INTERNATIONAL JOURNAL OF PROGRESSIVE RESEARCH IN ENGINEERING MANAGEMENT AND SCIENCE (IJPREMS)

www.ijprems.com
editor@ijprems.com

Vol. 04, Issue 04, April 2024, pp: 1355-1359

e-ISSN : 2583-1062

Impact Factor: 5.725

"BLOCK CHAINED ONLINE VOTING SYSTEM"

Mujawar suraj[1], Mulla Sarfaraj[2], Kasbekar Kshawadip[3], Mattekhane suhana[4], P. P. Kalyankar[5]

[1,2,3,4]Student, Dept of Computer Science & Engineering, BMIT"s, Solapur, India.

[5]Project Guide: Student, Dept of Computer Science & Engineering, BMIT"s, Solapur, India.

ABSTRACT

Voting is an essential activity in modern democracy. To facilitate the voting process, there were several attempts on proposing an electronic voting system such that, the voting and tallying processes can be done e silently and the results would be ac countable to the public. To date, however, an online electronic voting system has been rarely adopted in practice due to the possibility of having the voting result tampered through vote-rigging or cyber attacking. In 2009, the blockchain algorithm was proposed by Satoshi Nakamoto. Blockchain is a tech unique for recording transactions between self-auditing ledgers in an open, distributed, permanent, and variable manner. Even though blockchain was originally designed for a financial applications, it is possible to apply blockchain to other domains, including in the implementation of an online decentralized-based electronic voting system. In this study, the architecture of a blockchain-based electronic voting system, named Block VOTE, is proposed. The architecture design and all related formal definitions are given. To validate the proposal, two BlockVOTE prototypes were implemented using two different blockchain ap plication frameworks. The performance analysis of both versions of the prototypes are given. The analysis of both technical and management aspects on the possibility of adopting the proposed decentralized voting system in an actual voting scenario is also given at the end of this study.

Keyword: Blockchain, Voting System, Electronic Voting Systems, Decentralized Applications.

1. INTRODUCTION

In each democracy, the protection of an election may be a matter of national security. the pc security field has for a decade studied the probabilities of electronic choice systems, with the goal of minimizing the price of getting a national election, whereas fulfilling and increasing the protection conditions of an election from the dawn of democratically electing candidates, the legal system has been supported pen and paper commutation the normal pen and paper with a replacement election system is essential to limit fraud and having the choice method traceable and verifiable Electronic choice machines are viewed as blemished, by the protection community, based totally on physical security considerations. Anyone with physical access to such machine will sabotage the machine, there by moving all votes run up the said machine. Enter blockchain technology.

A blockchain could be a distributed, immutable, in-controvertible, public ledger. This new technology works through four main features: 1. The ledger exists in many different locations no single point of failure in the maintenance of the distributed ledger. 2. There is distributed management over United Nations agency will append new transactions to the ledger. 3. Any projected "new block" to the ledger should reference the previous version of the ledger making a change less chain from wherever the block chain gets its name, and so preventing meddling with the integrity of previous entries. 3 4. A majority of the network nodes must reach a consensus before a proposed new block of entries becomes a permanent part of the ledger. These technological options operate through advanced cryptography providing a security level equal and or bigger than any antecedent not able information .The blockchain technology is thus thought of by several, together with America, to be the best tool, to be accustomed produce the new fashionable democratic ballot method. This paper evaluates the employment of blockchain as a service to implement associate degree electronic ballot (e-voting) system. The system makes the subsequent original contributions: 1. research existing blockchain frameworks suited to constructing blockchain primarily based e-voting system, 2. Propose a blockchain-based e-voting system that uses "permissioned blockchain" to alter liquid democracy.

2. LITERATURE REVIEW

From the time it takes to the current technological development, there are online voting systems. That was clarified in this document. Develop voting plans to make more efficient voting services available with ICT resources than traditional paper-based voting methods. Voters regard themselves as consumers and it is expected that the government will make the voting business more convenient. In the past decade, various forms of electronic voting, especially as additional methods of voting for remote voting, political parties, candidates, the electoral administration, and most importantly to improve the efficiency and promise of the democratic process to the electorate have attracted considerable attention. It allows voters to access the public algorithm and parameters to confirm their turnout.

History Of Virtual Shopping- Existing System: Three types of voting systems exist: 1. System of paper voting The paper voting system is the most common system for voting. Before the electronic voting system is implemented, it will be used. The system of paper ballet includes paper and sealed ballet. Each voter uses and does not share one ballot. This system's disadvantages are i) the time it takes; 2. Electronic voting system 8 Electronic voting systems are electronic voting devices. A voting machine that uses an electronic voting machine to allow voters to pass on their secret ballots. The inconvenience is I poor computer science individuals cannot vote correctly, (ii) safety threats sensitive, (iii) electricity consumption at polling stations; and (iv) costs. 3. Online voting system A new platform for secure votes and voting is the online voting system. Online voting systems are a web-based voting system, which transmits votes via a web browser over the internet. Voters from all over the world are eligible to vote online. Security issues arising from online voting are as follows: In general applications, password protection is high and phishing attacks are not the focus of the application. Website users are not protected efficiently from phishing. The key proposal for ensuring a secure online polling protocol to meet privacy, anonymity, eligibility, equity, verification, and unique online voting safety requirements To achieve reliability, eligibility, transparency, accuracy, and uniqueness of the e-vote system**,** two milliardaires couples have created secure online voting for identities based on cryptographic algorithms.

3. SCOPE AND OBJECTIVE

Online Voting System has a good scope in future due to following reasons: i.) Voter can Vote from anywhere for his/her Constituency. ii.) Vote count will make easy and fast. iii.) Invalid Vote will be rejected. iv.) It Maintains all The Information of all the Candidates & their Votes. Thus, the voting system that is here by conceived must satisfy the following requirements: 1. The election system must be openly verifiable and transparent. 2.

The election system must ensure that the vote cast by the voter has been recorded. 3. Only eligible voters must be allowed to vote. 4. The election system should be tamper-proof. 5. No power-hungry organization must be able to manipulate and right election process. Using a Blockchain, the most important requirements are satisfied: • Authentication: Only registered voters will be allowed to vote. 4 • Anonymity: The system prevents any interaction between the votes casted by the voters and their identities. • Accuracy: Votes once cast are permanently recorded and cannot be modified or changed under any circumstances. • Verifiability: The system will be verifiable such that the number of votes accounted for.

4. PROPOSED WORK

Hash Algorithm The simple rationalization could be a ‘chain’ of blocks. A block is associate degree mass set of information. Knowledge square measure collected and method to suit in an exceedingly block through a process known as mining. Every block may be known employing a science hash (also referred to as a digital fingerprint). The block shaped can contain a hash of the previous block, so blocks will act as a sequence from the primary block ever (known as the Genesis Block) to the shaped block. During this method, all the information may be connected via a connected list structure.

Algorithm Working:

- The SHA-256 algorithm takes an input of any random length and produces an output of a fixed length (256bits).
- In the case of SHA-256 algorithm no matter how big or small is the input the output is of fixed length (256bits). A cryptographic hash function has the following properties:

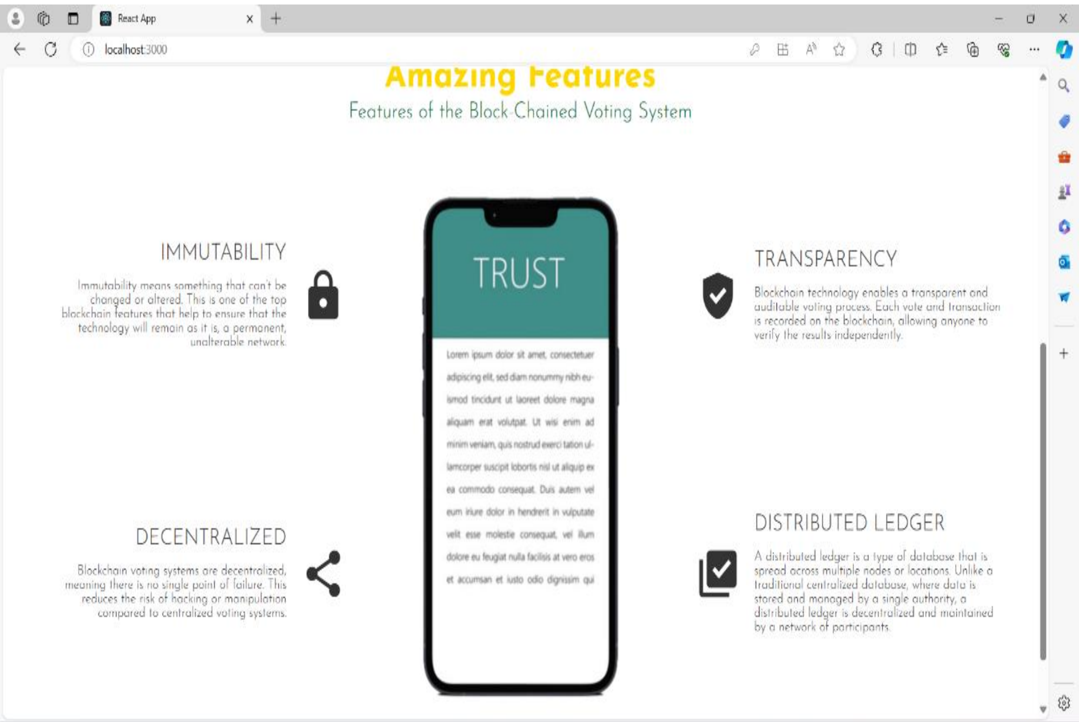
1. Deterministic: This means that no matter how many times we enter the same input we will get the same result.
2. Quick Computation: This means that the result is generated quickly and this leads to an increase in the system efficiency.
3. Pre-Image resistance: Suppose we are rolling a dot(1-6) and instead of getting a specific number we get the hash value. Now we calculate the hash value of each number and then compare it with the result. And for a larger data sets it is possible to break pre-Image resistance by brute force method and this takes tool on that it does not matter.
4. Small changes in Input change the whole Output: A minor change in the input significantly changes the whole output.
5. Collision Resistant: Every input will have a unique hash value.
6. Puzzle friendly: The combination of two values gives the hash value of new variable. The need of hashing in blockchain:

- The blockchain is a sequence of blocks that contain data.
- Each block has a hash pointer that contains previous block’s data.

- So if a hacker tries to attack a particular block, the changes will be reflected to the entire chain of blocks. • Therefore, the blockchain concept is so revolutionary.

5. METHODOLOGY TO BE USED:

1. What approach is taken by the author Once all the nodes of the network are running, a new user can connect to the server. The user registers a non-anonymous user (using aadhar Card, phone, password, etc), and performs the login. The user produces an RSA key pair locally (private key & public key). With the PublicKey server, the user blinds his public key. The public key of the user is blinded and forwarded to the server. The server Blind Signs the Public-Key blinded from the user and returns it to the user. The user unbinds the Public-Key signed by the server, and now has the Public-Key Blind Signed by the server. The user sends the Public-Key blind signed to the p2p network. The peers verify that the Public- Key Blind Signed is correctly signed by the server, if it is, they add the PublicKey to the Ethereum Blockchain, inside a new block. 2. Our approach: As per recent research RSA method to secure data with blind signature has some flaws and can be cracked using high-end computational devices. So we will be using a more secure Salsa20 security algorithm which is found more to be more secure than an existing algorithm like RSA and AES.



Amazing Features

Features of the Block Chained Voting System

IMMUTABILITY

Immutability means something that can't be changed or altered. This is one of the top blockchain features that help to ensure that the technology will remain as it is, a permanent, unalterable network.

TRUST

Lorem ipsum dolor sit amet, consectetuer adipiscing elit, sed diam nonummy nibh euismod tincidunt ut laoreet dolore magna aliquam erat volutpat. Ut wisi enim ad minim veniam, quis nostrud exerci tation ullamcorper suscipit lobortis nisl ut aliquip ex ea commodo consequat. Duis autem vel eum iriure dolor in hendrerit in vulputate velit esse molestie consequat, vel illum dolore eu feugiat nulla facilisis at vero eros et accumsan et iusto odio dignissim qui

TRANSPARENCY

Blockchain technology enables a transparent and auditable voting process. Each vote and transaction is recorded on the blockchain, allowing anyone to verify the results independently.

DECENTRALIZED

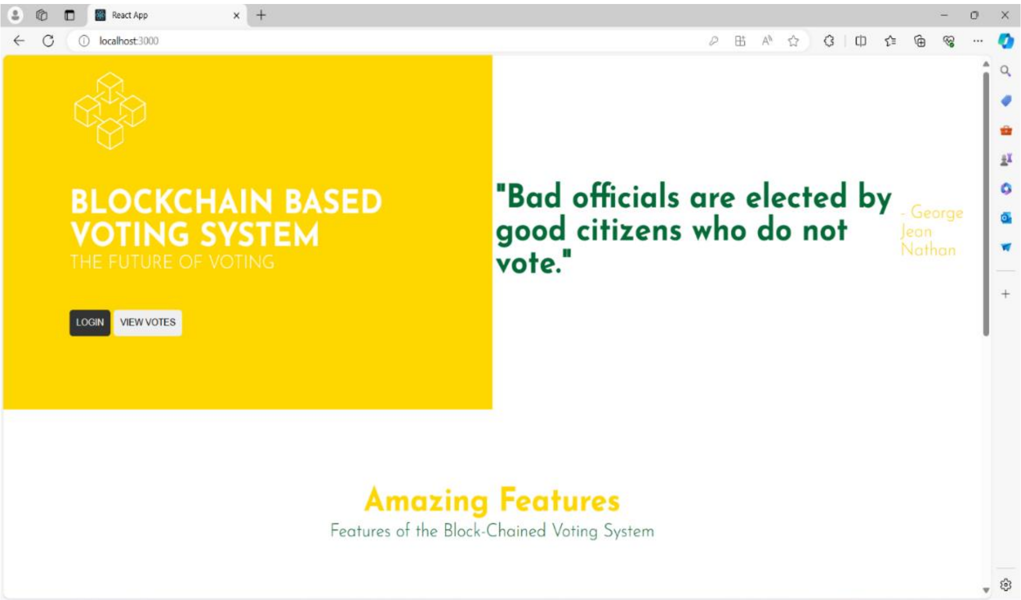
Blockchain voting systems are decentralized, meaning there is no single point of failure. This reduces the risk of hacking or manipulation compared to centralized voting systems.

DISTRIBUTED LEDGER

A distributed ledger is a type of database that is spread across multiple nodes or locations. Unlike a traditional centralized database, where data is stored and managed by a single authority, a distributed ledger is decentralized and maintained by a network of participants.

6. RESULT

Front page for user view



BLOCKCHAIN BASED VOTING SYSTEM

THE FUTURE OF VOTING

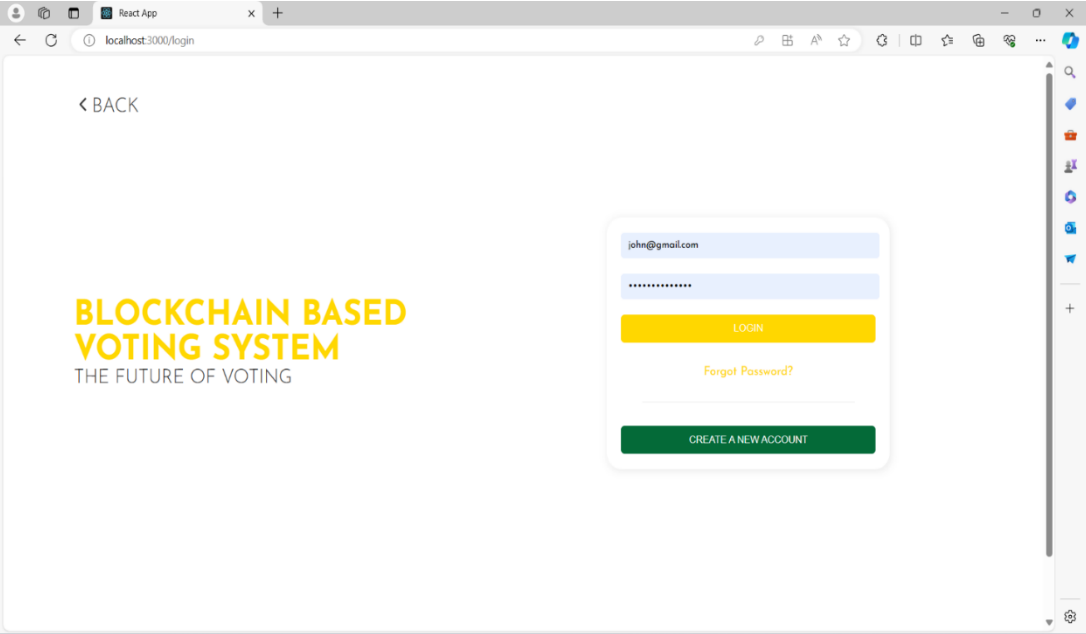
"Bad officials are elected by good citizens who do not vote."

- George Jean Nathan

Amazing Features

Features of the Block-Chained Voting System

User login page

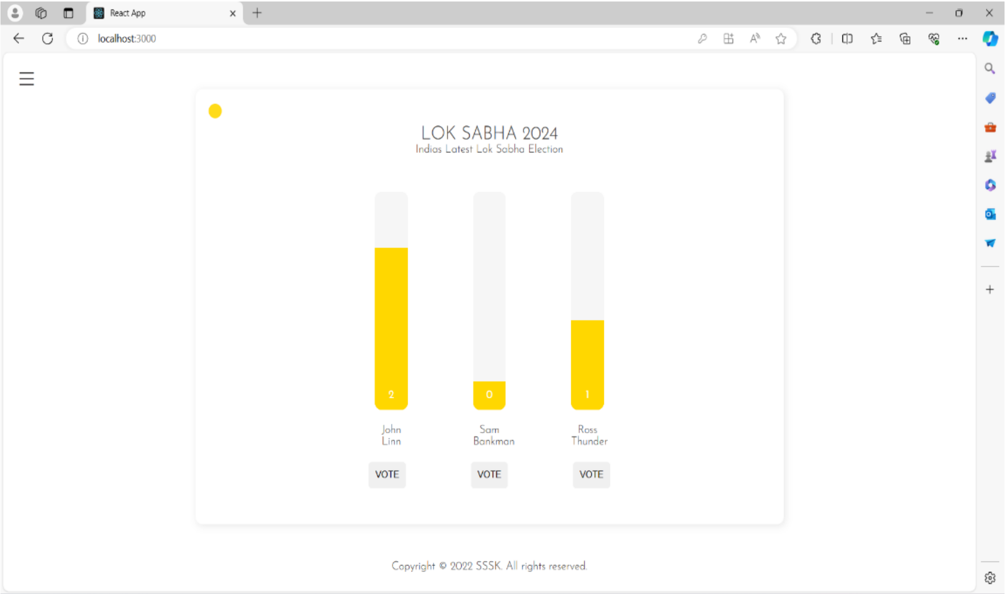


localhost:3000/login

BLOCKCHAIN BASED VOTING SYSTEM
THE FUTURE OF VOTING

john@gmail.com
••••••••••••••

Voting module



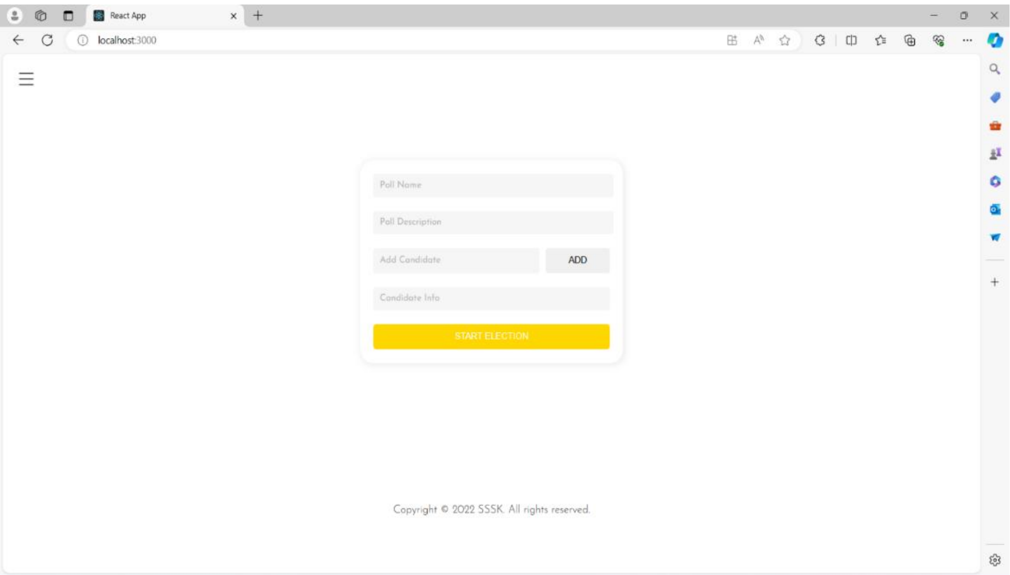
localhost:3000

LOK SABHA 2024
Indias Latest Lok Sabha Election

John Linn	Sam Bankman	Ross Thunder
2	0	1

Copyright © 2022 SSSK. All rights reserved.

Admin Module for starting election



localhost:3000

Copyright © 2022 SSSK. All rights reserved.

7. CONCLUSION

This Online Voting system will manage the Voter's information by which voter can login and use his voting rights. The system will incorporate all features of voting system. It's provided the tools for maintaining voter's vote to every party and it count total no. of votes of every party. There is a DATABASE which is maintained by the ELECTION COMMISION OF INDIA in which all the names of voter with complete information is stored. In this user who is above 18 year's register his/her information on the database and when he/she want to vote he/she has to login by his id and password and can vote to any party only single time. Voting detail store in database and the result is displayed by calculation. By online voting system percentage of voting is increases. It decreases the cost and time of voting process. It is very easy to use and It is vary less time consuming. It is very easy to debug. In conclusion, a block chained voting system represents a transformative approach to modernizing electoral processes, offering a paradigm shift in terms of transparency, security, and trust. By leveraging blockchain technology, this system introduces a decentralized and tamper-resistant ledger that ensures the immutability of voting records. The implementation of smart contracts automates the execution of election rules, providing a transparent and verifiable process from voter authentication to result declaration. The use of cryptographic techniques safeguards voter privacy while maintaining a robust verification mechanism. The decentralized nature of the blockchain network minimizes the risk of central points of failure or manipulation, fostering increased resilience against fraudulent activities. Furthermore, the system addresses longstanding challenges in traditional voting systems, including issues of tampering and result manipulation.

8. REFERENCES

[1] Bell, S., Benaloh, J., Byrne, M. D., Debeauvoir, D., Eakin, B., Kortum, P., McBurnett, N., Pereira, O., Stark, P. B., Wallach, D. S., Fisher, G., Montoya, J., Parker, M. and Winn, M. (2013). "Star-vote: A secure, transparent, auditable, and reliable voting system.", in 2013 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 13). Washington, D.C.: USENIX Association, 2013.

[2] Dalia, K., Ben, R., Peter Y. A, and Feng, H. (2012). "A fair and robust voting system." by broadcast, 5th International Conference on E-voting, 2012.

[3] Adida, B.; 'Helios (2008). "Web-based open-audit voting." in Proceedings of the 17th Conference on Security Symposium, ser. SS'08. Berkeley, CA, USA: USENIX Association, 2008, pp. 335348.

[4] Chaum, D., Essex, A., Carback, R., Clark, J., Popoveniuc, S., Sherman, A. and Vora, P. (2008). "Scantegrity: End-to-end voter-variable optical scan voting." IEEE Security Privacy, vol. 6, no. 3, pp. 40-46, May 2008.

[5] Bohli, J. M., Muller-Quade, J. and Rohrich, S. (2007). "Bingo voting: Secure and coercion- free voting using a trusted random number generator.", in Proceedings of the 1st International Conference on E-voting and Identity, ser. VOTE-ID'07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 111-124.

[6] Adida B. and Rivest, R. L. (2006). "Scratch and vote: Self-contained paper-based cryptographic voting." In Proceedings of the 5th ACM Workshop on Privacy in Electronic Society, ser. WPES '06. New York, NY, USA: ACM, 2006, pp. 29-40.

[7] Blockchain Basics: A Non-Technical Introduction in 25 Steps .

[8] Blockchain Revolution: How the Technology Behind Bitcoin and Other Cryptocurrencies Is Changing the World-Author Don Tapscott