e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 7, July 2024

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 7.521

International Journal of Multidisciplinary Research in Science, Engineering and Technology (IJMRSET)

| ISSN: 2582-7219 | www.ijmrset.com | Impact Factor: 7.521| Monthly, Peer Reviewed & Referred Journal|

| Volume 7, Issue 7, July 2024 |

| DOI:10.15680/IJMRSET.2024.0707022 |

Decentralized Voting System Using Blockchain

Miss.G.Sivagami, AP/MCA, Dr T. Geetha MCA.,M.Phil.,Ph.D., Mr. M. Pragatheeswaran MCA

Assistant Professor, Department of Master of Computer Application, Gnanamani College of Technology Namakkal, Tamil Nadu, India

HOD, Department of Master of Computer Application, Gnanamani College of Technology Namakkal, Tamil Nadu, India

PG Student, Department of Master of Computer Application, Gnanamani College of Technology Namakkal, Tamil Nadu, India

ABSTRACT: Election has a very major role in democracy because it is the deciding factor of the future of a country but the major concern is that society doesn’t trust the election system.The major issues that need to be addressed in the current voting system are vote rigging, EVM hacking, polling booth capture and election manipulation. The problems were investigated in the voting systems in this project and attempting to propose the online-voting model that can solve these problems. Using an efficient hashing algorithm technique, block formation and sealing, data collection and result declaration by versatile blockchain method is needed to solve the issue a high-end to end system that ensures security and privacy. This project proposes an online-voting system that uses the Blockchain Netbeans to create a wallet with the credentials of the user. The elector will obtain an authenticated and tamper-proof personal ID. The voter will be getting the chance to vote in the form of token which would be transferred anonymously from voter’s wallet to candidate’s wallet. The fundamental requirements for e-voting schemes and achieves end-to-end verifiability. The paper presents details of the proposed e-voting scheme along with its implementation using Multichain platform. The paper presents in-depth evaluation of the scheme which successfully demonstrates its effectiveness to achieve an end-to-end verifiable e-voting scheme. This paper mostly focuses on a review study of blockchain-based voting systems.

KEYWORDS: Blockchain, Digital voting system, SHA-256 Algorithm.

I. INTRODUCTION

In a democratic regime, voting is crucial to making collective decisions. Unfortunately, although this activity has great significance and value, little effort has been made to improve the way we vote. Paper ballots are still the most used method, although this method is relatively simple, brings many inconveniences, and represents a contradiction to the modern world and its advances.Election has a very major role in democracy because it is the deciding factor of the future of a country but the major concern is that society doesn’t trust the election system. Flawed electoral system is the issue faced by even the world’s largest democracies like India, United States, and Japan. The major issues that need to be addressed in the current voting system are vote rigging, hacking, polling booth capture and election manipulation. The problems were investigated in the voting systems in this project and attempting to propose the online-voting model that can solve these problems.Using an efficient hashing algorithm technique,block formation and sealing ,data collection and result declaration by versatile blockchain method is needed to solve the issue a high-end to end system that ensures security and privacy.

This project proposes an online-voting system that uses the Blockchain NetBeans to create a wallet with the credentials of the user.The elector will obtain an authenticated and tamper-proof personal ID. The voter will be getting the chance to vote in the form of token which would be transferred anonymously from voter’s wallet to candidate’s wallet. The vote can be easted from any geographical are a for voter’s allotted constituency. Blockchain also helps to preserve voters anonymity while still being open to public inspection. The proposed voting system uses more stable, tamper proof blockchain (unchanged from voting modifications either by the voter or by any other third party) and cost-effective.We would also extend the constraints of structure, engineering,design and implementation in our society of the voting mechanism.

II. EXISTING SYSTEM

The traditional paper ballot voting method presents some advantages, mainly the facility of use, even for illiterate people, and the secrecy of the vote, since the ballot is not linked in any way to the voter. Moreover, it has many disadvantages. Another voting method is electronic voting, it can be in the form of a voting machine in a process like paper voting but instead of paper, voters cast their vote via machines found in polling stations. Alternatively, it can be done online; voters cast their votes using their electronic devices. The election results are automatically counted; as a result, electronic voting is faster and more convenient than the traditional voting system. It has numerous issues. There is no guarantee that the voters' vote choice is not leaked or manipulated. Most electronic systems are black boxes and impossible to audit and are also centralized, which puts them at risk of denial of service attacks.Most paper voting systems require a trip to the polling stations.this dependency can be a struggle for people living in remote areas, citizens residing abroad, or people with disabilities.Running a national election is a huge project, and projects at that scale tend to go wrong.this traditional system takes a lot of time and money to implement and manage.the paper ballots are not faulted tolerant, many ballots are not valid and hence not counted, and therefore wasted.

III. LITERATURE SURVEY

BLOCKCHAIN: The concept of blockchain was proposed by Satoshi Nakamoto in 2008. Blockchain is an online ledger that provides decentralized and transparent data sharing. With distributed recordings, all transaction data (stored in nodes) are compressed and added to different blocks. Data of various types are distributed in distinct blocks, enabling verifications to be made without the use of intermediaries. All the nodes then form a blockchain with timestamps. The data stored in each block can be verified simultaneously and become inalterable once entered. The whole process is open to the public, transparent, and secure. The emergence of Ethereum Smart Contracts in 2013 boosted blockchain technology, which became blockchain2.0. As presented in blockchain 1.0 was mainly adopted by Bitcoin to solve problems concerning cryptocurrencies and decentralized payments. Blockchain 2.0 focused on decentralizing the entire market and is employed to transform assets through smart contracts, thereby creating value through the emergence of alternatives to Bitcoin.

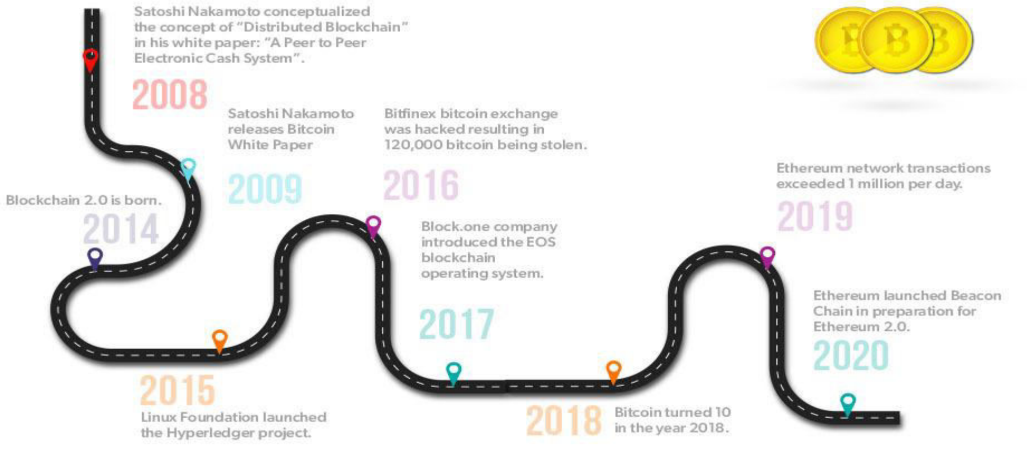

Satoshi Nakamoto conceptualized the concept of "Distributed Blockchain" in his white paper: "A Peer to Peer Electronic Cash System".
2008
Satoshi Nakamoto releases Bitcoin White Paper
2009
Bitfinex bitcoin exchange was hacked resulting in 120,000 bitcoin being stolen.
2016
Ethereum network transactions exceeded 1 million per day.
2019
Blockchain 2.0 is born.
2014
Block.one company introduced the EOS blockchain operating system.
2017
Ethereum launched Beacon Chain in preparation for Ethereum 2.0.
2020
2015
Linux Foundation launched the Hyperledger project.
2018
Bitcoin turned 10 in the year 2018.

Fig 1: History of Blockchain

SMART CONTRACTS: Smart contracts were first proposed by Nick Szabo in the early 990s. He explained that a smart contract enabled computers to execute transaction clauses. As blockchain has become popular, smart contracts have received increased attention. Smart contracts are the main feature of Ethereum, a blockchain platform founded in 2015. A smart contract is "a digital contract that is written in source code and executed by computers, which integrates the tamper-proof mechanism of blockchain". Smart contracts can be created using the Ethereum blockchain. Developers are able, according to their needs, to specify any instruction in smart contracts; develop various types of applications, including those that interact with other contracts; store data; and transfer others. Additionally, smart contracts that are deployed in block-chains are copied to each node to prevent contract tampering.

IV. PROPOSED SYSTEM

It is a symmetric key cryptographic scheme, which encrypts message using public key and retrieve message back from cipher text using corresponding private key.blockchain has probabilistic nature, Every time the cipher text is encrypted using Blockchain system a new cipher text is generated, due to which it is difficult to uniquely identify whether both the cipher text are generated for same message or not.It supports additive properly of homomorphic cryptosystem.We are proposing a system which has greater accessibility as it is an web based application and possess greater security as authentication, authorization and verification. In this system the voter/user has to first register themselves using a registration form available within the web based application and once the registration form is being submitted, an entry is being made in the centralized database. After the registration the user can login to the application and be a part of the polling process. The user with its valid credentials can login to the system and verify them by entering the one-time-password which is valid for a limited period of time. Once the user is logged into their respective account the dashboard contains all the information which is retrieved from the centralized database.After the user logs into the account the user is being authenticated using fingerprint. Each account is provided with a single token which he will use to cast a vote , casting of vote will take place by transferring the token from the respective user account to the candidate's wallet. A web application is being developed to measure the majority of votes which has the details about the total number of voters, the number of votes cast and the percentage of votes cast. Only one vote can be casted from one account and once a vote is being casted from an account the account is disabled from current voting process.

BLOCKCHAIN IN A DATABASE

Blockchain is a decentralized,distributed, public ledger. Blockchain is of three different types, i.e. public, private, and consortium blockchain.This is proofed by the complex mathematical functions. This research uses public blockchain.Blockchain basically consists of a chain of blocks where a block is the primary component of the blockchain. A block is the header and the body, the block body contains the transactions that are being written to the network.The block header contains the block information which includes previous hash, nonce value and difficulty, block time stamp and transactions. This would make it easier to secure and thus increase confidence in the system. The blockchain is private and access-protected. The system benefits from the known advantages of a blockchain (forgery protection, immutability, etc.) and at the same time avoids the disadvantages of completely public blockchain infrastructures (e.g., increased power consumption due to methods for building trust).

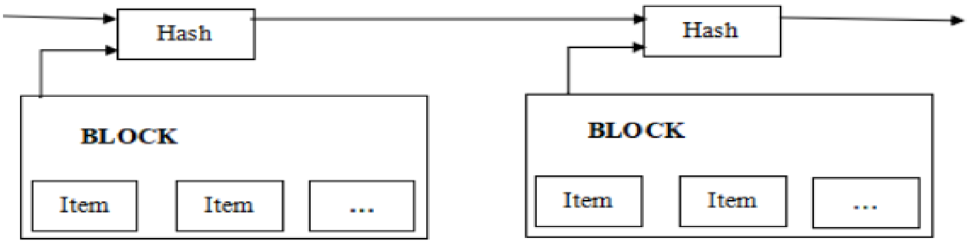


Fig 2:Blockchain blocks

HASHING

Hashing is the method of adjusting the arbitrary and variable input size to a fixed output size. There are various functions which perform different levels of hashing.We have implemented security by using SHA-256. SHA-256 is one of the SHA-1(collectivelyreferredtoasSHA-2) success or hash functions and is one of the strongest hash functions available. SHA-256 is not much more difficult to code than SHA1 and is in noway corrupted yet. The 256 bit key makes AES a good partner feature which is a symmetrical key encryption cipher, meaning that the same key is used for encryption and decryption. Unlike its other predecessors, the algorithm's versatility is that item braces any input length and produces an arbitrary output length,while stall other algorithms generate a set output length.

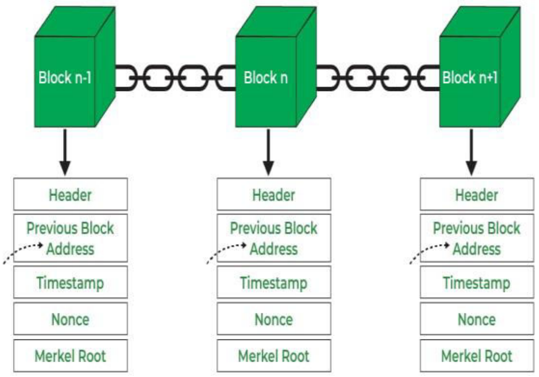


Fig 3:Hash values

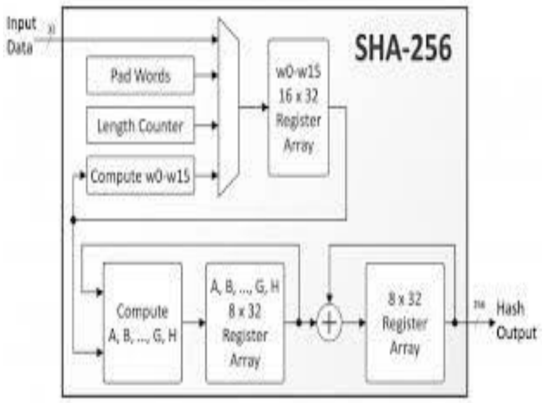


Fig 4: SHA-256

BLOCKCHAIN BASED FOR VOTING SYSTEM

Voters send their personal data to administrators for verification via their devices, which we assume to be secure. The interaction between voters and system administrators is off-chain, which means that it is not part of the blockchain system. When a voter's identity is confirmed, the administrators issue the tokens that let voters to cast their vote into the blockchain. Eligible voters receive one token in their blockchain application that acts as an electronic wallet; it is also the interface to interact with the blockchain to vote and audit. The token can only be used once and cannot be transferred or sold between wallets.

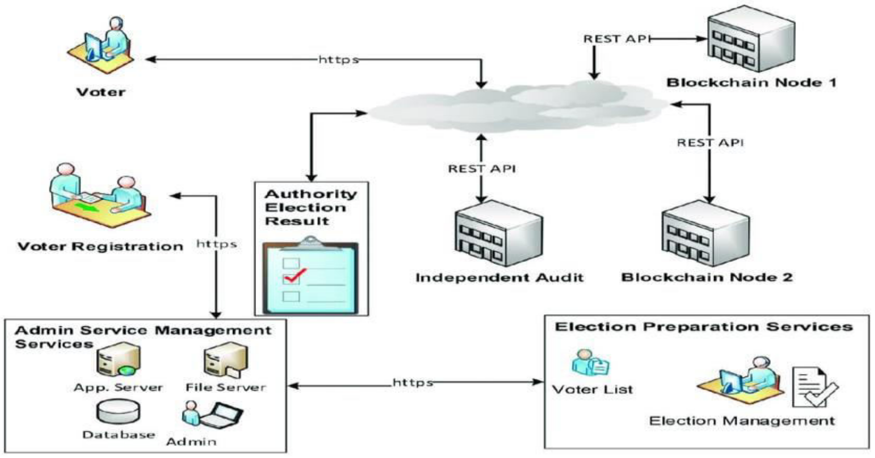


Fig 5:Blockchain voting for admin service management

When a voter wants to fill out his ballot to cast the vote, the application generates a zero-knowledge set membership proof (ZKSMP) code to prove the validity of the choice made without having to reveal it; the vote must be within a list of candidates predefined by the administrators. So, both the token and the code will be used to validate the ballot; this will eliminate the risk of Sybil attacks. All voters have to cast their ballot within a period previously configured by the administrators. Proof of Authority validators act like miners in the online blockchain system. They validate transactions and add them to the blockchain over the voting phase.

BLOCKCHAIN VOTING SYSTEM FOR MODULES

The client or an individual will fill out the registration form in the registration module of the process after which their entry will be registered in the database and they are now eligible to vote for their preferred candidate. Registration form filling is mandatory without which the person is not allowed or is not eligible to vote. The registration form includes the voter information and also some documents have to be uploaded once it is done the form is submitted and the entry is reflected in the database. After the registration form is submitted the phone number and the email id given by the user is verified and the registration process is completed.

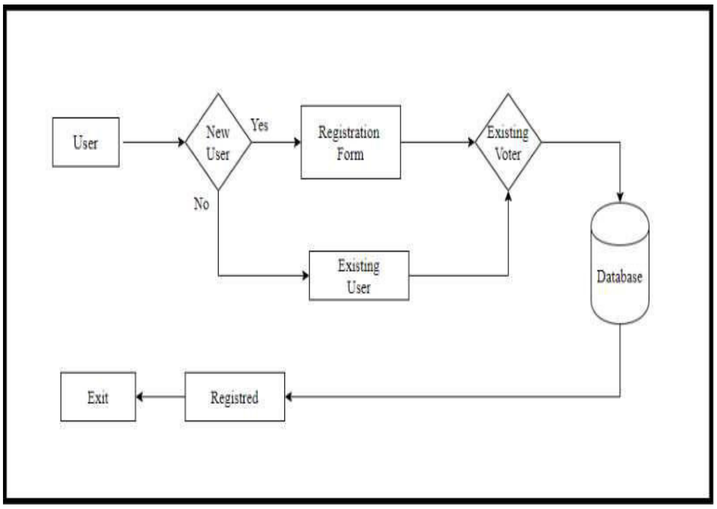


Fig 6:Registration Module

Once the registration form is submitted, the person is now eligible to vote.This module handles enter the registered Aadhar_number or voter_id logs in to the system.the registration of eligible voters onto the blockchain network. It may involve identity verification and authentication processes to ensure the integrity of the voting pool. The user will sign into the credentials in the authentication module and after which credentials will be checked and the user will only be able to access the dashboard after the verification has been completed. Once the user is verified then the user is authenticated with their Email verification only after which the voter wallet is generated and a token is provided to the voter which will be used to cast their vote. The votes are casted by transferring the token from the voter's wallet to the respective candidate's wallet.

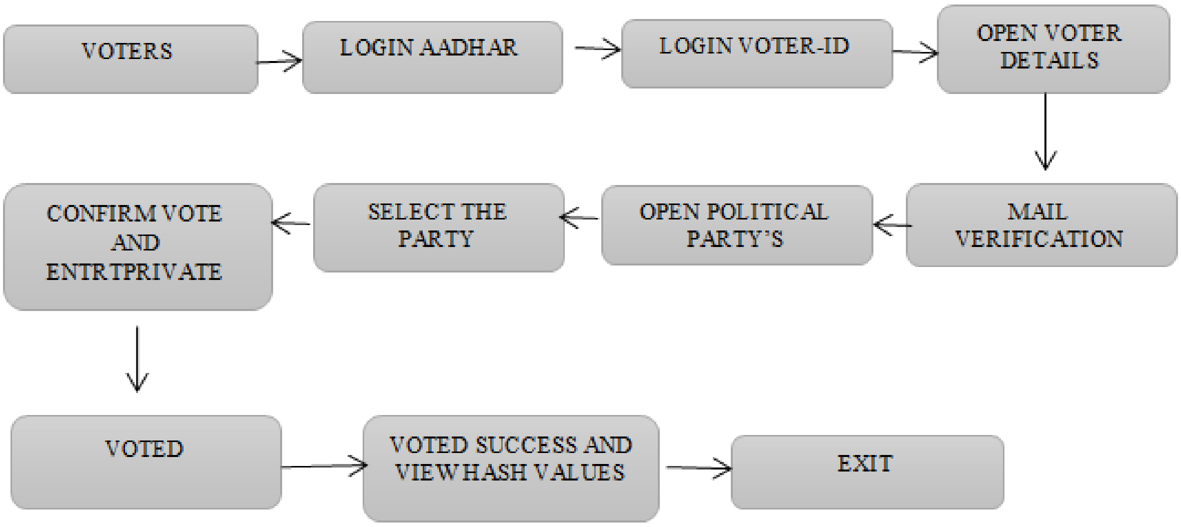
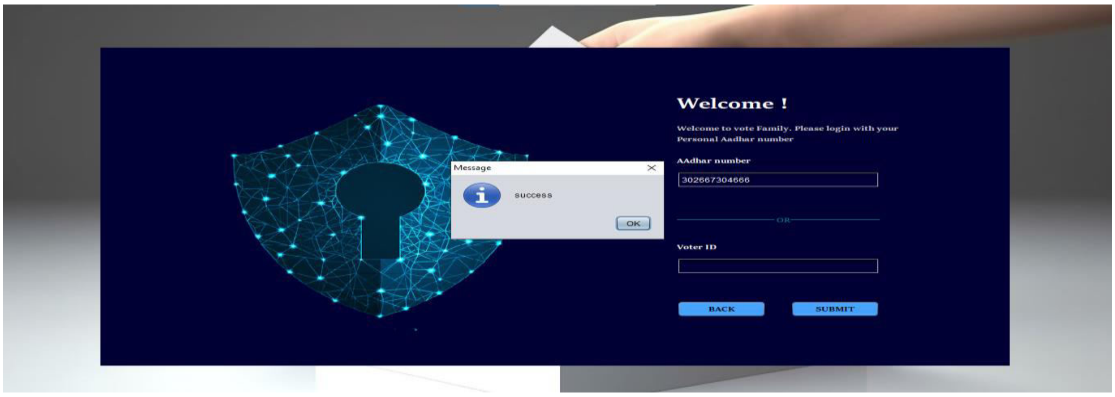


Fig 7:Flowchart

After login the user view the user Information like,Aadhar number,voter id,name,phone number,profile picture and date of birth.Once the user is verified then the user is authenticated with their Email verification only after which the voter wallet is generated and a token is provided to the voter which will be used to cast their vote. The votes are casted by transferring the token from the voter's wallet to the respective candidate's wallet.

V. RESULT

SCREENSHOT:



Welcome !

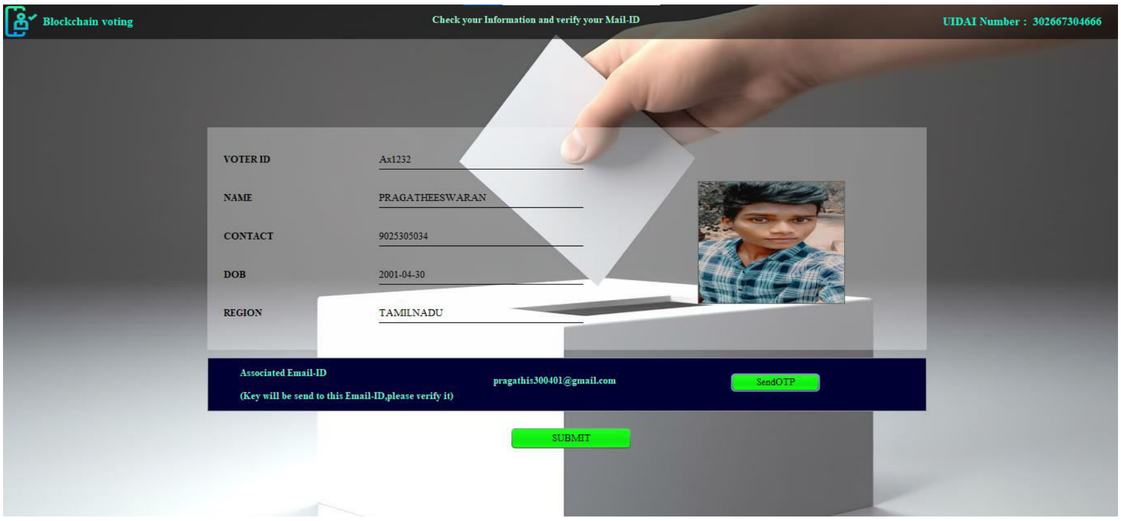
Welcome to vote Family. Please login with your Personal Aadhar number

AAdhar number: 302667304666

Voter ID:

Message: success

Fig 8:Voters login



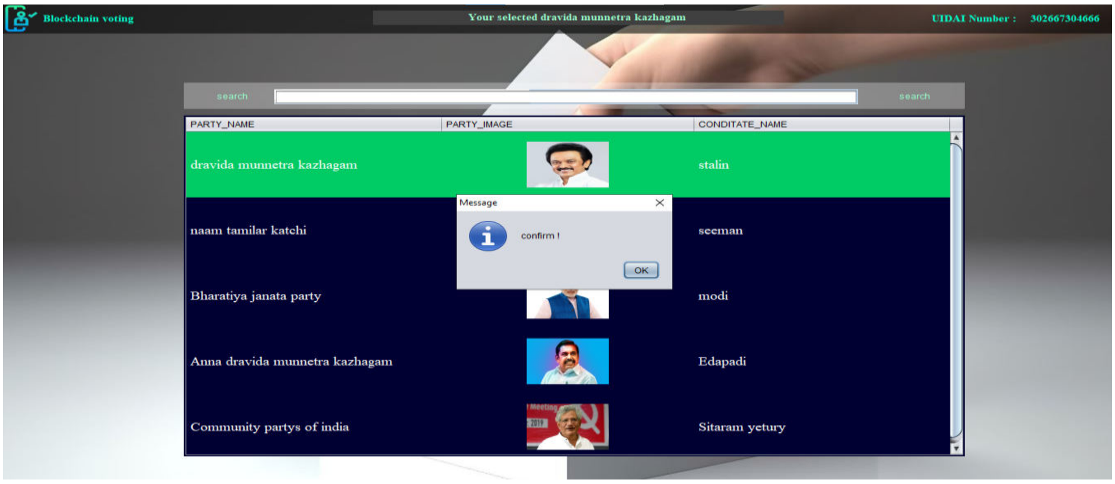
Blockchain voting — Check your Information and verify your Mail-ID — UIDAI Number : 302667304666

VOTER ID	Ax1232
NAME	PRAGATHEESWARAN
CONTACT	9025305034
DOB	2001-04-30
REGION	TAMILNADU

Associated Email-ID: pragathis300401@gmail.com

(Key will be send to this Email-ID,please verify it)

Fig 9: Voters Information

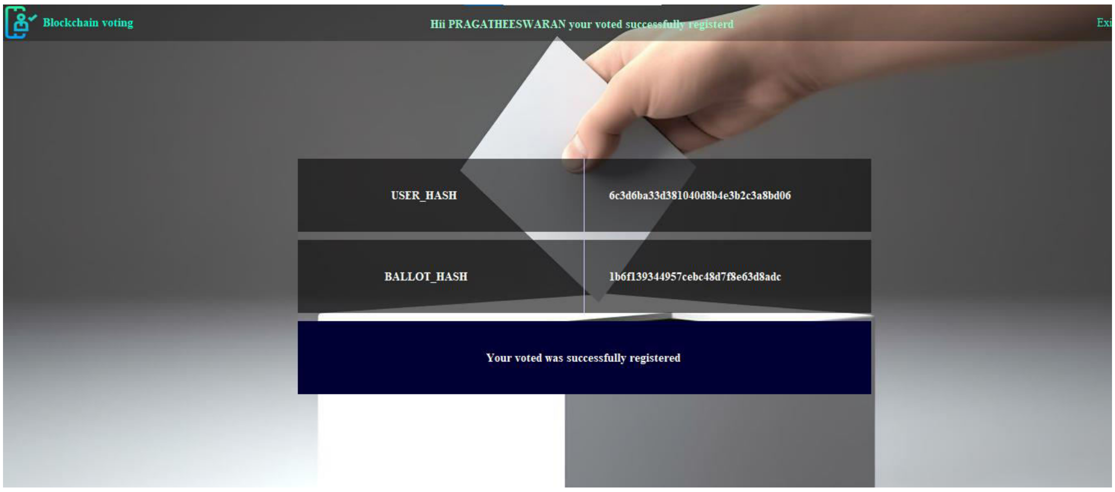


Blockchain voting — Your selected dravida munnetra kazhagam — UIDAI Number : 302667304666

PARTY_NAME	PARTY_IMAGE	CONDITATE_NAME
dravida munnetra kazhagam		stalin
naam tamilar katchi		seeman
Bharatiya janata party		modi
Anna dravida munnetra kazhagam		Edapadi
Community partys of india		Sitaram yetury

Message: confirm !

Fig 10:Political party’s

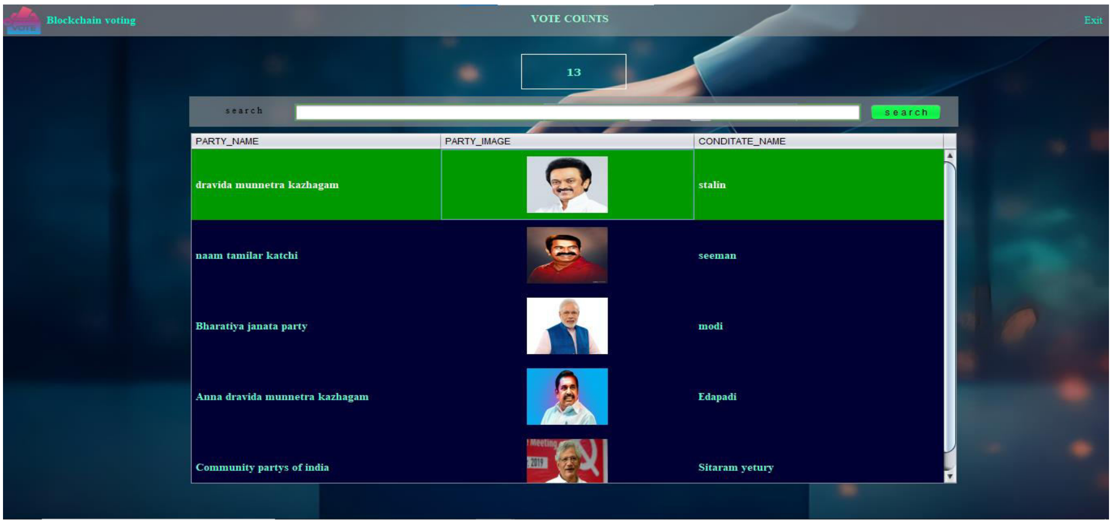


Hii PRAGATHEESWARAN your voted successfully registerd

USER_HASH	6c3d6ba33d381040d8b4e3b2c3a8bd06
BALLOT_HASH	1b6f139344957cebc48d7f8e63d8adc

Your voted was successfully registered

Fig 11:View hash values for voters confirmation

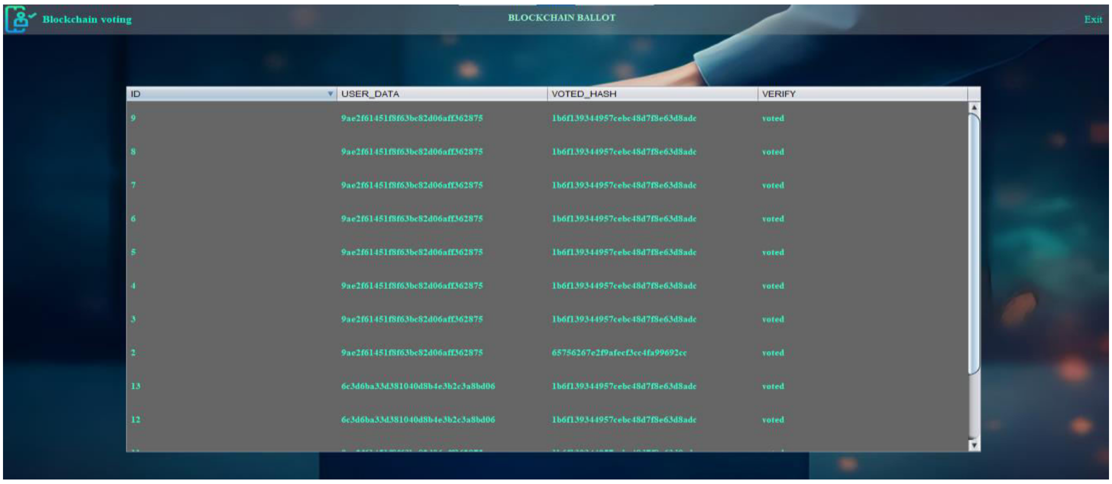


VOTE COUNTS

13

PARTY_NAME	PARTY_IMAGE	CONDITATE_NAME
dravida munnetra kazhagam		stalin
naam tamilar katchi		seeman
Bharatiya janata party		modi
Anna dravida munnetra kazhagam		Edapadi
Community partys of india		Sitaram yetury

Fig 12:Vote counts



BLOCKCHAIN BALLOT

ID	USER_DATA	VOTED_HASH	VERIFY
9	9ae2f61451f8f63bc82d06aff362875	1b6f139344957cebc48d7f8e63d8adc	voted
8	9ae2f61451f8f63bc82d06aff362875	1b6f139344957cebc48d7f8e63d8adc	voted
7	9ae2f61451f8f63bc82d06aff362875	1b6f139344957cebc48d7f8e63d8adc	voted
6	9ae2f61451f8f63bc82d06aff362875	1b6f139344957cebc48d7f8e63d8adc	voted
5	9ae2f61451f8f63bc82d06aff362875	1b6f139344957cebc48d7f8e63d8adc	voted
4	9ae2f61451f8f63bc82d06aff362875	1b6f139344957cebc48d7f8e63d8adc	voted
3	9ae2f61451f8f63bc82d06aff362875	1b6f139344957cebc48d7f8e63d8adc	voted
2	9ae2f61451f8f63bc82d06aff362875	65756267e2f9afecf3cc4fa99692cc	voted
13	6c3d6ba33d381040d8b4e3b2c3a8bd06	1b6f139344957cebc48d7f8e63d8adc	voted
12	6c3d6ba33d381040d8b4e3b2c3a8bd06	1b6f139344957cebc48d7f8e63d8adc	voted

Fig 13:Voters Blockchain Ballot

OUTCOMES: To create the Decentralized online voting system using blockchain ensures transparency and immutability by recording each vote as a transaction on a distributed ledger. This transparency enhances trust in the electoral process as voters and stakeholders can independently verify the integrity of the results without relying on centralized authorities. by incorporating mail verification, the system can authenticate the identity of voters securely, reducing the risk of fraudulent or duplicate votes. This dual-layer approach not only strengthens security but also increases voter confidence in the fairness and accuracy of the election outcomes. decentralization eliminates the need for a central authority to oversee the voting process, reducing administrative costs and potential points of failure or manipulation.This automation also streamlines the tallying process, providing faster and more reliable election results.

VI. CONCLUSION

The design of a secured database system using blockchain technology is important to the society.As the world is advancing in a new technological age, there is a need to create a decentralized database system that will enable transparency in registering voters and casting votes without involving third party. If not adopted, may lead to mutability of data, single point failure regarding the third party and various security threats that might lead to malicious acts.this has contributed to the massive manipulation of votes in our voting system as well as being vulnerable to attackers. Therefore, introducing a blockchain-based database in our voting system will help minimize the scalability issues which will in turn creates trust between different participants who want to enter into a business agreement through the consensus algorithm, complete transparency of data and decentralized while keeping the users' privacy.

REFERENCES

1. Alrebdi et al., 2022,Norah Alrebdi, Abdulatif Alabdulatif, Celestine Iwendi,Zhuotao Lian Svbe: searchable and verifiable blockchain-based electronic medical records system Scientific Reports.
2. Alvi et al., 2020,Syada Tasmia Alvi, Mohammed Nasir Uddin, Linta Islam,Digital voting: A blockchain-based e-voting system using biohash and smart contract 2020 Third International Conference on Smart Systems and Inventive Technology (ICSSIT) (2020).
3. Ayed, 2017,Ahmed Ben Ayed, A conceptual secure blockchain based electronic voting system International Journal of Network Security & Its Applications, 9 (2017).
4. Alvi et al., 2021,Syada Tasmia Alvi, Linta Islam, Tamanna Yesmin Rashme, Mohammed Nasir Uddin Bsevoting: A conceptual framework to develop electronic voting system using sidechain 2021 8th International Conference on Electrical Engineering, Computer Science and Informatics (EECSI) (2021)..
5. Bosri et al., 2019,R. Bosri, A.R. Uzzal, A.A. Omar, A.S.M.T. Hasan, M.Z.A. Bhuiyan Towards a privacy-preserving voting system through blockchain technologies 2019 IEEE Intl Conf on Dependable, Autonomic and Secure Computing.
6. Chaieb et al., 2019,Marwa Chaieb, Mirko Koscina, Souheib Yousfi, Pascal Lafourcade, Riadh Robbana Dabsters:A privacy preserving e-voting protocol for permissioned blockchain International Colloquium on Theoretical Aspects of Computing, Springer (2019).
7. Dimitriou, 2020,Tassos Dimitriou Efficient, coercion-free and universally verifiable blockchain-based voting Computer Networks, 174 (2020).
8. Gautam et al., 2021,Mehul Gautam, Shoaib Akthar, Aktar Basha, Golda Dilip Blockchain for secure and proper management of medical data and records 2021 5th International Conference on Electronics, Communication and Aerospace Technology (ICECA) (2021).
9. Uddin et al., 2021,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.
10. Braghin et al., 2019,Chiara Braghin, Stelvio Cimato, Simone Cominesi, Ernesto Damiani, and Lara Mauri. Towards Blockchain-Based E-Voting Systems, pages 274–286. 12 2019.

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

| Mobile No: +91-6381907438 | Whatsapp: +91-6381907438 | ijmrset@gmail.com |

www.ijmrset.com