




An IoT Application Based Decentralized Electronic Voting System Using Blockchain

Yash Gupta¹, Rishabh Verma¹, S. S. P. M. B. Sharma², and Indrajeet Kumar¹ (✉) 

¹ School of CSIT, Symbiosis University of Applied Sciences, Indore, India
indrajeetnitp2050@gmail.com

² School of MT, Symbiosis University of Applied Sciences, Indore, India

Abstract. In 21st century, there is huge political unrests among political leaders in many developing countries, in spite of Boom of Internet users, still the elections are held in semi-old fashion. The cost associated with these elections (i.e. appliances, workforce related, transport etc.) act as burden on tax payer's money & cuts the huge possibilities of R&D in any nation. Specially in south-east nations, Indians (NRIs) move abroad for various reasons; To demonstrate the feasibility of our protocol in real-world scenarios, we have implemented it using Ethereum's blockchain as a public bulletin board. As a result, casting vote for them becomes very difficult, hence we created mechanism where NRIs can vote securely using their passports.

Keywords: Arduino · Blockchain LDR · Eye Blink Sensor · Ultrasonic Sensor

1 Introduction

Originally, blockchain was just known to some CS fellows & researchers for how to structure & share data. Today blockchains are hailed the “5th evolution” [1] of computing. Blockchain (Blockchain) in a Network, where Block allude to the list of transactions noted into distributed ledgers over a given period of time. It has three main components i.e., Size, Period, & Trigger Event [2–5] for each block. Chain alludes to a hash that associates one block to another. It's also the magic that glues blockchains together & allowed them to define mathematical trust. Network [6–8] is composed of “full nodes”. A blockchain is a kind of data structure that makes it possible to create a digital distributed ledger of data & share it among a network of independent parties [9–12]. Blockchain is mainly classified into 3 major types i.e., Public: very large distributed networks running through a native cryptocurrency mostly Bitcoin, Ethereum. Fully Open Source. Permissioned [13] Large distributed network; control roles for individuals within network. Private: Distributed Ledger Tech i.e., smaller & no token nor any cryptocurrency required [14].

The main reason why blockchain becomes word of mouth so quickly is the “Consensus”. As mentioned in Fig. 1, the consensus blockchain creates honest systems where they self-correct themselves (i.e., nodes in a network) without any third-party monitoring [15]. This consensus algorithm is the process of creating an accord or concurrence among group of commonly distrustful shareholders.

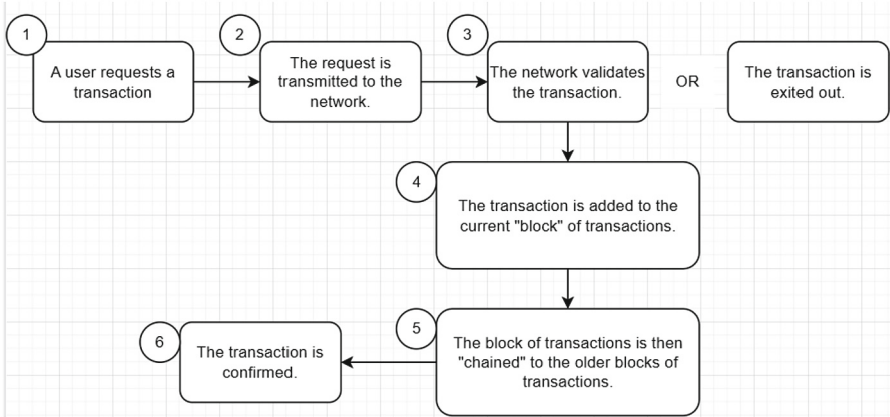


Fig. 1. Process of Consensus Algorithm for e- voting system using blockchain.

Blockchains are also now being used in various industries such as Security: To counter code piracy, securing IOT devices from spoofing & hacking [16–20]. One of the significant advantages of MIMO for IoT is its ability to provide improved connectivity and extended coverage [21–25]. By employing multiple antennas, MIMO systems can mitigate the effects of multipath fading and enhance signal reception in challenging environments [26]. This capability is particularly crucial for IoT devices deployed in complex urban settings or harsh industrial environments, where reliable connectivity is vital for seamless data transmission and reception [27]. Government-Agencies: Maintaining shatterproof Land-Record Systems. ICOs: Smart Contract that allows the issuer to grant token for Investment-Funds related to Banks [28, 29]. The Existing System of general public election is running manually [30–34]. The Voter has to Visit to Booth to cast their votes. As a result, many people don't go out to cast their vote which is one of the major drawbacks of current voting system. In democracy, every citizen of a country must vote [25]. By a new online system which will limit the voting frauds and make the voting as well as counting more efficient and transparent.

The remaining sections of the paper are organized as follows: The subsequent section offers the necessary background information to comprehend the proposed work, including a discussion on similar studies conducted by other researchers and the gaps present in their research. Section 2 outlines the specific work proposed in this paper and provides details on the design of the system. Section 3 presents the implementation of the E-voting system, accompanied by an illustrative example that demonstrates how the system functions. Lastly, Sect. 4 concludes the study by providing a summary of the current progress and outlining plans for future work.

2 System Model

In Fig. 2, we are explaining the complete architecture CodeFlow of our decentralized E-Voting application using Hardhat as blockchain platform [12]. Here, in Front-End Part we designed 3 ways i.e. User can login using web application, mobile application or even

via SMS Gateway (for Tier-2 & Tier-3 cities). Also, NRIs can login with passport login, while others can login with MetaMask wallet [13]. After successful login, we can create voter's & candidates. As MetaMask is verified, voter registration can be accepted and also, we can see the voter list [14]. In create new voter, voter can upload photo, user name, address of MetaMask, age. By using hardhat blockchain - block I is connected to Block II and so on [15]. Hardhat blockchain is connected to MongoDB for NRI users and distributed ledger are created. Event Management Server is connected to Etherscan [16] block explorer and analytics platform for Ethereum. All of the process of authentication the Administrator can have all access to allow list of voters and have all the rights for the security reasons. We setup MongoDB Compass as distributed ledger cluster in which each node has its own ledger for maintaining the entire state of cluster as it works on Consensus algorithm.

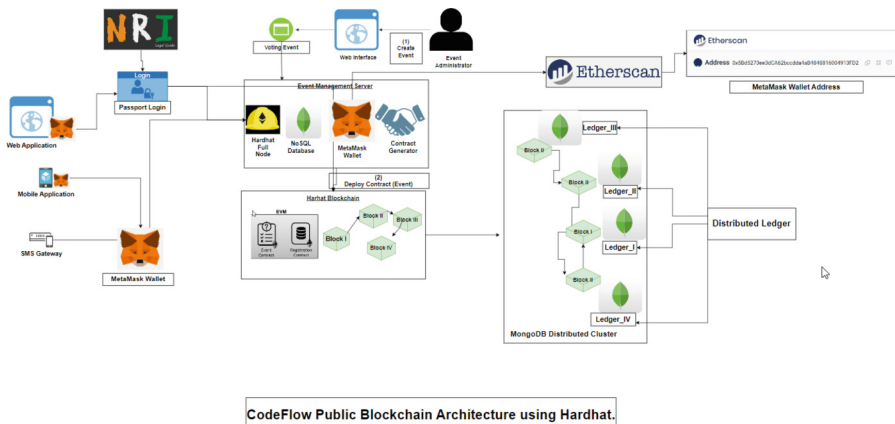


Fig. 2. Showing entire Code flow using Hardhat

As shown in Fig. 3, we explained our Full-Stack directory-level tree structure where we created directories i.e., assets, components, context, contracts, pages, scripts, styles, test & configs [17]. In components, we have NavBar, voter Card which includes NavBar.js, voterCard.js & NavBar.module.css etc. In context we created Voter.js, constants.js & Create.json etc. In pages directory, we created candidate_registration.js, _app.js, allowed-voters.js, voterList.js etc. In scripts we created deploy.js. Under styles directory, we created allowedVoter.module.css, globals.module.css, index.module.css, voterList.module.css. In test directory, we created Lock.js file. In configs file, we hardhat.config.js, next.config.js, package.json, package-lock.json. There are multiple dependencies used in this project such as openzeppelin, axios, ethers, hardhat, ipfs-http-client, dot-env, web3modal [18].

As shown in Fig. 4, we explained our entire directory-level tree structure where we created directories i.e., configs, data, server & views. In server directory we created database.js, server.js & passportConfig.js. Inside database.js file we created the database schema which contains all the collection name & their datatype. We have three main fields i.e., passport_no, name, email-id & password. In views directory, we created index.ejs,

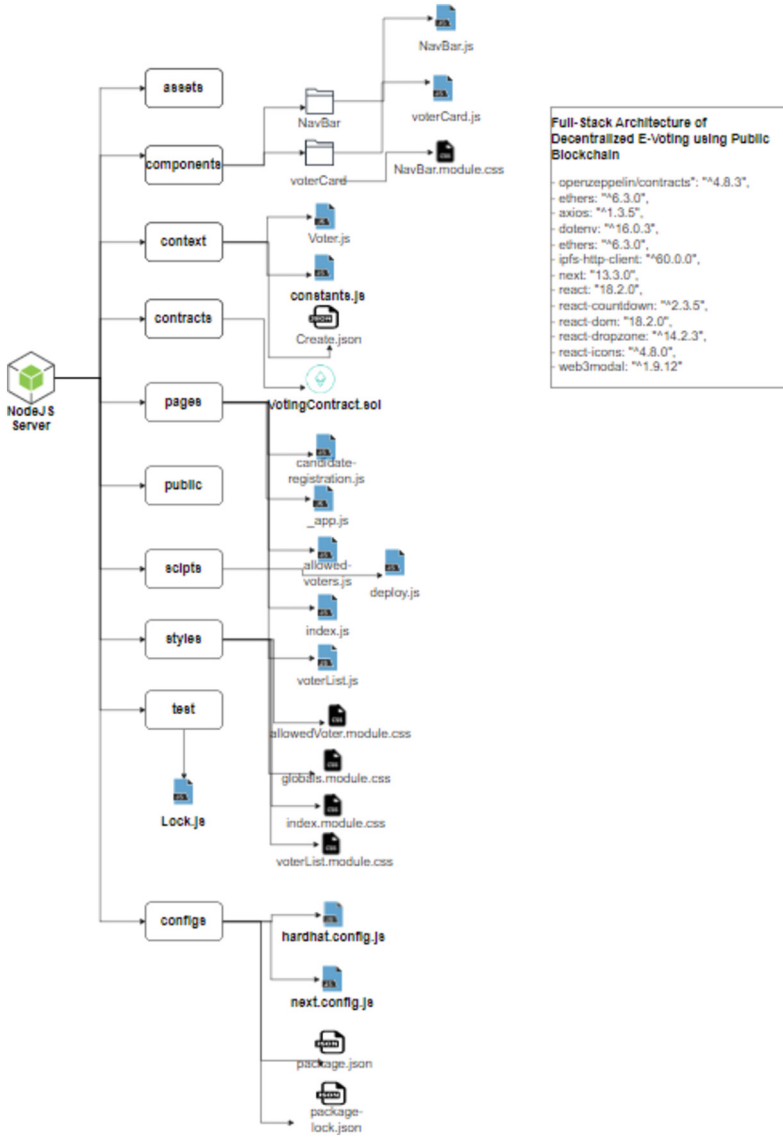


Fig. 3. Showing entire directory structure of project

login.ejs & register.ejs. The .ejs extension is embedded javascript file. In scripts we created deploy.js. In configs file, we created package.json, package-lock.json. There are multiple dependencies used in this project such as ejs, express, express-session, local, mongoose, nodemon, passport, passport-local etc.

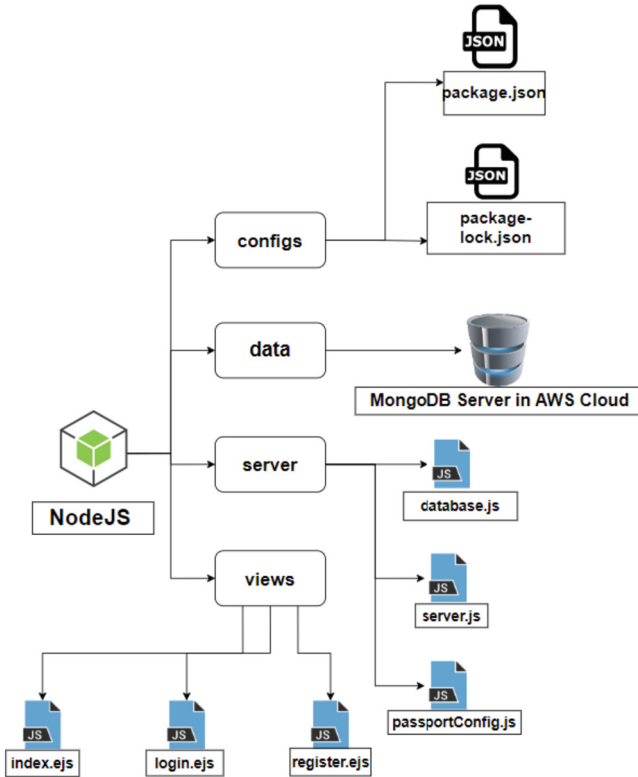


Fig. 4. Showing entire directory structure of passport authentication system for NRIs login

3 Simulation Results

As shown in Fig. 5, we are connecting with MetaMask Account by clicking on Connect Wallet. Then, MetaMask will connect it to Etherscan by calling API mentioned in context/constanst.js. In simple terms, the explanation states that in Fig. 5, a process is depicted where we establish a connection with a MetaMask Account. This connection is established by clicking on the “Connect Wallet” option. MetaMask, which is a digital wallet used for interacting with blockchain networks, then connects to Etherscan, a popular blockchain explorer, by making use of an application programming interface (API) mentioned in the context/constanst.js file.

As displayed in Fig. 6, now we are using candidate-register.js file for registering our candidate. Also, in the figure it is showing No. of Candidate’s & No. of Voter’s in this page.

In Fig. 7, we have created a web form which takes name of candidate, Address from which location it belongs & for the post he/she is contesting for. Here, candidate can also upload his/her image.

In Fig. 8, candidate is selecting his/her photo by using index.js file & uploading images present in assets directory. Also, these images are stored in local database (Fig. 9).

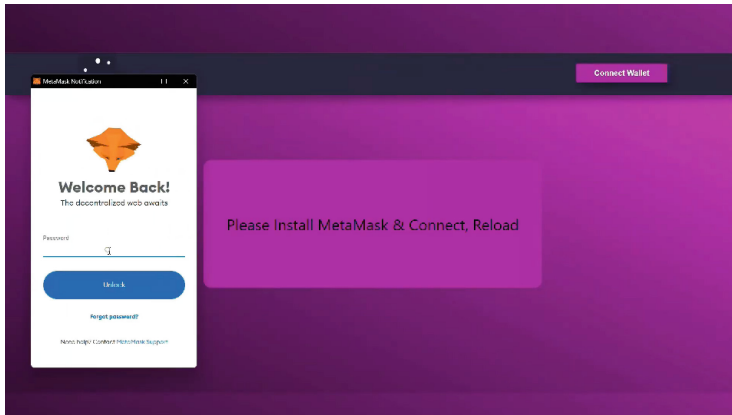


Fig. 5. Picture depicting Connection with MetaMask.

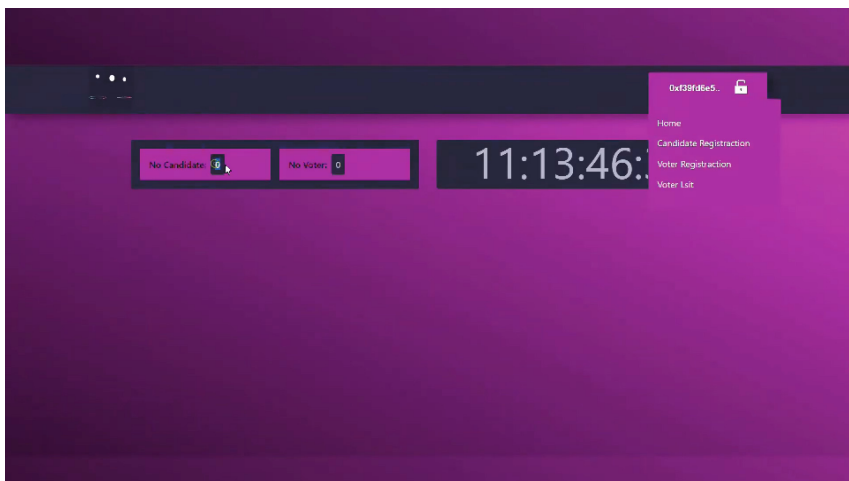


Fig. 6. Selecting option of Candidate Registration

As name, address & position, candidate clicked on Authorized Candidate. After that, MetaMask wallet address with registered account gets initiated & Ethereum (ETH) gas fee gets deducted from MetaMask wallet.

In this Fig. 10, we successfully registered our candidate, also the status of Number of Candidates gets incremented by one.

In the Fig. 11, after filling all the form details such as name, address & age, voter clicks on Authorized Voter.

In above Fig. 12, the Voter is created successfully, yet he/she hasn't voted i.e., displayed as Not Voted. This method of contract is coded in VotingContract.sol file under contracts directory.

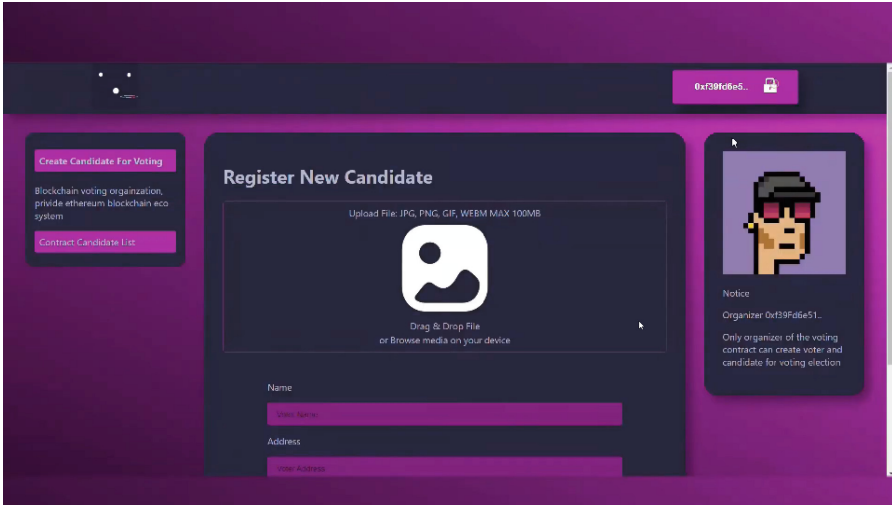


Fig. 7. Register New Candidate by filling Name, Address, Position etc.

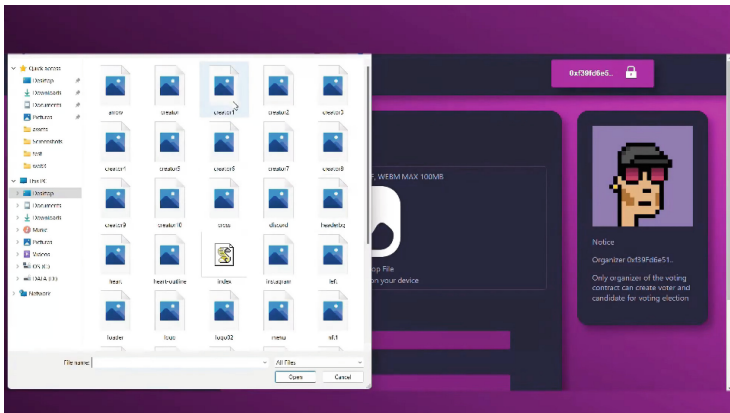


Fig. 8. Select 'Candidate Photo' for upload

As mentioned in Fig. 13, MetaMask wallet address with registered account gets initiated & Ethereum (ETH) gas fee gets deducted from MetaMask wallet as voter clicks on Confirm button. The vote gets casted. All these transaction histories can be seen in Etherscan platform.

As shown in Fig. 14, the status of voter from Not Voted to You Already Voted gets changed. The time taken by showing this status is very less.

Hardcoding a single vote: Within the “Voting Contract.sol” file, it is hardcoded or explicitly defined that each voter can only cast a single vote. This means that once a voter has cast their vote, they cannot cast another vote using the same wallet address associated with their unique private key. Unique wallet address and private key: Each voter is assigned a unique wallet address, which is associated with their private key.

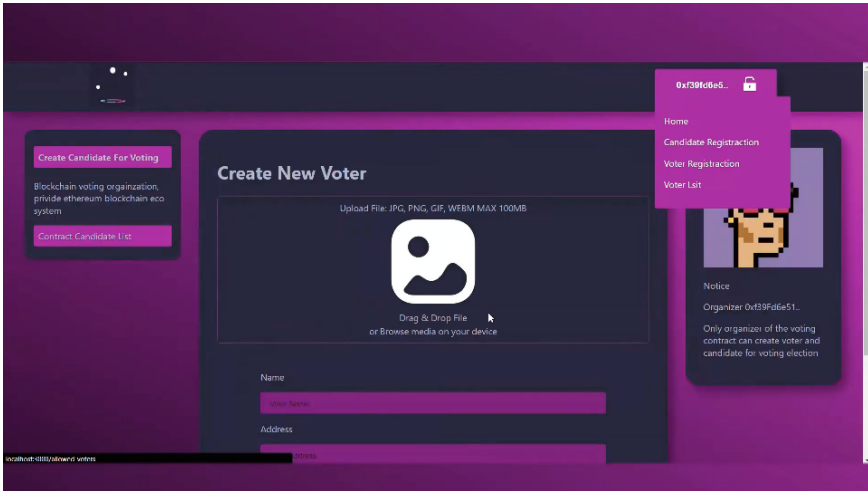


Fig. 11. Create New Voter by filling Name, Address, Age.

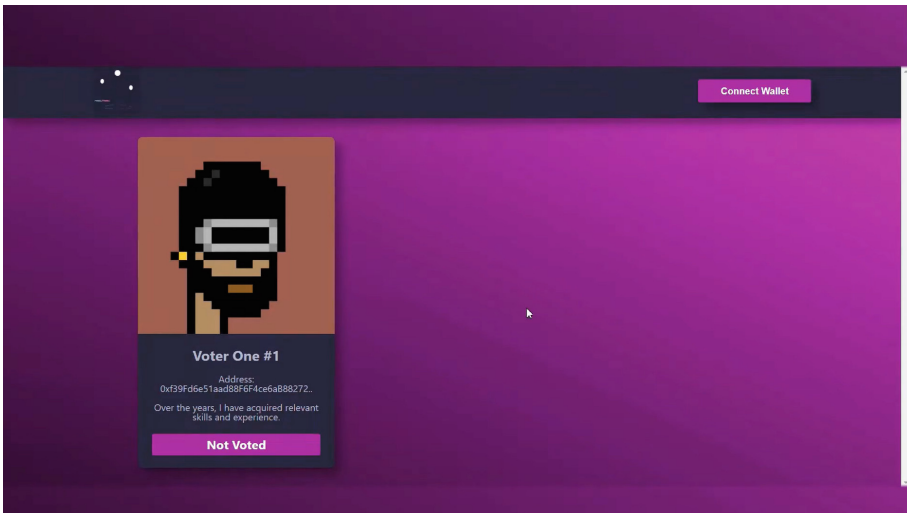


Fig. 12. Page showing status of Voter_One#1 i.e. Not Voted.

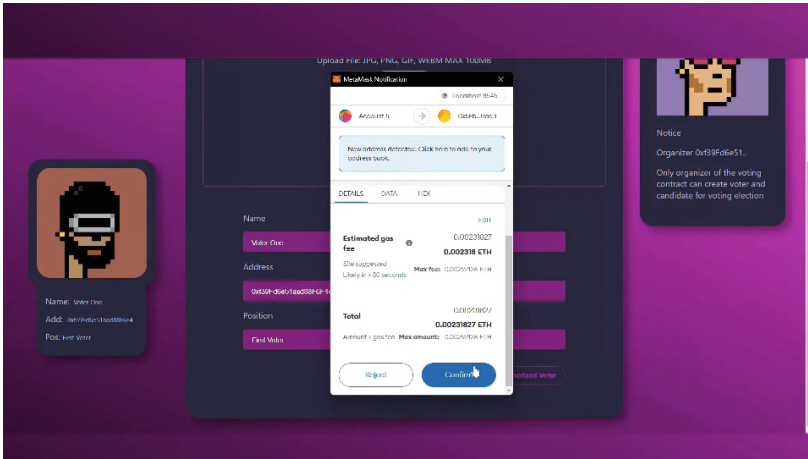


Fig. 13. Voter successfully casted his vote.

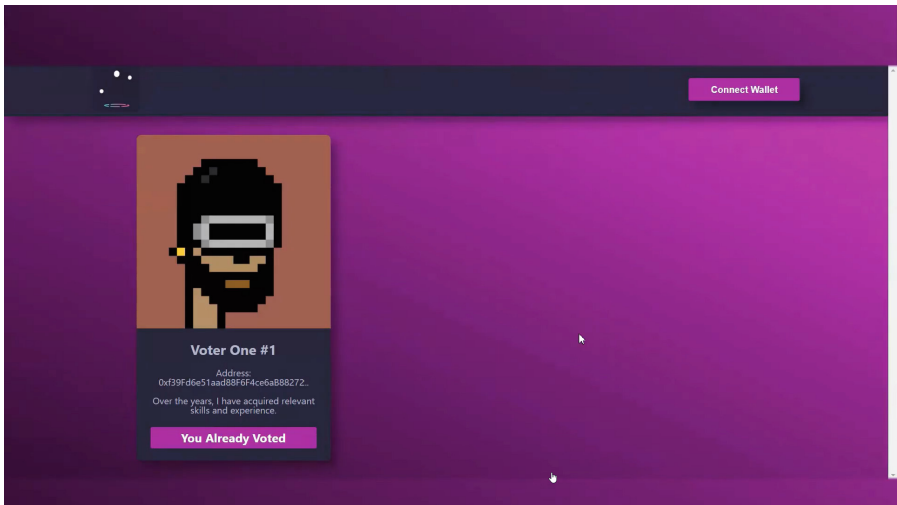


Fig. 14. Page showing status of Voter_One#1's vote i.e. You Already Casted.

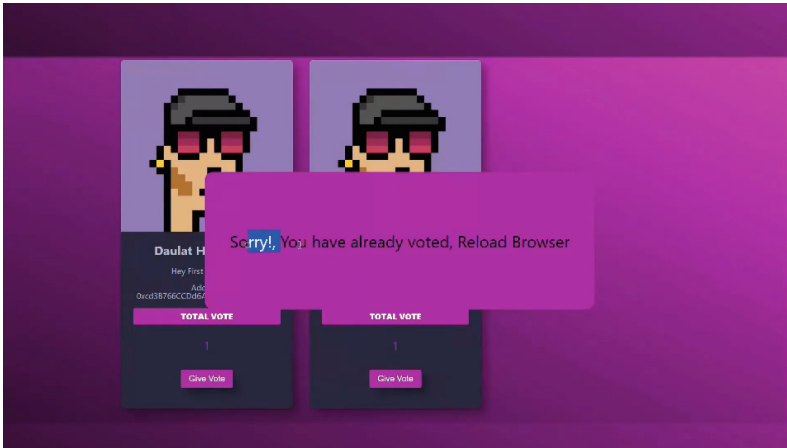


Fig. 15. You Already Voted status so that One Person, One Vote.

4 Conclusion

Blockchain technology has the potential to revolutionize various sectors and services by reducing the initial cost of investment and improving performance in specific areas. One notable application of blockchain technology is in the realm of voting systems. By using BCT individual's vote privacy can be kept secret. Voters can give their vote at their ease of space or according to their comfort zone. Voting system can be helpful for giving vote in the elections happened in the colleges etc. Block chain technology reduces the errors at the time of vote counting. Online voting system will able to take care the voter's information where voter can have access and use their voting rights. Our research paper concludes that usefulness or ease of use are still important to decision makers while implementing EVs, but our research shows that building trust faith is prime.

References

1. Rathee, G., Iqbal, R., Waqar, O., Bashir, A.K.: On the design and implementation of a blockchain enabled e-voting application within IoT-oriented smart cities. *IEEE Access* **9**, 34165–34176 (2021). <https://doi.org/10.1109/ACCESS.2021.3061411>
2. Vladucu, M.-V., Dong, Z., Medina, J., Rojas-Cessa, R.: E-voting meets blockchain: a survey. *IEEE Access* **11**, 23293–23308 (2023). <https://doi.org/10.1109/ACCESS.2023.3253682>
3. Li, H., Li, Y., Yu, Y., Wang, B., Chen, K.: A blockchain-based traceable self-tallying E-voting protocol in AI era. *IEEE Trans. Network Sci. Eng.* **8**(2), 1019–1032 (2021). <https://doi.org/10.1109/TNSE.2020.3011928>
4. Zhang, X., Zhang, B., Kiayias, A., Zacharias, T., Ren, K.: An efficient E2E crowd verifiable E-voting system. *IEEE Trans. Depend. Secure Comput.* **19**(6), 3607–3620 (2022). <https://doi.org/10.1109/TDSC.2021.3103336>
5. Gao, S., Zheng, D., Guo, R., Jing, C., Hu, C.: An anti-quantum E-voting protocol in blockchain with audit function. *IEEE Access* **7**, 115304–115316 (2019). <https://doi.org/10.1109/ACCESS.2019.2935895>

6. Panizo Alonso, L., Gascó, M., Marcos del Blanco, D.Y., Hermida Alonso, J.Á., Barrat, J., Aláiz Moreton, H.: E-voting system evaluation based on the council of europe recommendations: helios voting. *IEEE Trans. Emerg. Top. Comput.* **9**(1), 161–173 (2021). <https://doi.org/10.1109/TETC.2018.2881891>
7. Villafiorita, A., Weldemariam, K., Tiella, R.: Development, formal verification, and evaluation of an E-voting system with VVPAT. *IEEE Trans. Inf. Forensics Secur.* **4**(4), 651–661 (2009). <https://doi.org/10.1109/TIFS.2009.2034903>
8. Benabdallah, A., Audras, A., Coudert, L., El Madhoun, N., Badra, M.: Analysis of blockchain solutions for E-voting: a systematic literature review. *IEEE Access* **10**, 70746–70759 (2022). <https://doi.org/10.1109/ACCESS.2022.3187688>
9. Oprea, S.-V., Băra, A., Andreescu, A.-I., Cristescu, M.P.: Conceptual architecture of a blockchain solution for E-voting in elections at the university level. *IEEE Access* **11**, 18461–18474 (2023). <https://doi.org/10.1109/ACCESS.2023.3247964>
10. Zaghoul, E., Li, T., Ren, J.: D-BAME: distributed blockchain-based anonymous mobile electronic voting. *IEEE Internet Things J.* **8**(22), 16585–16597 (2021). <https://doi.org/10.1109/JIOT.2021.3074877>
11. Al-madani, A.M., Gaikwad, A.T.: Iot data security via blockchain technology and service-centric networking. In: 2020 International Conference on Inventive Computation Technologies (ICICT), pp. 17–21. IEEE (2020)
12. Al-madani, A.M., Gaikwad, A.T., Mahale, V., Ahmed, Z.A.T.: Decentralized e-voting system based on smart contract by using blockchain technology. In: 2020 International Conference on Smart Innovations in Design, Environment, Management, Planning and Computing (ICSIDEMPC), pp. 176–180. IEEE (2020)
13. Ayed, A.B.: A conceptual secure blockchain-based electronic voting system. *Int. J. Network Secur. Appl.* **9**(3), 01–09 (2017)
14. Bell, S., et al.: STAR-Vote: a secure, transparent, auditable, and reliable voting system. In: 2013 Electronic Voting Technology Workshop/Workshop on Trustworthy Elections (EVT/WOTE 13). USENIX Association, Washington, D.C. (2013)
15. Bohli, J.-M., Müller-Quade, J., Röhricht, S.: Bingo voting: secure and coercionfree voting using a trusted random number generator. In: Alkassar, A., Volkamer, M. (eds.) *E-Voting and Identity. Vote-ID 2007*. LNCS, vol. 4896. Springer, Berlin, Heidelberg (2007). https://doi.org/10.1007/978-3-540-77493-8_10
16. C. abuk, U.C., Adiguzel, E., Karaarslan, E.: A survey on feasibility and suitability of blockchain techniques for the e-voting systems. *arXiv preprint arXiv:2002.07175* (2020)
17. Canessane, R.A., Srinivasan, N., Beuria, A., Singh, A., Kumar, B.M.: Decentralised applications using ethereum blockchain. In: 2019 Fifth International Conference on Science Technology Engineering and Mathematics (ICONSTEM), vol. 1, pp. 75–79. IEEE (2019)
18. Chaum, D.: Secret-ballot receipts: true voter-verifiable elections. *IEEE Secur. Priv.* **2**(1), 38–47 (2004)
19. Chaum, D., et al.: Scantegrity: end-to-end voter-verifiable optical-scan voting. *IEEE Secur. Priv.* **6**(3), 40–46 (2008)
20. Chaum, D., Ryan, P.Y.A., Schneider, S.: A practical voter-verifiable election scheme. In: de Capitani, S., di Vimercati, P., Syverson, D.G. (eds.) *Computer Security – ESORICS 2005: 10th European Symposium on Research in Computer Security*, Milan, Italy, September 12–14, 2005. Proceedings, pp. 118–139. Springer Berlin Heidelberg, Berlin, Heidelberg (2005). https://doi.org/10.1007/11555827_8
21. Shankar, R., Kumar, I., Mishra, R.K.: Outage probability analysis of MIMO-OSTBC relaying network over Nakagami-m fading channel conditions. *Traitement du Signal* **36**(1), 59–64 (2019). <https://doi.org/10.18280/ts.360108>

22. Kumar, I., Mishra, M.K., Mishra, R.K.: Performance analysis of NOMA downlink for next-generation 5G network with statistical channel state information. *Ingénierie des systèmes d'information* **26**(4), 417–423 (2021). <https://doi.org/10.18280/isi.260410>
23. Shankar, R., Kumar, I., Mishra, R.: Pairwise error probability analysis of dual hop relaying network over time selective Nakagami-m fading channel with imperfect CSI and node mobility. *Traitement du Signal* **36**(3), 281–295 (2019). <https://doi.org/10.18280/ts.360312>
24. Kumar, I., Kumar, A., Mishra, R.K.: Performance analysis of cooperative NOMA system for defense application with relay selection in a hostile environment. *J. Defense Model. Simul. Appl. Methodol. Technol.* **20**(4), 553–561 (2022). <https://doi.org/10.1177/15485129221079721>
25. Ashish, Kumar, I., Mishra, R.K.: Performance analysis for wireless non-orthogonal multiple access downlink systems. In: 2020 International Conference on Emerging Frontiers in Electrical and Electronic Technologies (ICEFEET), pp. 1–6. Patna, India (2020). <https://doi.org/10.1109/ICEFEET49149.2020.9186987>
26. Kumar, I., Mishra, R.K.: An investigation of spectral efficiency in linear MRC and MMSE detectors with perfect and imperfect CSI for massive MIMO systems. *Traitement du Signal* **38**(2), 495–501 (2021). <https://doi.org/10.18280/ts.380229>
27. Kumar, I., Mishra, R.: An efficient ICI mitigation technique for MIMO-OFDM system in time-varying channels. *Mathematical Modelling of Engineering Problems* **7**(1), 79–86 (2020). <https://doi.org/10.18280/mmep.070110>
28. Gupta, N., Kumar, I., Rathod, I., Sharma, B.S.S.P.M.: Sustainable production systems with ai and emerging technologies: a moderator-mediation analysis, vol. 12, Special Issue-8, pp. 2819–2832 (2023). <https://doi.org/10.48047/ecb/2023.12.si8.200>. 2023
29. Chaum, D.L.: Untraceable electronic mail, return addresses, and digital pseudonyms. *Commun. ACM* **24**(2), 84–90 (1981)
30. Dhinakaran, K., Britto Hrudaya Raj, P.M., Vinod, D.: A secure electronic voting system using blockchain technology. In: Goyal, D., Gupta, A.K., Piuri, V., Ganzha, M., Paprzycki, M. (eds.) *Proceedings of the Second International Conference on Information Management and Machine Intelligence. LNNS*, vol. 166, pp. 307–313. Springer, Singapore (2021). https://doi.org/10.1007/978-981-15-9689-6_34
31. Erdenebileg, M.: e-voting anwendung auf ethereum plattform als smart contract. *Fachhochschule Campus Wien* (2019)
32. Hanifatunnisa, R., Rahardjo, B.: Blockchain based e-voting recording system design. In: 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA), pp. 1–6. IEEE (2017)
33. Hj´almarsson, F., Hreiðarsson, G.K., Hamdaqa, M., Hj´almt´ysson, G´.: Blockchain-based e-voting system. In: 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), pp. 983–986 (2018)
34. Pareek, P., Maurya, N.K., Singh, L., Gupta, N., Reis, M.J.C.S.: Study of smart city compatible monolithic quantum well photodetector. In: Gupta, N., Pareek, P., Reis, M. (eds.) *Cognitive Computing and Cyber Physical Systems. IC4S 2022. LNICS, Social Informatics and Telecommunications Engineering*, vol. 472. Springer, Cham (2023). https://doi.org/10.1007/978-3-031-28975-0_18
35. Sharma, B.S.S.P.M., Ravishankar Kamath, H., Siva Brahmaiah Rama, V.: Modelling of cloud based online access system for solar charge controller *Int. J. Eng. Technol.* **7**(2.21), 58–61 (2018)
36. Gupta, S., Sharma, B.S.S.P.M.: Design and development of an intelligent aqua monitoring system using cloud based online access control systems. *Int. J. Recent Technol. Eng. ISSN: 2277-3878* **8**(4) (2019)

37. Ravishankar Kamath, H., Sharma, B.S.S.P.M., Siva Brahmaiah Rama, V.: PWM based solar charge controller using IoT. *Int. J. Eng. Technol.* **7**(2.7), 284–288 (2018)
38. Ravishankar Kamath, H., Siva Brahmaiah Rama, V., Sharma, B.S.S.P.M.: Street light monitoring using IOT. *Int. J. Eng. Technol.* **7**(2.7), 1008–1012 (2018)
39. Sharma, B.S.S.P.M., Kumar, A., Meena, B.K.: An intelligent solar based farm monitoring using cloud based online access control systems. *Int. J. Recent Technol. Eng.* ISSN: 2277–3878 **8**(3), (2019)