86. https://doi.org/10.4018/978-1-4666-3640-8.ch006

[11] Alvi, S. T., Uddin, M. N., Islam, L., & Ahamed, S. (2022). DVTChain: A blockchain-based decentralized mechanism to ensure the security of digital voting system voting system. *Journal of King Saud University - Computer and Information Sciences*, *34*(9), 6855–6871. https://doi.org/10.1016/j.jksuci.2022.06.014

[12] Ahubele, B. O., & Oghenekaro, L. U. (2022). *Secured Electronic Voting System Using RSA Key Encapsulation Mechanism*. *6*(2), 81–87.

[13] Salman, S. A. B., Al-Janabi, S., & Sagheer, A. M. (2022). A Review on E-Voting Based on Blockchain Models. *Iraqi Journal of Science*, *63*(3), 1362–1375. https://doi.org/10.24996/ijs.2022.63.3.38

[14] Daramola, O., & Thebus, D. (2020). Architecture-centric evaluation of blockchain-based smart contract E-voting for national elections. *Informatics*, *7*(2). https://doi.org/10.3390/informatics7020016

[15] Yang, X., Yi, X., Nepal, S., Kelarev, A., & Han, F. (2020). Blockchain voting: Publicly verifiable online voting protocol without trusted tallying authorities. *Future Generation Computer Systems*, *112*, 859–874. https://doi.org/10.1016/j.future.2020.06.051

[16] Ellis Solaiman, Todd Wike, I. S. (2020). Implementation and evaluation of smart contracts using a hybrid on- and off- blockchain architecture. *Concurrency and Computation - 2020*. https://doi.org/10.1002/cpe.5811

[17] Chaieb, M., Yousfi, S., Lafourcade, P., & Robbana, R. (2021). Design and practical implementation of verify-your-vote protocol. *Concurrency and Computation: Practice and Experience*, *33*(1), 1–17. https://doi.org/10.1002/cpe.5813

[18] Tso, R., Liu, Z. Y., & Hsiao, J. H. (2019). Distributed E-voting and E-bidding systems based on smart contract. *Electronics (Switzerland)*, *8*(4), 1–22. https://doi.org/10.3390/electronics8040422

[19] Mohammad Nabiluzzaman Neloy,Md. Abdul Wahab,Sheikh Wasif,Abdulla All Noman,Mustafizur Rahaman,Tahmid Hasan Pranto,A. K. M. Bahalul Haque, R. M. R. (2022). A remote and cost-optimized voting system using blockchain and smart contract. *IET Blockchain*. DOI: 10.1049/blc2.12021

[20] Umar, B. U., Olaniyi, O. M., Olajide, D. O., & Dogo, E. M. (2022). Paillier Cryptosystem Based ChainNode for Secure Electronic Voting. *Frontiers in Blockchain*, *5*(June), 1–11. https://doi.org/10.3389/fbloc.2022.927013

[21] Pramulia, D., & Anggorojati, B. (2020). Implementation and evaluation of blockchain based e-voting system with Ethereum and Metamask. *Proceedings - 2nd International Conference on Informatics, Multimedia, Cyber, and Information System, ICIMCIS 2020*, 18–23. https://doi.org/10.1109/ICIMCIS51567.2020.9354310

[22] Abuidris, Y., Kumar, R., Yang, T., & Onginjo, J. (2021). Secure large-scale E-voting system based on blockchain contract using a hybrid consensus model combined with sharding. *ETRI Journal*, *43*(2), 357–370. https://doi.org/10.4218/etrij.2019-0362

[23] Jafar, U., Ab Aziz, M. J., Shukur, Z., & Hussain, H. A. (2022). A Systematic Literature Review and Meta-Analysis on Scalable Blockchain-Based Electronic Voting Systems. *Sensors*, *22*(19). https://doi.org/10.3390/s22197585

[24] Goyal, M., & Kumar, A. (2021). Sustainable E-Infrastructure for Blockchain-Based Voting System. *Digital Cities Roadmap: IoT-Based Architecture and Sustainable Buildings*, 221–251. https://doi.org/10.1002/9781119792079.ch7

[25] Lahane, A. A., Patel, J., Pathan, T., & Potdar, P. (2020). Blockchain technology based e-voting system. *ITM Web of Conferences*, *32*, 03001. https://doi.org/10.1051/itmconf/20203203001

[26] Jabbar, A., & Dani, S. (2020). Investigating the link between transaction and computational costs in a blockchain environment. *International Journal of Production Research*, *58*(11), 3423–3436. https://doi.org/10.1080/00207543.2020.1754487

[27] Indapwar, A. (2020). E-Voting system using Blockchain technology. *International Journal of Advanced Trends in Computer Science and Engineering*, *9*(3), 2775–2779. https://doi.org/10.30534/ijatcse/2020/45932020

[28] Vladucu, M. V., Dong, Z., Medina, J., & Rojas-Cessa, R. (2023). E-voting Meets Blockchain: A Survey. *IEEE Access*, *11*(March), 23293–23308. https://doi.org/10.1109/ACCESS.2023.3253682

[29] Li, C., Xiao, J., Dai, X., & Jin, H. (2021). AMVchain: authority management mechanism on blockchain-based voting systems. *Peer-to-Peer Networking and Applications*, *14*(5), 2801–2812. https://doi.org/10.1007/s12083-021-01100-x

[30] G. Wood. (2014). Ethereum: a secure decentralised generalised transaction ledger. *Ethereum Project Yellow Paper*, *151*, 1–32.

[31] Grover, A., Apet, K., Fulzele, A., & Agarwal, R. (2020). *Implementing Electronic Voting System Using Block chain*. *7*(6), 1445–1453.

[32] Roopak, T. M., & Sumathi, R. (2020). Electronic Voting based on Virtual ID of Aadhar using Blockchain Technology. *2nd International Conference on Innovative Mechanisms for Industry Applications, ICIMIA 2020 - Conference Proceedings*, *Icimia*, 71–75.

[33] Panja, S., & Roy, B. (2021). A secure end-to-end verifiable e-voting system using blockchain and cloud server. *Journal of Information Security and Applications*, *59*.

[34] Zaghloul, E., Li, T., & Ren, J. (2021). D-BAME: Distributed Blockchain-Based Anonymous Mobile Electronic Voting. *IEEE Internet of Things Journal*, *8*(22), 16585–16597.

[35] Rathore, D., & Ranga, V. (2021). Secure remote E-voting using blockchain. *Proceedings - 5th International Conference on Intelligent Computing and Control Systems, ICICCS 2021*, *Iciccs*, 282–287.

[36] Pooja, S., Raju, L. K., Chhapekar, U., & Chandrakala, C. B. (2021). Face Detection using Deep Learning to ensure a Coercion

Resistant Blockchain-based Electronic Voting. *Engineered Science*, *16*, 341–353.

[37] Taş, R., & Tanriöver, Ö. Ö. (2021). A Manipulation Prevention Model for Blockchain-Based E-Voting Systems. *Security and Communication Networks*, *2021*.

[38] Rathee, G., Iqbal, R., Waqar, O., & Bashir, A. K. (2021). On the Design and Implementation of a Blockchain Enabled E-Voting Application within IoT-Oriented Smart Cities. *IEEE Access*, *9, 34165–34176*.

[39] Prabhakar, E., Kumar, K. N., Karthikeyan, S., Kumar, A. N., & Kavin, P. (2021). Smart Online Voting and Enhanced Deep Learning To Identify Voting Patterns. *International Research Journal of Modernization in Engineering Technology and Science*. *04*, 162–165.

[40] Vemula, S., Kovvur, R. M. R., & Marneni, D. (2021). Secure E-Voting System Implementation Using CryptDB. *SN Computer Science*, *2*(3), 1–6.

[41] Agate, V., De Paola, A., Ferraro, P., Lo Re, G., & Morana, M. (2021). SecureBallot: A secure open source e-Voting system. *Journal of Network and Computer Applications*, *191*(May), 103165.

[42] https://ethereum.org/en/developers/docs/gas/ [online] (accessed 17 September 2023)

[43] Subashini, B., & Hemavathi, D. (2023). Scalable Blockchain Technology for Tracking the Provenance of the Agri-Food. *Computers, Materials and Continua*, *75*(2), 3339–3358. https://doi.org/10.32604/cmc.2023.035074

[44] https://trufflesuite.com/ganache/[online] (accessed 17 September 2023)