e-ISSN:2582-7219

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

Volume 7, Issue 3, March 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 3, March 2024 |

| DOI:10.15680/IJMRSET.2024.0703045 |

E-Voting Using Blockchain Technology

Mr. V.Lingamaiah, S. Nikhil, S. Meghana, K. Bhanu Prakash

Assistant Professor, Department of CSE, Anurag University, Hyderabad, India

Department of CSE, Anurag University, Hyderabad, India

ABSTRACT: Election could be a important event during a trendy democracy however massive sections of society round the world don't trust their election system that is major concern for the democracy. Even the world's largest democracies like Republic of India, us, and Japan still suffer from a blemished legal system. Vote rigging, hacking of the EVM (Electronic vote machine), election manipulation, and booth capturing square measure the key problems within the current electoral system. during this system, we tend to square measure work the problems the problems within the election vote systems and attempting to propose the E-voting model which might resolve these issues. The system can highlight a number of the popular blockchain frameworks that provide blockchain as a service and associated electronic E-voting system that is predicated on blockchain that addresses all limitations severally, it additionally preserve participant's obscurity whereas still being hospitable public examination.

Building Associate in Nursing electronic electoral system that satisfies the legal necessities of legislators has been a challenge for an extended time. Distributed ledger technologies is Associate in Nursing exciting technological advancement within the info technology world. Blockchain technologies supply Associate in Nursing infinite vary of applications cashing in on sharing economies.

Blockchain could be a unquiet technology of current era and guarantees to enhance the resilience of e-voting systems. this technique presents a shot to leverage edges of blockchain like cryptological foundations and transparency to attain an efficient theme for e-voting. The projected theme conforms to the elemental necessities for e-voting schemes and achieves end-to-end verifiability. The system presents in-depth analysis of the theme that with success demonstrates its effectiveness to attain Associate in Nursing end-to-end verifiable e-voting theme.

KEYWORDS: Bitcoin, Blockchain technology, cryptographic function, Decentralized application, digital signature, distributed ledger technology (DLT), E- voting, hashing, Merkle tree, time stamp.

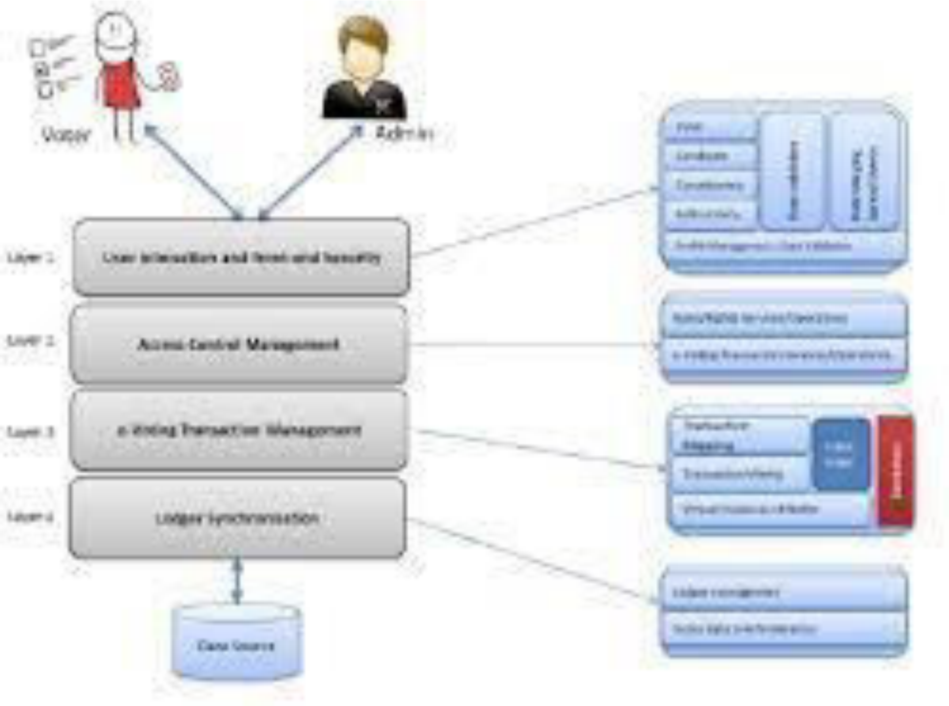
I. INTRODUCTION

Elections are fundamental pillar of a democratic system enabling the general public to express their views in the form of a vote. Due to their significance to our society, the election process should be transparent and reliable so as to ensure participants of its credibility. Within this context, the approach to voting has been an ever evolving domain. This evolution is primarily driven by the efforts to make the system secure, verifiable and transparent. In view of its significance, continuous efforts have been made to improve overall efficiency and resilience of the voting system. Electronic voting or e-voting has a profound role in this. Since its first use as punched-card ballots in 1960's, e-voting systems have achieved remarkable progress with its adaption using the internet technologies. However, e-voting systems must adhere to specific benchmark parameters so as to facilitate its widespread adoption. These parameters include anonymity of the voter, integrity of the vote and non-repudiation among others.

Blockchain is one of the emerging technologies with strong cryptographic foundations enabling applications to leverage these abilities to achieve resilient security solutions. A Blockchain resembles a data structure which maintains and shares all the transactions being executed through its genesis. It is primarily a distributed decentralized database that maintains a complete list of constantly germinating and growing data records secured from unauthorized manipulating, tampering and revision. Blockchain CORE Metadata, citation and similar papers at core.ac.uk Provided by UWL Repository allows every user to connect to the network, send new transactions to it, verify transactions and create new blocks. Each block is assigned a cryptographic hash (which may also be treated as a finger print of the block) that remains valid as long as the data in the block is not altered. If any changes are made in the block, the cryptographic hash would change immediately indicating the change in the data which may be due to a malicious activity. Therefore, due to its strong foundations in cryptography, blockchain has been increasingly used to mitigate against unauthorized transactions across various domains.

II. RELATED WORKS

In (Kiayias & Yung, 2002), a self-tallying voting system is proposed that does not require any trusted third parties for vote aggregation and any private channel for voter- to-voter privacy. The proposed protocol involves extensive computation. In (Hao et al, 2010) a two round protocol is proposed that computes the tally in two rounds without using a private channel or a trusted third party. The protocol is efficient in terms of amputation and bandwidth consumption but is neither robust nor fair in certain conditions (Dalia et al, 2012). In (Dalia et al, 2012) a protocol is proposed to improve the robustness and fairness of the two round protocol (Hao et al, 2010). In (Shahandashti & Hao, 2016), authors propose E2E verifiable voting system named DRE-ip (DRE-in with enhanced privacy), that overcomes limitations of DRE-i (Chaum et al, 2008). Instead of pre-computing ciphertexts, DRE-ip encrypts the vote on the fly during voting process. DRE-ip achieves E2E verifiability without TAs, but at the same time provides a significantly stronger privacy guarantee than DRE-in. In (Chaum, 2004) end-to-end verifiability is achieved through the Mixnet protocol (Chaum, 1981) that recovers the plaintext ballot in an unlikable manner by randomizing the ciphertext through a chain of mix servers. Scantegrity is proposed in (Chaum et al, 2008) that achieves end-to-end (E2E) verifiability with confirmation codes that allow voters to prove to themselves that their ballots are included in the final tally as they really are. Another scheme Prêt à Voter based on (Chaum, 2004) is proposed in (Chaum et al, 2005) that ensures privacy by constructing the ballot with two columns i.e. voting options are listed in one column and the voter's choice is entered in an adjacent column. The work in (Adida & Rivest, 2006) is based on Prêt à Voter but using homomorphic tabulation and it uses scratch stripes to allow off-line auditing of ballots. Other systems that have been proposed for electronic voting include: Bingo Voting (Bohli et al, 2007), Helios (Adida, 2008), DRE- i (Hao et al, 2014) and DRE-ip (Shahandashti & Hao, 2016), Star-Vote (Bell et al, 2013) and (Sandler et al, 2008) to name a few.

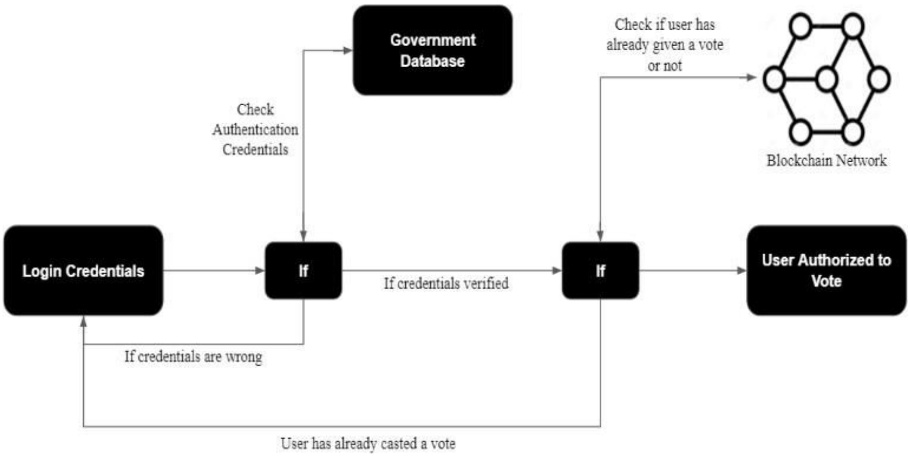


III. EXISTING METHOD

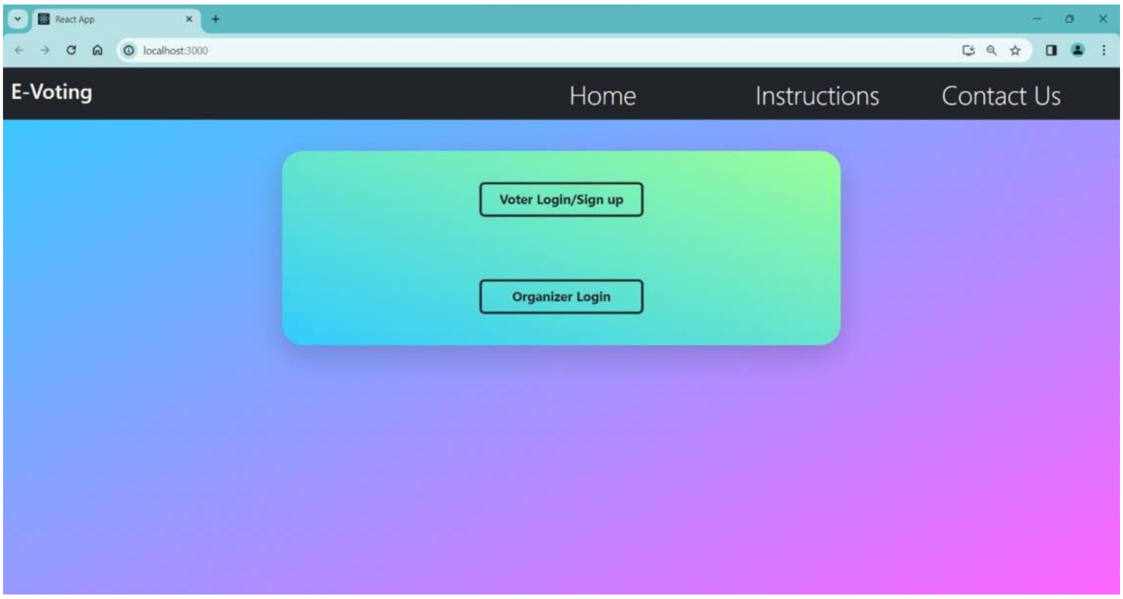
The existing approaches perform well for end-to-end verifiability without compromising the privacy of voters. In (McCorry et al, 2017), authors presented the implementation of decentralized and self-tallying internet voting protocol over the blockchain using Ethereum. Authors used the open vote (Chaum et al, 2008) e-voting approach as their baseline. The focus of our research is to explore the exciting opportunities presented by blockchain technologies by investigating their application in diverse application domains. Within this context, this paper presents our efforts to develop an e-voting system by leveraging blockchain technology. To this end, our proposed scheme fulfils the specific requirements for e-voting as discussed in section 2 and illustrated further in the following sections.

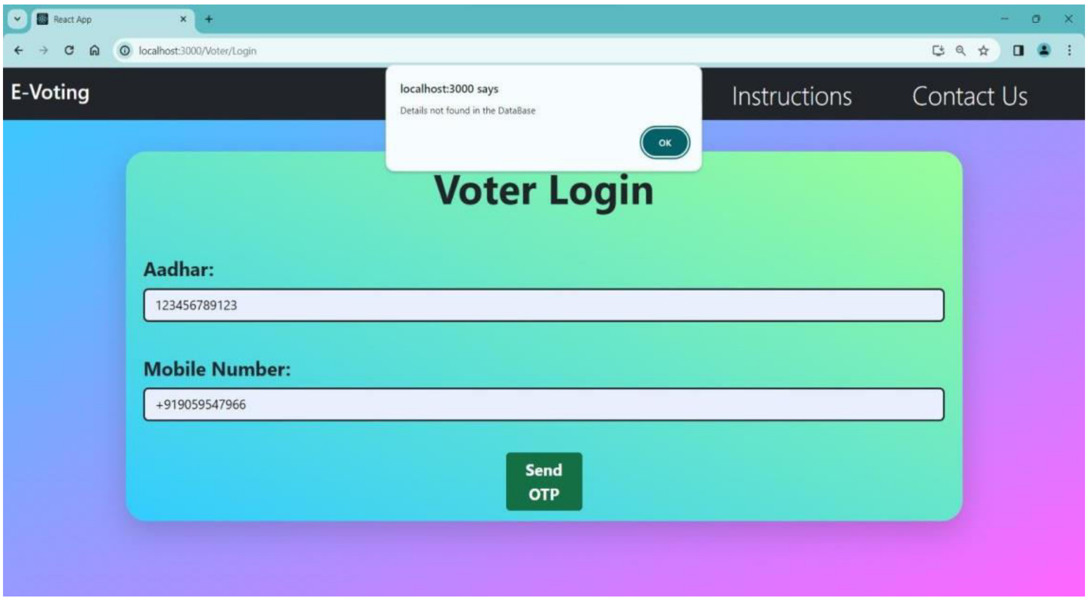
IV. PROPOSED SYSTEM DEISGN

The proposed e-voting system is based on the well-established Prêt à Voter e-voting approach identified in (Ryan, 2008). The system has been designed to support a voting application in the real world environment taking into account specific requirements such as privacy, eligibility, convenience, receiptfreeness and verifiability. The proposed system aims to achieve secure digital voting without compromising its usability. Within this context, the system is designed using a web-based interface to facilitate user engagement with measures such as finger printing to protect against double voting. With a clear need to administer the voters, constituencies and candidates for constituencies, a user-friendly administrator interface is implemented to enable ease of access. Furthermore, the system allows all voters equal rights of participation and develops a fair and healthy competition among all the candidates while keeping the anonymity of the voters preserved. The cryptographic hash of the transaction (ID) is emailed to the voter as a proof that the vote has been casted which may later on be tracked outside the premises of the constituency.



V. RESULTS





localhost:3000/Voter/Login

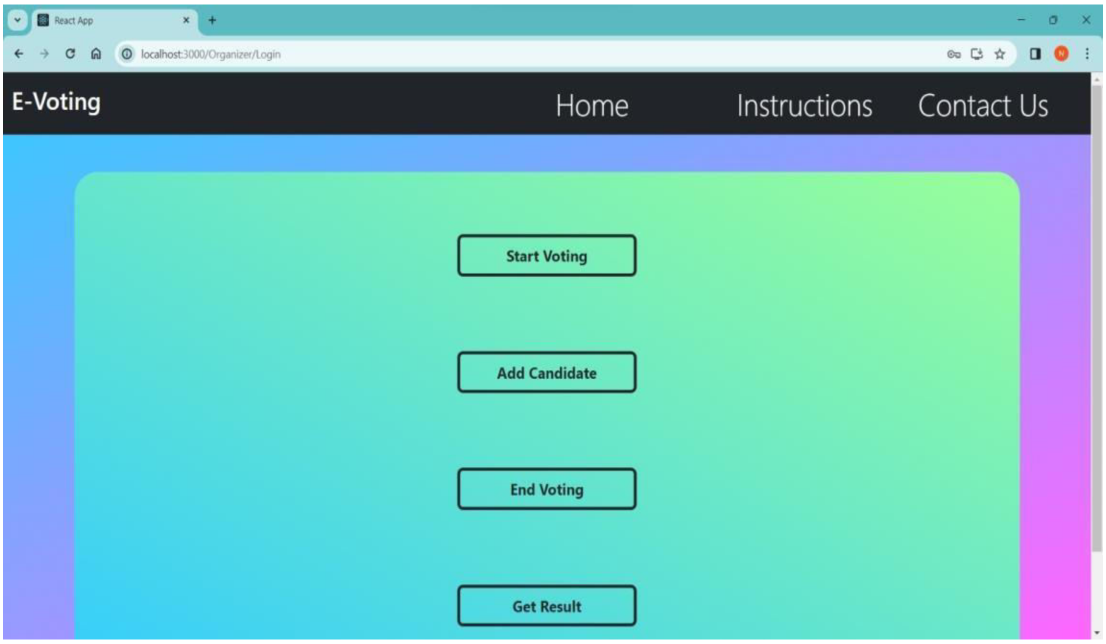
localhost:3000 says

Details not found in the DataBase

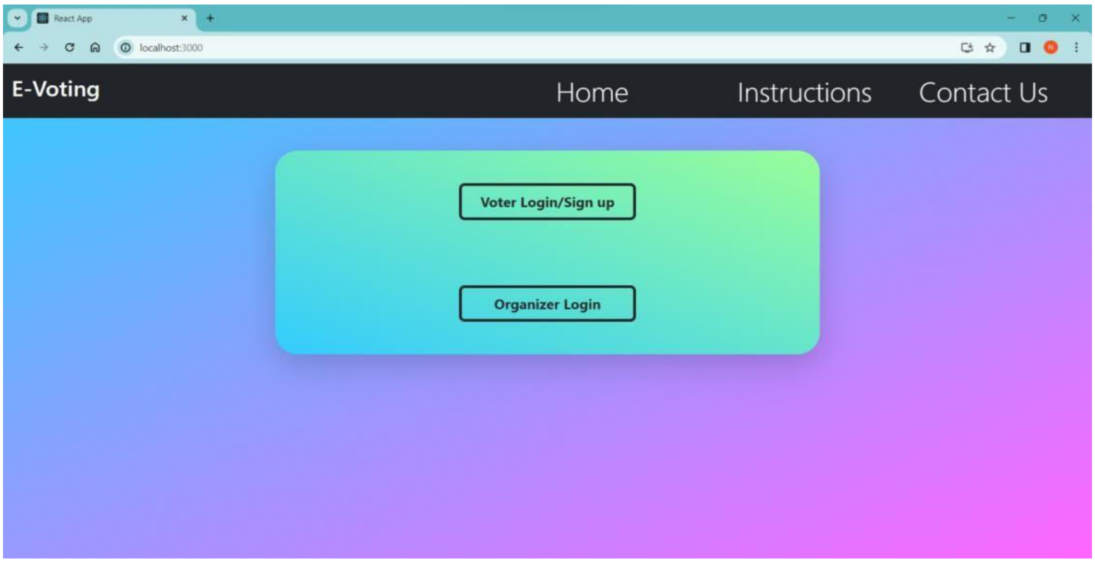
Voter Login

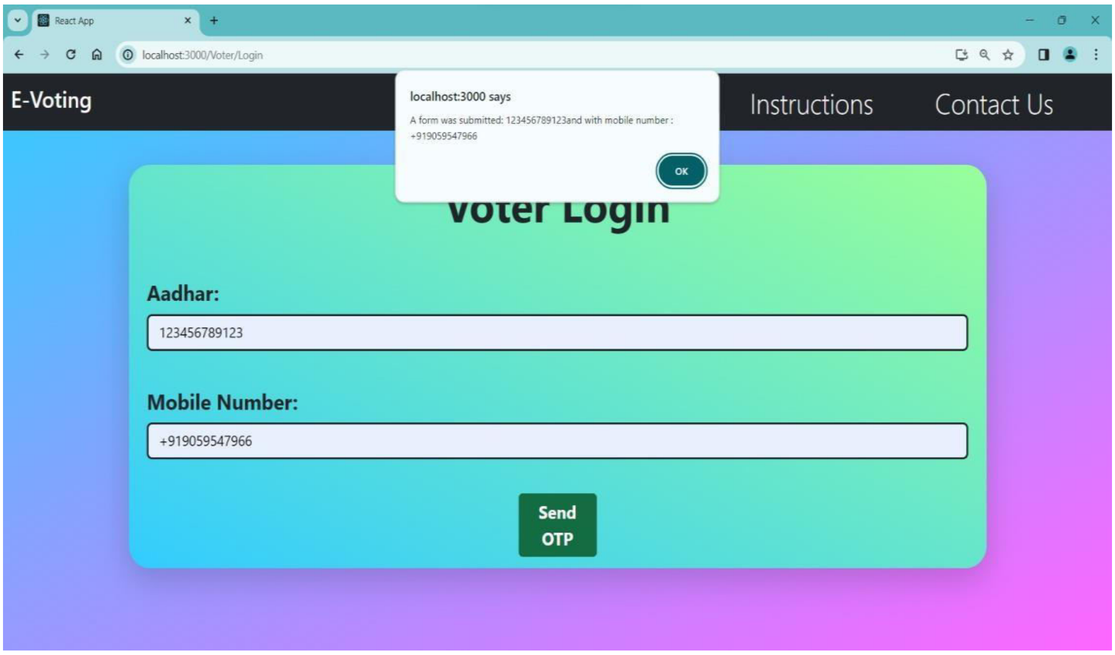
Aadhar: 123456789123

Mobile Number: +919059547966



localhost:3000/Organizer/Login



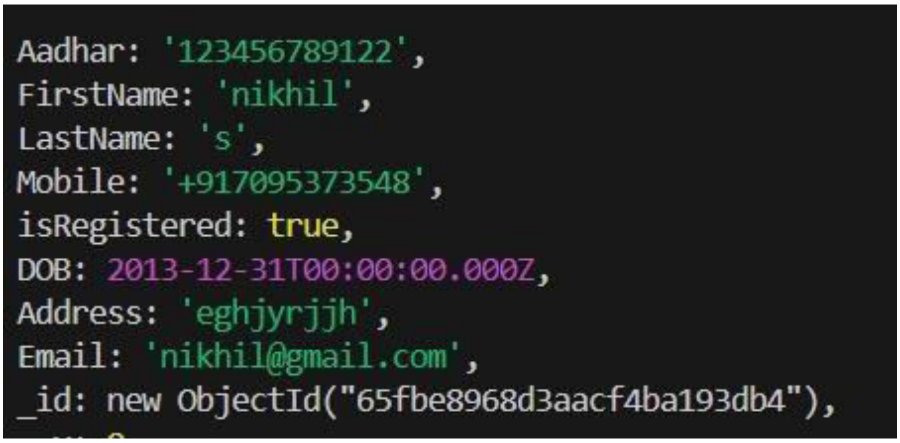


localhost:3000 says

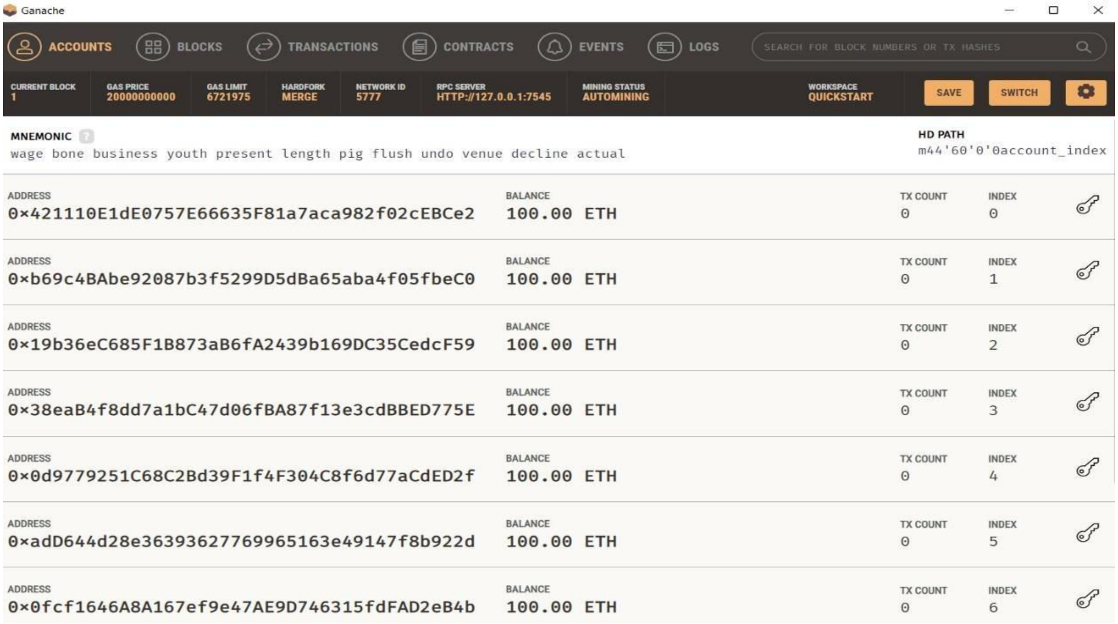
A form was submitted: 123456789123and with mobile number : +919059547966

Aadhar: 123456789123

Mobile Number: +919059547966



```
Aadhar: '123456789122',
FirstName: 'nikhil',
LastName: 's',
Mobile: '+917095373548',
isRegistered: true,
DOB: 2013-12-31T00:00:00.000Z,
Address: 'eghjyrjjh',
Email: 'nikhil@gmail.com',
_id: new ObjectId("65fbe8968d3aacf4ba193db4"),
```



CURRENT BLOCK	GAS PRICE	GAS LIMIT	HARDFORK	NETWORK ID	RPC SERVER	MINING STATUS	WORKSPACE
1	20000000000	6721975	MERGE	5777	HTTP://127.0.0.1:7545	AUTOMINING	QUICKSTART

MNEMONIC
wage bone business youth present length pig flush undo venue decline actual

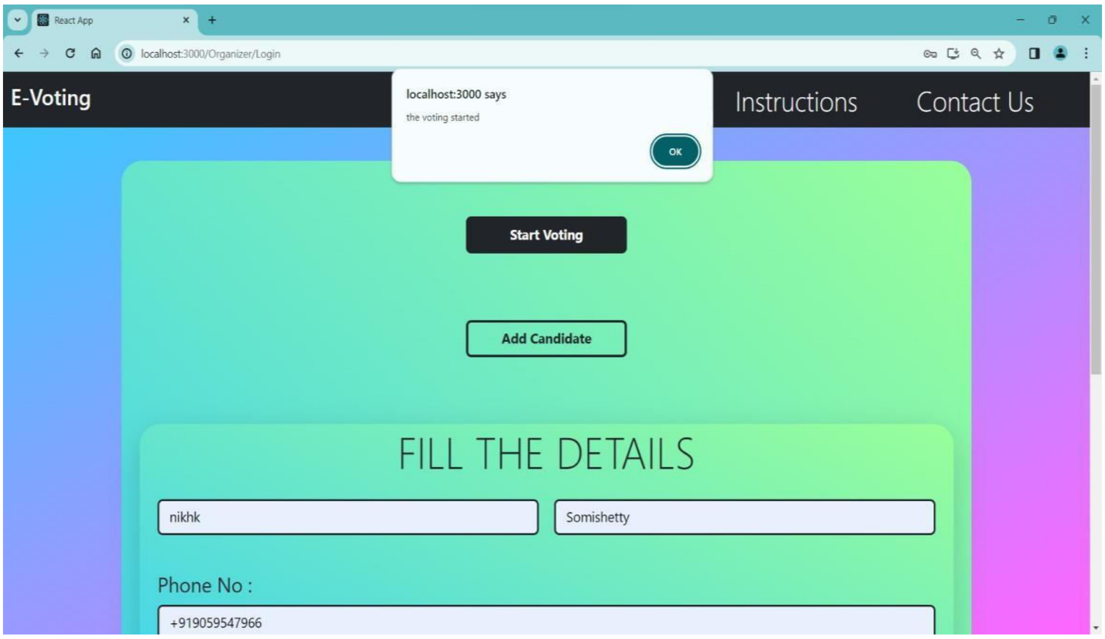
HD PATH
m44'60'0'0account_index

ADDRESS	BALANCE	TX COUNT	INDEX
0×421110E1dE0757E66635F81a7aca982f02cEBCe2	100.00 ETH	0	0
0×b69c4BAbe92087b3f5299D5dBa65aba4f05fbeC0	100.00 ETH	0	1
0×19b36eC685F1B873aB6fA2439b169DC35CedcF59	100.00 ETH	0	2
0×38eaB4f8dd7a1bC47d06fBA87f13e3cdBBED775E	100.00 ETH	0	3
0×0d9779251C68C2Bd39F1f4F304C8f6d77aCdED2f	100.00 ETH	0	4
0×adD644d28e36393627769965163e49147f8b922d	100.00 ETH	0	5
0×0fcf1646A8A167ef9e47AE9D746315fdFAD2eB4b	100.00 ETH	0	6

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

| Volume 7, Issue 3, March 2024 |

| DOI:10.15680/IJMRSET.2024.0703045 |



localhost:3000/Organizer/Login

E-Voting

localhost:3000 says

the voting started

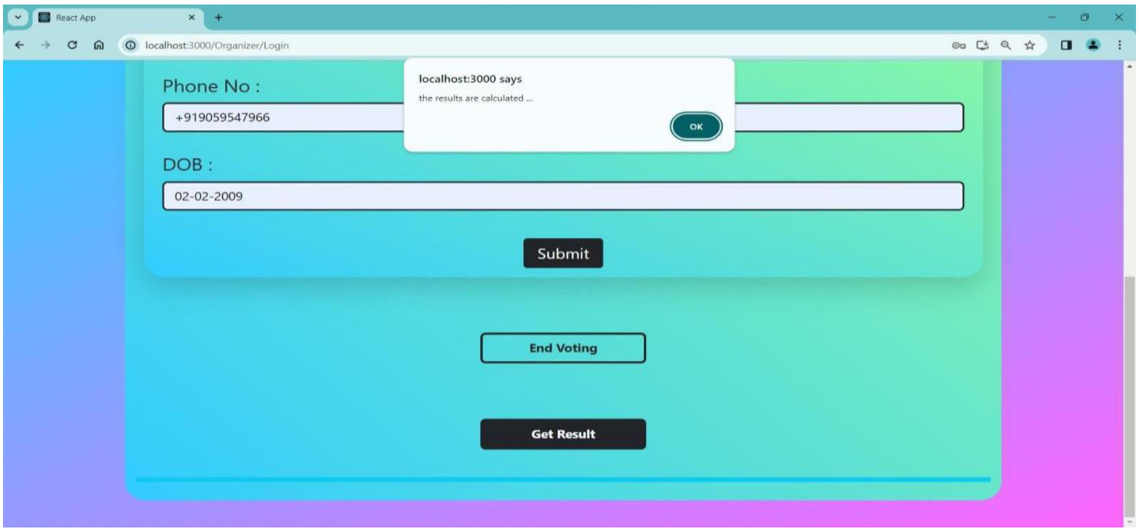
FILL THE DETAILS

nikhk

Somishetty

Phone No :

+919059547966



localhost:3000/Organizer/Login

localhost:3000 says

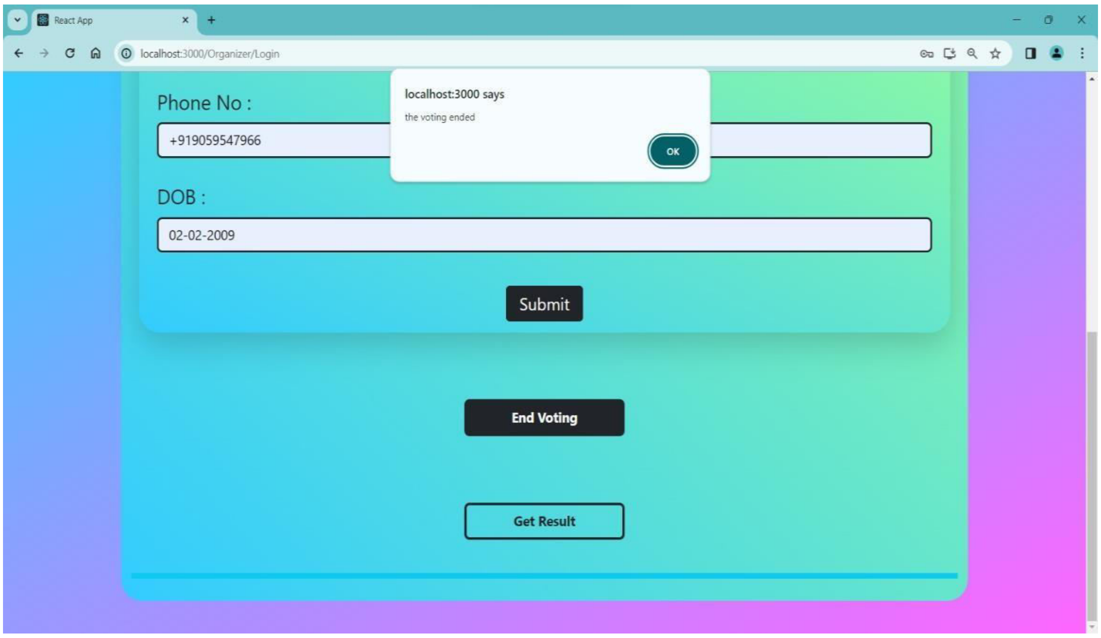
the results are calculated ...

Phone No :

+919059547966

DOB :

02-02-2009



localhost:3000/Organizer/Login

localhost:3000 says

the voting ended

Phone No : +919059547966

DOB : 02-02-2009

VI. CONCLUSION AND FUTURE WORK

Electronic voting has been used in varying forms since 1970s with fundamental benefits over paper based systems such as increased efficiency and reduced errors. With the extraordinary growth in the use of blockchain technologies, a number of initiatives have been made to explore the feasibility of using blockchain to aid an effective solution to e-voting. This paper has presented one such effort which leverages benefits of blockchain such as cryptographic foundations and transparency to achieve an effective solution to e-voting. The proposed approach has been implemented with Multichain and in- depth evaluation of approach highlights its effectiveness with respect to achieving fundamental requirements for an e-voting scheme. In continuation of this work, we are focused at improving the resistance of blockchain technology to ‘double spending’ problem which will translate as ‘double voting’ for e-voting systems. Although blockchain technology achieves significant success in detection of malleable change in a transaction however successful demonstration of such events have been achieve which motivates us to investigate it further. To this end, we believe an effective model to establish trustworthy provenance for e-voting systems will be crucial to achieve an end- to-end verifiable e-voting scheme. The work to achieve this is underway in the form of an additional provenance layer to aid the existing blockchain based infrastructure

REFERENCES

1. 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. 335{348.
2. Adida B. and Rivest, R. L. (2006). Scratch & 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.
3. 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,

4. in 2013 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 13). Washington, D.C.: USENIX Association, 2013.
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. Chaum, D., Essex, A., Carback, R., Clark, J., Popoveniuc, S., Sherman, A. and Vora,
7. P. (2008) Scantegrity: End-to-end voter-veri_able optical- scan voting, IEEE Security Privacy, vol. 6, no. 3, pp. 40-46, May 2008.
8. Chaum, D. (2004) Secret-ballot receipts: True voter-verifiable elections, IEEE Security Privacy, vol. 2, no. 1, pp. 38{47, Jan 2004.
9. Chaum, D. (1981) Untraceable electronic mail, return addresses, and digital pseudonym', Commun. ACM, vol. 24, no. 2, pp. 84{90, Feb. 1981.
10. Chaum, D., Ryan, P. Y. A. and Schneider, P. Y. A. (2005). A practical voter-verifiable election scheme, in Proceedings of the 10th European Conference on Research in Computer Security, ser. ESORICS'05. Berlin, Heidelberg: Springer-Verlag, 2005, pp. 118- 139.
11. 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.
12. Hao, F., Kreeger, M. N., Randell, B., Clarke, D., Shahandashti, S. F. and Lee, P. H.-J. (2014). Every vote counts: Ensuring integrity in large-scale electronic voting, in 2014

INNO SPACE
SJIF Scientific Journal Impact Factor
Impact Factor
7.521

INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

निस्केयर
NISCAIR

INTERNATIONAL JOURNAL OF MULTIDISCIPLINARY RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

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

www.ijmrset.com