International Journal of Scientific Research & Engineering Trends
Volume 10, Issue 5, Sept-Oct-2024, ISSN (Online): 2395-566X

Decentralized E-Voting System Using Blockchain Technology

Professor Disha Nagpure, Jidnesh Shah, Abhay Sanap, Hanuman Keskar, Krushna Khairnar
Department of Artificial Intelligence and Machine Learning,
Alard College of Engineering and Management, Marunji, Pune, Maharashtra, India

Abstract- Elections are a cornerstone of modern democracies. However, concerns regarding trust and potential manipulation plague traditional voting systems. This paper explores the potential of decentralized e-voting systems powered by blockchain technology and Aadhaar OTP verification. By leveraging the immutability, transparency, and security of blockchain, combined with the robust authentication of Aadhaar OTP, this system aims to revolutionize the electoral process. It addresses key challenges of traditional methods, such as fraud and lack of trust, through the use of smart contracts, voter identity verification, and cryptographic techniques.

Index Terms- Blockchain, Decentralization, Voting Scheme, Aadhaar OTP Verification, Distributed System, EVM.

I. INTRODUCTION

The advent of blockchain technology has ushered in a new era of decentralized applications, significantly impacting various industries. One area with immense potential for disruption is the electoral process. Traditional voting systems often face challenges such as fraud, manipulation, and lack of trust. To address these issues, decentralized e-voting systems have emerged as a promising alternative. This research explores the feasibility and benefits of implementing a decentralized e-voting system utilizing blockchain technology and Aadhaar OTP (One-Time Password) verification. By leveraging the immutability, transparency, and security of blockchain, combined with the robust authentication mechanism of Aadhaar OTP, this system aims to enhance the integrity and efficiency of the electoral process.some guidelines.

Blockchain technology offers a decentralized, distributed ledger that is resistant to tampering. This ensures that votes are securely recorded and cannot be altered or deleted. Additionally, the public nature of the blockchain allows for transparency and public verification of the voting process, fostering trust and confidence among voters.

1. Traditional E-Voting System

Recent major technical challenges regarding e-voting systems include, but not limited to, secure digital identity management. Any potential voter should have been enrolled in the voting system prior to the elections. Their information should be in a digitally processable format. Besides, their identity information should be kept private in any involving database. Traditional E-voting system may face following problems:

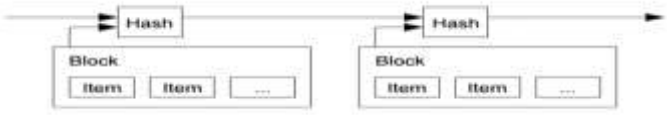
Anonymous Vote-Casting: Ensuring anonymity of votes after submission is crucial.

Individualized Ballot Processes: Representing votes in web applications or databases securely remains an open question.
Ballot Casting Verifiability: Voters require a mechanism to verify their submitted votes.

High Initial Setup Costs: Initial deployments of e-voting systems can be expensive.

Increasing Security Problems: Cybersecurity threats pose a significant risk to online voting systems.

2. What is Blockchain technology?

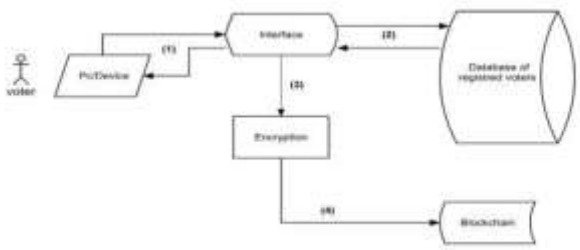


Blockchain is a decentralized, distributed ledger technology that records transactions in a secure and transparent manner. It's a chain of blocks, each containing a record of data or transactions. Once a block is added to the chain, it cannot be altered or deleted, ensuring the immutability of the data. The public nature of the blockchain allows for transparency and public verification of the voting process, fostering trust and confidence among voters.

3. Working of E-Voting Using Blockchain

BAs per the above structure the working of e-voting system using blockchain is: Blockchain Based Electronic Voting System:

© 2024 IJSRET



Requesting to Vote: The user will have to log in to the voting system using his credentials- in this case, the e-voting system will use his Social Security Number, his address, and the voting confirmation number provided to registered voters by the local authorities . The system will check all information entered and, if matched with a valid voter, the user will be authorized to cast a vote. Our e-Voting system will not allow participants to generate their own identities and register to vote. Systems that allow identities to be arbitrarily generated are usually vulnerable to the Sybil attack where attackers claim a large number of fake identities and stuff the ballot box with illegitimate votes.

Casting a Vote: Voters will have to choose to either vote for one of the candidates or cast a protest vote. Casting the vote will be done through a friendly user interface . For each voter a token is generated known as Ethereum, with initial Boolean value one, once a vote is casted it becomes 0. A voter can cast a vote if and only if Ethereum value is 1.In this way the revoting problem is resolved.

Encrypting Votes: After the user casts his vote, the system will generate an input that contains the voter identification number followed by the complete name of the voter as well as the hash of the previous vote. This way each input will be unique and ensure that the encrypted output will be unique as well. The encrypted information will be recorded in the block header of each vote cast. The information related to each vote will be encrypted using SHA one-way hash function that has no known reverse to it. The only theoretically possible way to reverse the hash would be to guess the seed data and the encryption method and then hash it to see if the results match. This way of hashing votes makes it nearly impossible to reverse engineer, therefore there would be no way voters' information could be retrieved .

Adding the Vote to the Blockchain: After a block is created, and depending on the candidate selected, the information is recorded in the corresponding blockchain. Each block gets linked to the previously cast vote.

4. Consensus Algorithms

Consensus algorithms are essential components of blockchain technology that ensure the integrity and security of the distributed ledger. They are mechanisms that enable nodes in the network to agree on the validity of transactions and the order in which they should be added to the blockchain. This consensus helps to prevent double-spending, maintain data consistency, and ensure the overall security of the network. Consensus Algorithms are protocols employed by blockchain to ensure that all ledgers in the nodes of a blockchain network are persistently consis- tent. This survey reviews the following con-sensus algorithms used in blockchain e-voting systems: Proof of Work, Proof of Stake, Dele- gated Proof of Stake, Proof of Activity, Proof of Burn, Practical Byzantine Fault Tolerance, Proof of Vote, and Parallel Proof of Vote. Proof of Work (PoW) is the most popular consensus algorithm deployed by Bitcoin and Ethereum.

Nodes in the P2P network, called miners or validators, compete to solve a computation- ally challenging puzzle also known as a ‘hard mathematical problem’ to link the new block to the last block in the valid blockchain. The winner is the miner who finds the right solu- tion. They get the right to create a new block in the blockchain, The process is called ‘mining’.

Proof of Stake (PoS) is a consensus algorithm that makes blockchain networks more effi- cient by eliminating the computational-intensive mining process used in PoW . In PoS, the miners are called forgers and the mining process is known as forging. Forgers deposit a certain number of coins that they own as stakes. This stake is used by the protocol to select the next forger in the network. PoS has two forger selection methods, namely, the coin-age selection and the randomized block selection.

5. Aadhar

Aadhaar is a 12-digit unique identity number that can be obtained by residents of India, based on their biometric and demographic data (see Figure.1). The data is collected by a statutory authority, the Unique Identification Authority of India (UIDAI). Aadhaar is the world's largest biometric ID system. The detailed personal information being collected is of extremely high importance to a private. Major financial transactions are linked with information collected in Aadhaar. Data leaks are a gold mine for criminals. The UIDAI confirms quite 200 government websites were publicly displaying confidential Aadhaar data[1]; though removed now, the data leaked cannot be scrubbed from hackers' databases. Those

© 2024 IJSRET

confidential Aadhaar details are stored in a single database and it is maintained by UIDAI. Since the database is centralized there are so many disadvantages. The main disadvantage is the security threat. If those data are stored in the blockchain, data vulnerability is going to be reduced.

Blockchains are cryptographically signed digital ledgers where transactions are framed into blocks. Each block is linked to the previous block with its hash value which is generated cryptographically. When new blocks are added, it is reflected across all copies of the ledger in the network. At their initial level, they enable a group of users to record transactions in a ledger which is public to that group, such that no transaction can be changed once published.

6. Aadhar Verification

Aadhar Verification is the type of verification which enables the user to verify, manage storage, authentication, authorization, data sharing and protection of identities within the organization and on the web. The currently deployed system is susceptible to single point failure, lack of interoperability and privacy issues . The blockchain based systems ensures the consensus, transparency and integrity of the personal data sharing on distributed ledger technology.

Aadhaar OTP (One-Time Password) verification is a security measure used in various online transactions in India. It adds an extra layer of security by requiring users to enter a unique, time-sensitive code sent to their registered mobile number. This helps prevent unauthorized access and fraudulent activities.

In the context of decentralized e-voting systems, Aadhaar OTP verification can be implemented to enhance security and prevent voter impersonation. When a voter registers for the system, their Aadhaar number is linked to their account. During the voting process, the system sends an OTP to the voter's registered mobile number. The voter must enter the correct OTP to proceed with casting their vote. This ensures that only the rightful owner of the Aadhaar card can access the voting system and cast their vote.

The proposed Aadhar OTP verification provides self sovereign identity through decentralized networks with no third party to share their personal identity information without their consent.

7. Comparison of Hashing Algorithms

In the following table the comparison between the various cryptographic hash algorithms like SHA-1, SHA-2, and SHA-3 shows various parameters.

Ethereum, in a consensus engine called Ethash uses Keccak 256. Keccak may be a family of hash functions that eventually got standardized to SHA-3 (SHA256 is a component of a family of hash functions called SHA-2). Ethereum called it Keccak rather than SHA-3 because it has slightly different parameters than the present SHA-3. SHA-256 (more specifically SHA-2 i.e. SHA-256(SHA-256(TXN)) is employed to encrypt blocks of blockchain for bitcoin cryptocurrency. Ethash is employed to encrypt blocks of blockchain for Ethereum cryptocurrency. Ethereum uses Keccak-256 rather than the NIST standardized SHA-3 hash function, solidity 0.4.3 has introduced keccak256. (It is an alias to sha3, meaning that keccak256 produces identical results to sha3, but with the intent to avoid confusion, especially for developers new Ethereum.)

Properties	Name of Algorithms		
	SHA-1	SHA-2	SHA-3
Block size	512 bits	512/1024 bits	1088/576 bits
Word size	32 bits	32/64 bits	320/320 bits
Output size	160 bits	256/512 bits	1600/1600 bits
Rounds	80	64/80	24/24
Operations	ADD, XOR, OR, AND, NOT, ROTATE	ADD, XOR, OR, AND SHIFT, ROTATE	-
Constructions	Merkle-Damgard	Merkle-Damgard	Sponge

It's recommended that the new code use keccak 256 rather than sha3. Keccak is predicated on a completely unique approach called sponge construction. [14] Sponge construction is predicated on a good random function or random permutation, and allows inputting ("absorbing" in sponge terminology) any amount of knowledge, and outputting ("squeezing") any amount of knowledge while acting as a pseudorandom function with reference to all previous inputs. This results in great flexibility.

8. Algorithm

- Enter the details such as user name, contact number, Email ID to create a wallet for the user.
- Hash will be created for the transaction that created the wallet.
- Upload Aadhaar identity details and the scanned copy of Aadhaar that will be saved in the IPFS with hashed addresses stored in the Blockchain.
- Smart contract helps in signing a particular transaction and generates hash value which will be stored in each block in the block chain. If any slight changes in the block, the hash value of that block changes drastically.
- Third party companies requesting to access specific details of a person for authentication purposes, a notification will be sent to the individuals owning the identity.

© 2024 IJSRET

- Once the user allows the companies to access their details, third-parties can use the identifiable information for authenticating a person. Blockchain does not store the user's data or information. Instead, the transactions made between identity holders and companies will only be recorded on the blockchain. The Aadhaar details are stored on IPFS in an encrypted form.

9. Literature Survey

Decentralized e-voting systems powered by blockchain technology have emerged as a promising alternative to traditional voting methods. The integration of Aadhaar verification adds an extra layer of security and authenticity to the process. This literature survey explores existing research and developments in this field.

Blockchain technology provides a secure, transparent, and immutable ledger for recording votes. Studies have demonstrated its potential to enhance the integrity and reliability of elections. Aadhaar, India's unique identification system, can be used to verify voter identity and prevent fraud. Integrating Aadhaar OTP verification adds an extra layer of security to the voting process.

Smart contracts can automate various aspects of the voting process, such as ballot creation, voting, and tallying, reducing the risk of human error and manipulation. Researchers have explored cryptographic techniques to protect voter privacy and ensure the security of the voting process. Addressing scalability challenges for large-scale elections is a key area of research. Techniques such as sharding and layer-2 solutions are being investigated. Ensuring interoperability between different blockchain-based e-voting systems is crucial for widespread adoption.

These studies have explored various aspects of decentralized e-voting systems, including system architecture, security measures, privacy protection, scalability, and interoperability. While significant progress has been made, further research is needed to address remaining challenges and ensure the widespread adoption of this technology.

II. METHODS AND MATERIAL

The proposed decentralized e-voting system consists of the following components:

Blockchain Network: A permissioned blockchain network (e.g., Hyperledger Fabric, Ethereum) is deployed to securely store and manage voting data.

Smart Contracts: Smart contracts are deployed on the blockchain to automate voting procedures, such as ballot creation, voting, and tallying.

Voter Registration Module: A module for registering eligible voters, including verification of identity using Aadhaar OTP.

Voting Interface: A user-friendly interface for voters to cast their votes securely.

Authentication Server: An Aadhaar authentication server for verifying voter identity using OTP.

Workflow

Voter Registration: Eligible voters register their information on the system, providing their Aadhaar number.The system sends an OTP to the voter's registered mobile number for verification.Upon successful verification, the voter's information is stored on the blockchain.

Ballot Creation: Smart contracts generate unique, encrypted ballots for each registered voter.Ballots are stored on the blockchain, ensuring immutability and transparency.

Voting: Voters access the voting interface using their credentials.They select their preferred candidates and cast their votes.Votes are recorded as transactions on the blockchain.

Tallying: Smart contracts automatically tally the votes on the blockchain.

Result Publication: The final results are published on the blockchain, providing an auditable and tamper-proof record.

III. CONCLUSION

Decentralized e-voting systems using blockchain technology and Aadhaar verification offer a promising solution to the challenges faced by traditional voting systems. While significant progress has been made, further research is needed to address scalability, privacy, and regulatory concerns. By addressing these challenges, blockchain-based e-voting systems can contribute to enhancing the integrity and efficiency of democratic processes.

REFERENCES

1. A. A. Mandavkar and R. V. Agawane, "Mobile based facial recognition using OTP verification for voting system," 2015 IEEE International Advance Computing Conference (IACC), Banglore, India, 2015, pp. 644-649, doi: 10.1109/IADCC.2015.7154786.
2. N. Choudhary, S. Agarwal, G. Lavania, "Smart Voting System through Facial Recognition",April 2019, https://doi.org/10.26438/ijsrcse/v7i2.710. pp. 7-10, doi:

© 2024 IJSRET

3. A. Alvappillai, P. N. Barrin, "Face Recognition using MachineLearning",2017.doi:https://api.semanticscholar.org/CorpusID :43539771 .
4. H. Agarwal and G. N. Pandey, "Online voting system for India based on AADHAAR ID," 2013 Eleventh International Conference on ICT and Knowledge Engineering, Bangkok, Thailand, 2013, pp. 1-4, doi: 10.1109/ICTKE.2013.6756265.
5. Ayesha Shaikh, Bhavika Oswal, Divya Parekh, Prof. B. Y. Jani, 2014, E-voting Using One Time Password and Face Detection and Recognition, Issue 02.
6. J. Liu, B. Li, L. Chen, M. Hou, F. Xiang and P. Wang, "A Data Storage Method Based on Blockchain for Decentralization DNS," 2018 IEEE Third International Conference on Data Science in Cyberspace (DSC), Guangzhou, China, 2018, pp. 189-196, doi: 10.1109/DSC.2018.00035.
7. Dagher, Gaby G.; Marella, Praneeth Babu; Milojkovic, Matea; and Mohler, Jordan. (2018). "BroncoVote: Secure Voting System Using Ethereum's Blockchain". ICISSP 2018: Proceedings of the 4th International Conference on Information Systems Security and Privacy, 2018-January, http://dx.doi.org/10.5220/0006609700960107
8. Hanifa Tunisia, Rifa & Rahardjo, Budi. (2017). Blockchain based e voting recording system design. 1-6. 10.1109/TSSA.2017.8272896.
9. S. A. Adeshina and A. Ojo, "Maintaining Voting Integrity using Blockchain," 2019 15th International Conference on Electronics, Computer and Computation (ICECCO), Abuja, Nigeria, 2019, pp. 1-5, doi: 10.1109/ICECCO48375.2019.9043225.
10. F. Schroff, D. Kalenichenko and J. Philbin, "FaceNet: A unified embedding for face recognition and clustering," 2015 IEEE Conference on Computer Vision and Pattern Recognition (CVPR), Boston, MA, USA, 2015, pp. 815-823, doi: 10.1109/CVPR.2015.7298682.
11. I. William, D. R. Ignatius Moses Setiadi, E. H. Rachmawanto, H. A. Santoso and C. A. Sari, "Face Recognition using FaceNet (Survey, Performance Test, and Comparison)," 2019 Fourth International Conference on Informatics and Computing (ICIC), 2019, pp. 1-6, doi: 10.1109/ICIC47613.2019.8985786..

© 2024 IJSRET