MIJRD Multidisciplinary International Journal of Research and Development

Volume: 01 | Issue: 03 | 2022 - Open Access - Website: www.mijrd.com - ISSN: 2583-0406

An Efficient E-Voting Algorithm and Dapp Using Blockchain Technology

Basharat Ali[1], Fawad Iqbal[2], Irshad Hussain[3], and Muhammad Younas[4]

[1,2,3,4]Software College, Northeastern University, Shenyang 110169, China

Email: [1]basharatalimian@outlook.com

Abstract— Various e-voting systems have been available for years with the objective of promoting the protection and reducing prices. A secure voting system promises to be achievable now that Ethereum, a randomized platform that enables distributed apps has established. There is a whole number of options for dealing with these problems, including organizing the additional votes, which would also be cost-effective and time-consuming. If indeed the subscriber authenticates with the appropriate national Identification card number and tries to enter the proper OTP. The core principle is to use blockchain technology in connection with a mutual authentication scheme and encryption algorithm to create a centralized e-voting system that does not rely on a trusted third party. It permits for a public and open process of voting while also safeguarding voter identification, data transmission privacy, and ballot reliability and validity throughout the payment phase.

Keywords— OTP, Distributed System, Decentralized technology, solidity, smart contract, Blockchain voting, Testrpc.

I. INTRODUCTION

Blockchain is a popular buzzword these days, owing to its role as the backbone of one of the most well-known crypto currencies in the world, bitcoin. One block holds the record/hashtags of the preceding block/node, and blockchain is a collection of blocks/nodes that are firmly related to each other. The first block/node is always named genesis block. Blockchain is entirely decentralized, with data stored in blocks/nodes rather than a single server or database and is maintained by a peer-to-peer network rather than being managed by a single institution. Because polling every vote generates a new block and no one can edit immutable data in blocks, prior entries in the chain of blocks/nodes cannot be modified, providing next-level security and integrity. Currently, a large number of electronic voting systems are centralized data processing servers. Blockchain web 3.0 is primarily concerned with sophisticated scripting languages, such as Solidity, which is underpinned by Cryptocurrency and contributes to the formation of efficient and secure decentralized applications. Here As when the system can have every user's regional identification code and mobile contact information, the program generates an OTP to check and verify the user. If somehow the details are completely inaccurate, the program will update the expected error, whereas the corroborated user will also be directed to the home website to vote for a person, and after voting, the user will immediately log out. The credibility of democracies is based on secure voting techniques. In document voting, recounting is a significant element in determining the winners. In addition, because the nature of

Volume: 01 | Issue: 03 | 2022 - Open Access - Website: www.mijrd.com - ISSN: 2583-0406

the blockchain enables good protection, interconnectivity, and scalability, the voting will indeed be committed as a genesis process to the network. This data will have to be unchangeable and permanent. Because the nature of blockchain provides high security, integration, and scalability, the vote will be recorded as a new block to the blockchain, and this data will be unchangeable and immutable.

1.1 Demonstrates the actual flow of the E-voting system

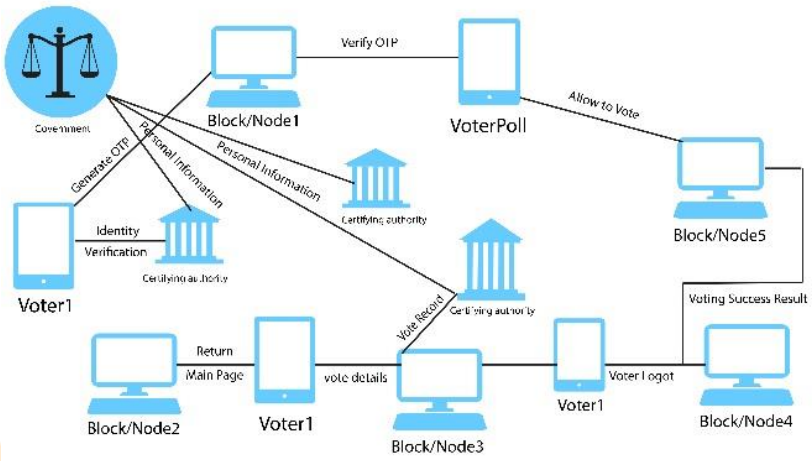

Figure 1: the actual flow of the e-voting system

2. RELATED WORK

The purpose of implementing a system of voting with new technology is not a novel one, but now with the passage of time, everything has been put into practice to measure their benefits and disadvantages. Though electronic voting is not generally seen on a widespread basis anywhere within the universe, it becomes more and more common. When compared to other options voting procedures, modern computers may have benefits [1]. An electronics voting system can be used in some of the other procedures in the process of implementing, publishing, weighing, retrieving, and checking ballot papers, and hence may not always provide an advantage in any of the above steps. There are already significant drawbacks, such as the probability of malfunctions or deficiencies in any electrolytic capacitor. However, if the records of online voting are highly centralized, any other null hypothesis is that the politician can use unconventional methods to commit manipulation, along with steal the information and change it wherever they see fit. To account for both the limited number of applicants the new algorithm was proposed by Tian et al [21]. who implemented Zhao and Chan's technique regulations as a subsystem. The usage of cryptocurrency in internet voting has evolved into commercial areas, as seen by ballot chain, an electronic blockchain-voting platform supported by Rated frequency bitcoin. Due to the architectural models, cryptocurrency virtual machine, solidity computer program, and pragma variants, blockchain technology still has limits [19]. Many researchers failed to acknowledge that by wanting to replace the cryptocurrency virtual machine with a user-friendly interaction and using smartphone validation with a governmental permanent residency handful, we could even solve the problem at some point and gladly accept more changes to a proposed

Volume: 01 | Issue: 03 | 2022 - Open Access - Website: www.mijrd.com - ISSN: 2583-0406

federal technique model to improve efficiency and availability [2]. Many Distributed System research teams failed to acknowledge that even by replacing the Cryptocurrency virtual machine with a customer interface and using portable proof of identity with a governmental citizenship number, we could perhaps solve the problem at some point and welcome more variations to a recently developed computer program model to improve quality and performance.

3. THE PROPOSED MODEL'S IMPLEMENTATION

As previously stated, we used private block chain, which is a permissioned blockchain, to set up our blockchain infrastructure, where the smart contract is deployed with multiple languages and technologies in order to achieve the privacy, security, and transparency concerns for electronic voting algorithms using blockchain technology to ensure that election process does not enable coerced voting. Nodejs, JavaScript express, and web3.0 are installed in the environment. Then, instead of creating the application against the real Ethereal blockchain; we utilized an in-memory blockchain called TestRpc, which may be thought of as a blockchain emulator [16].

One of the most crucial installing library and solidity compilers required to install SOLC for constructing voting decentralized applications is the real solidity compiler, and every generation of SOLC is generated to JavaScript. To check the transactions, TestRpc produces ten reasons for conducting, including one that generates 100 phony ETHERS to implement the program [3].

Ganache-CLI was used to generate a live blockchain for evaluating each block's transaction among each vote and time. Aside from it though, Ganache-CLI delivers a practical demonstration of the applications with 10 tester accounts and 100 fake checking accounts. ETHERS to represent the location voting block transaction [27].

The applications are listening on localhost 8545 through eth accounts and eth send operations, according to Ganache-CLI. This would also show that the operation was completed at the destination, and then it will display the desired contact information along with a service agreement for gas use and block numbers, as it was the day and time of voting [14]. This program, using blockchain-based, can resolve a very challenging and complex challenge that every country on this planet encounters [4].

The core implementations and framework of the vote's process design demonstrate how different methods are interconnected and operate together again to complete the activity. The given figure demonstrates the voting application's core architecture design.

The figure 2 shows how the actual voting process works, including how the ethereal virtual machine can be replaced by ganache CLI, how each block is generated with a vote, and how the immutable block chain grows as each vote pole adds one block to the blockchain with specific gas usage and other details. If someone has a fundamental understanding of all of these connected technologies, the implementation process will be lot easier.

Multidisciplinary International Journal of Research and Development

Volume: 01 | Issue: 03 | 2022 - Open Access - Website: www.mijrd.com - ISSN: 2583-0406

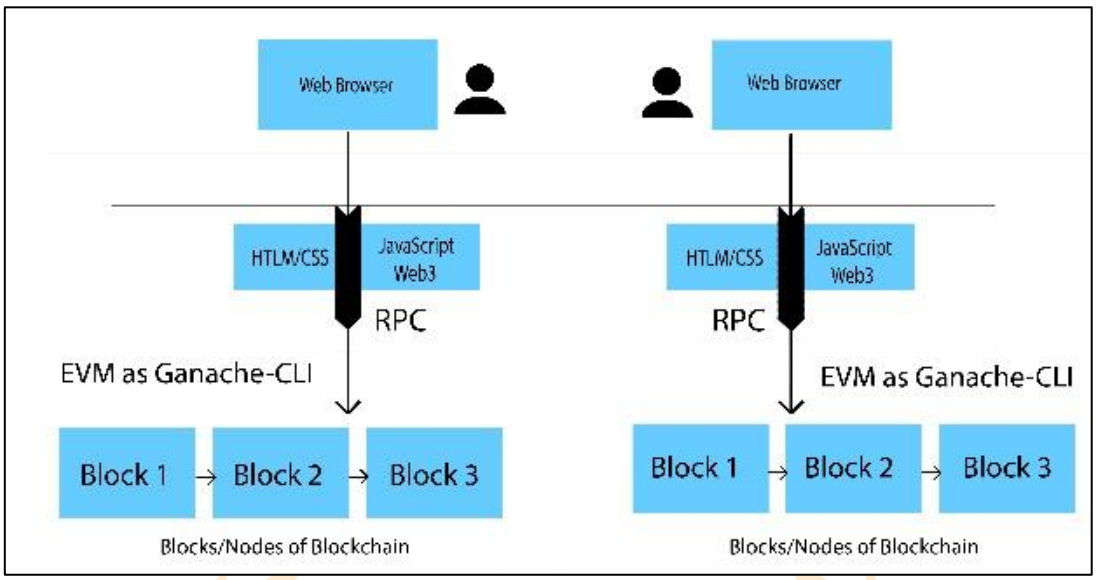

Figure 2: Architecture of the e voting

4. THE PROPOSED MODEL'S METHODOLOGY

As previously stated, we already use Cryptocurrency as our distributed ledger technology. A database is where most a company will maintain knowledge on its staff members. This database's material would be used by the system to put together a list of valid candidates in elections in our systems.

Crushers are indeed the people who assess if payments are genuine and add chains to the database in distributed ledger technology [18]. We adopted blockchain technology for our system because we have been primarily operating with a corporation or collection of institutions [9].

Only selected persons in a private blockchain have access to this information in the database; in other words, those certain people in the organization have the permission to authenticate and add transactional transactions to the blockchain [5]. Throughout gatherings where people in the community must make decisions that improve election, they rely on current social media deciding to vote tools.

Very few of the current blockchain technology serves as a mechanism to allow existing neighbours on the system to vote. We propose a receipt-free, absolutely verifiable, and private information peer voting protocol throughout this article, which may also allow peers on a cryptocurrency platform to vote more easily. For voting registration or vote counting, no trustworthy third parties are involved.

5. MODULES, KEY VARIABLES, AND FUNCTIONALITIES

Now we will go beyond the key parameters and modules that our blockchain technology electoral system depends on. We provide a brief explanation of each property and its functionality.

- Chairperson/admin: This would be the username of the casting smart general contractor that administers all components of the ledger voting system.

Volume: 01 | Issue: 03 | 2022 - Open Access - Website: www.mijrd.com - ISSN: 2583-0406

- Candidate: This structured variable essentially contains the information on the contestants standing for governor.
- Voters: This structured variable gives data on thousands of voters who may have registered.
- Majority: This parameter determines the proportion that somehow a competitor would have to get in order to win the popular vote. This attribute is set by that of the committee chair or indeed the voting system admin.
- Number of Voters: The aggregate number of participants throughout the voting system is stored in this parameter.

6. EFFICIENT E-VOTING ALGORITHM

A secure Voting System is an electoral college that seems to be safe, economical, and uncomplicated to just use. For cybersecurity threats, humans should use algorithms therefore in work [6]. Our proposed alternative introduces a unique e-voting solution that meets the e-voting process's infrastructure needs.

In our project, there have been three main processes that really should be completed: voter e-registration, vote upload, and result displays [7]. The system will facilitate safe and rapid e-vote upload, and therefore a traditional voting procedure inside this event the e-voting failures.

Algorithm 1: Voter verification and validation

- Num of Candidates: This parameter maintains a record of the total group of applicants running for public office.
- Add Candidate (): That service is only available to that same voting system's chairwoman or supervisor. This technique introduced a different contestant to our electoral college, permitting them to run for political office.
- Vote (): All consumers or voters will provide their opinions to the candidate and deposit their registration in this activity.
- Find No of Votes (): That function is used to calculate the voting numbers for each competitor and displays the information.
- Redistribute votes (): If designers might not have a substantial victory in this method, the votes for both the final candidate are divided according to voters' inclinations for this kind of member. Either the final participant is disqualified from the race, or his or her results are reallocated to other students depending on the different terminology in the qualifying contenders' votes. As long as there is not a massive majority winner, this operation deserves to be called.
- Set Majority (): The majority's variable is set using the same function. Only was the administrative or chair has the capacity to alter this characteristic in agreement with the organization's human resources.
- Winning result (): This individual will be able to the election outcome for the successful contestant who obtained a massive majority.

Volume: 01 | Issue: 03 | 2022 - Open Access - Website: www.mijrd.com - ISSN: 2583-0406

"Procedure: verifiy_CNIC_using_list(encrypted_ID_proofs)"

"Result: True if valid else false"

"Return list[encrypted_CNIC_ID_proofs]"

"Procedure register_a_voter(wallet_address,"

"Encrypted_ID_proofs)"

"Require(verification_phase_end == false)"

"res=verify_id_using_list(); //this can be replaced by a"

"More authentic than"

"If res== true then"

"Add address to eligible_voter_list;"

Else

End;

Algorithm 2: Initialization

"procedure give_voters_token()"

"require (verification of voter if== true)"

"For address in eligible_voter_list"

"registered_voter(address,1); // registered voter is a smart contract function will be defined already"

"procedure end_verfication_phase()"

"require(msg.sender==voter)"

"require(verification_phase_end == true)"

"require(verification_phase_end == false)"

"give_voter_token to vote();"

"add block to blockchain();"

End;

Algorithm 3: Voting Phases

"Procedure cast_vote(name,address,of citizen and Token);"

"Require (electionstart=true and electionend =false)"

"Require (tokens==block==1)"

"Balance[msg.sender]=balance[msg.sender] –1"

"Balance[address of candidate] = balance[address] +1"

"Add the data on blockchain or block added with"

"Specific gas amount and timing and date mentioned"

end();

Volume: 01 | Issue: 03 | 2022 - Open Access - Website: www.mijrd.com - ISSN: 2583-0406

6.1 Login page:

The site login pages are available at the starting of the website and if a user is having an account then he or she needs to log in the same page there are also optional of registration. The users who are new to the site are needed to be register in the website with the help of the Gmail and phone number.

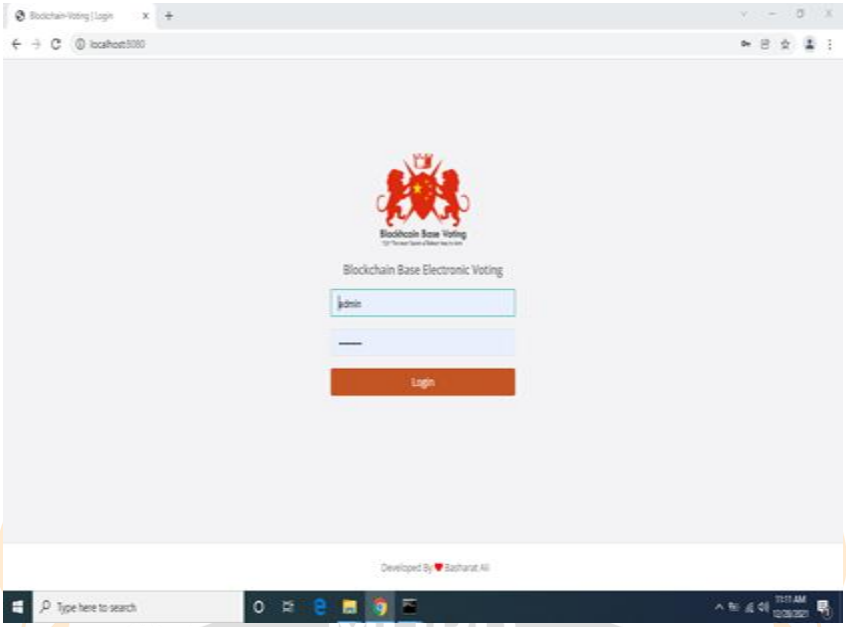

Figure 3: Login page

6.2 OTP Verification

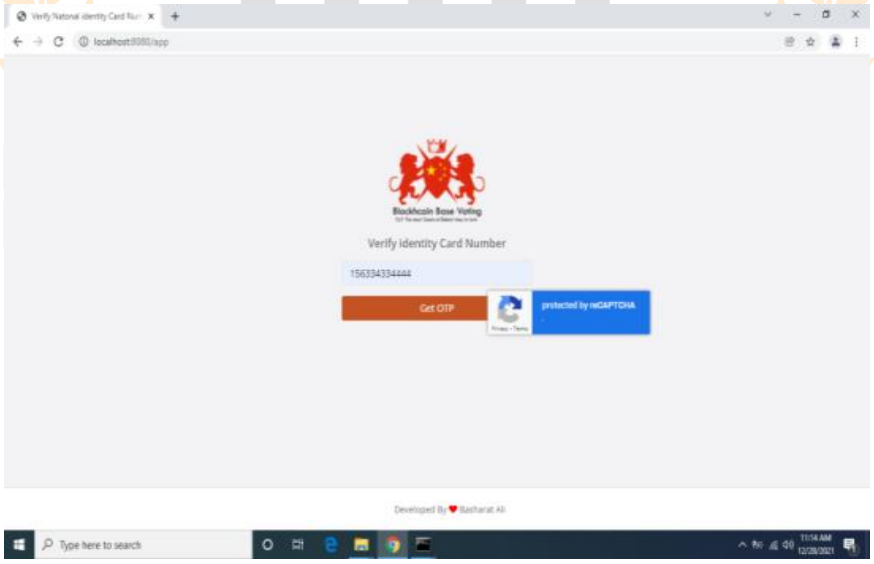

Figure 4: OTP Verification

When a person is logging in for the first time or forgot the password then these OTP is used for selecting new password for the old user or to set a password for the new user also. These are very important to maintain the security of the user.

Volume: 01 | Issue: 03 | 2022 - Open Access - Website: www.mijrd.com - ISSN: 2583-0406

6.3 Voting Phase:

In this part the rating percentages of the people are visible. Along with that it is also seen here that each party has gained how much votes.

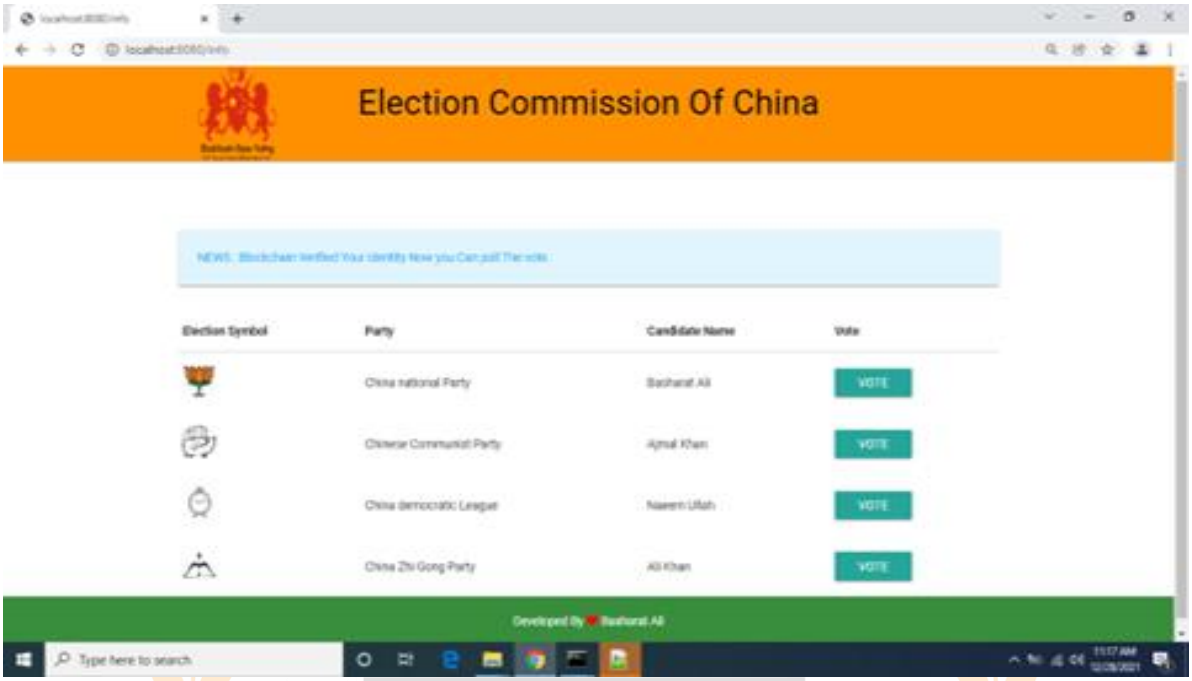

Figure 5: Voting Phase

8. CONCLUSION

In this dissertation, we designed a secure online voting system using an algorithm featuring two keys, something for cryptography and the other one for deciphering, for the authentication process, and another scheme, a cryptographic hash function with a hash algorithm, for the voting transition stage in the Electoral College. Such two techniques ensure that vote counting is stable and reliable. For years, many e-voting systems have been offered with the goal of enhancing consumer protection and lowering prices. Blockchain is a big technological breakthrough that creates a highly secure environment. Now that Ethereum, a randomized platform for distributed programs, has been built, a safe voting mechanism appears to be possible. Many firms have shifted their focus to employing decentralized voting software. Any government should go to the next stage of development if its elections are transparent and safe. It is not simple to challenge and solve a very interesting subject with blockchain technology, and we have always continued taking on extraordinary tasks since we were a youngster. It was aware that peer-to-peer centrally controlled technology can provide a solution to any problem outside of the financial sector, which meant that even though blockchain was initially used primarily for cryptocurrencies and financial transactions, and is only one feature of public ledger, the world is now moving to something far more unique: using blockchain to solve health, traffic, and government problems. With distributed ledger technology, we can tackle any problems since it ushers in a new age of next-generation reliability, resilience, security,

Volume: 01 | Issue: 03 | 2022 - Open Access - Website: www.mijrd.com - ISSN: 2583-0406

consistency, scalability, and interconnectivity. Nonetheless, further technology and features will be added and the solution in order to make it more flawless and to improve its performance and reliability.

REFERENCE

[1] Hjálmarsson, F.Þ., Hreiðarsson, G.K., Hamdaqa, M. and Hjálmtýsson, G., 2018, July. Blockchain-based e-voting system. In 2018 IEEE 11th International Conference on Cloud Computing (CLOUD) (pp. 983-986). IEEE.

[2] Sharma, T., Krishna, C.R. and Bahga, A., 2021, March. A Cost-Efficient Proof-of-Stake-Voting Based Auditable Blockchain e-Voting System. In IOP Conference Series: Materials Science and Engineering (Vol. 1099, No. 1, p. 012038). IOP Publishing.

[3] Raikar, D. and Vatsa, A., BCT-Voting: A Blockchain Technology Based Voting System.

[4] Teja, K., Shravani, M.B., Simha, C.Y. and Kounte, M.R., 2019, April. Secured voting through Blockchain technology. In 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI) (pp. 1416-1419). IEEE.

[5] TOMA, C., POPA, M., DOINEA, M. and IANCU, B., VOTING DAPP IN EMBEDDED DEVICES USING BLOCKCHAIN TECHNOLOGY AND SECURITY CHALLENGES.

[6] Geetha, S.K., Sathya, S. and Sakthi, S.T., 2021, May. A Secure Digital E-Voting Using Blockchain Technology. In Journal of Physics: Conference Series (Vol. 1916, No. 1, p. 012197). IOP Publishing.

[7] Saindane, P., Punwani, A., Pendal, P. and Sajeev, A., 2020. Plasma Voting: A Secure e-Voting Platform. SAMRIDDHI: A Journal of Physical Sciences, Engineering and Technology, 12(SUP 1), pp.211-217.

[8] Kumar, S., Darshini, N., Saxena, S. and Hemavathi, P., 2019. VOTEETH: An E-voting system using blockchain. Int. Res. J. Comput. Sci., 6(6), pp.11-18.

[9] Benítez-Martínez, F.L., Hurtado-Torres, M.V. and Romero-Frías, E., 2021. A neural blockchain for a tokenizable e-Participation model. Neurocomputing, 423, pp.703-712.

[10] Košťál, K., Bencel, R., Ries, M. and Kotuliak, I., 2019, October. Blockchain e-voting done right: Privacy and transparency with public blockchain. In 2019 IEEE 10th International Conference on Software Engineering and Service Science (ICSESS) (pp. 592-595). IEEE.

[11] Raj, A., George, G.T., Konnully, P. and Nair, S.R., Vote Blocks: A Block Chain Based E–Voting System.

[12] Khan, S., Arshad, A., Mushtaq, G., Khalique, A. and Husein, T., 2020. Implementation of Decentralized Blockchain E-voting. EAI Endorsed Transactions on Smart Cities, 4(10).

[13] Nayak, N., Patinge, A., Patinge, A. and Sathe, R., ETHEREUM DECENTRALIZED VOTING SYSTEM.

[14] Monteiro, J.D.S.A.S., 2019. Blockchain-based Decentralized Application for Electronic Voting using an Electronic ID (Doctoral dissertation).

[15] Alam, M., Khan, I.R. and Tanweer, S., 2020, April. Blockchain Technology: A Critical Review and Its Proposed Use in E-Voting in India. In Proceedings of the International Conference on Innovative Computing & Communications (ICICC).

[16] Alam, M., Khan, I.R. and Tanweer, S., 2020, April. Blockchain Technology: A Critical Review and Its Proposed Use in E-Voting in India. In Proceedings of the International Conference on Innovative Computing & Communications (ICICC).

[17] Pathak, M., Suradkar, A., Kadam, A., Ghodeswar, A. and Parde, P., 2021. Blockchain Based E-Voting System.

[18] Sanjaya, M.D., 2021. A Blockchain Based Approach for Secure E-Voting System (Doctoral dissertation).

[19] Rezvani, M.H. and Khani, H., 2019. e-Voting over Blockchain Platforms: A Survey. Journal of Network Security and Data Mining, 2(3), pp.1-14.

[20] Varalakshmi, M.V., Malarvizhi, S., Shamitha, A., Srimathi, S. and Vinisha, V., 2020. Blockvote: Aadhar Based Electronic Voting System Using Blockchain. Int. J. Sci. Res. Eng. Dev, 3(3), pp.421-427.

[21] Khoury, D., Kfoury, E.F., Kassem, A. and Harb, H., 2018, November. Decentralized voting platform based on ethereum blockchain. In 2018 IEEE International Multidisciplinary Conference on Engineering Technology (IMCET) (pp. 1-6). IEEE.

[22] Jin, C., Chen, G., Zhao, J., Gao, S. and Yu, C., 2019. Identity-based Deniable Authenticated Encryption for E-voting Systems. KSII Transactions on Internet and Information Systems (TIIS), 13(6), pp.3299-3315.

[23] Jinasena, T.M.K.K. and Gangodawila, N., Blockchain-based Secure, Reliable, and Distributed Voting System for Decision Making in Government Policies and Projects.

[24] Rupa, C., Midhunchakkaravarthy, D., Hasan, M.K., Alhumyani, H. and Saeed, R.A., 2021. Industry 5.0: Ethereum blockchain technology based DApp smart contract. Mathematical Biosciences and Engineering, 18(5), pp.7010-7027.

[25] Pujari, C., Muniyal, B. and Chandrakala, C.B., 2020. A decentralized consensus application using blockchain ecosystem. International Journal of Electrical and Computer Engineering, 10(6), pp.6399-6411.

[26] Mann, S., Jain, T. and Vyas, A., The Blockchain Revolution: Paradigm Shifts in Traditional Voting Practices. International Journal of Computer Applications, 975, p.8887.

[27] Almeida, R.L., Almeida RL, Ricci L., Camarinha-Matos LM (2019) voteChain: Community Based Scalable Internet Voting Framework. In: Technological Innovation for Industry and Service Systems. DoCEIS 2019. IFIP Advances in Information and Communication Technology, vol 553, p 70-80.

[28] Gaikwad, A.D. and Hatwar, P., 2020. Online Voting System Using Blockchain. IJRAR-International Journal of Research and Analytical Reviews (IJRAR), 7(1), pp.374-379.

[29] Singh, D., 2021. Blockchain based framework and approach for global healthcare system.

[30] Khanna, A., Sah, A., Bolshev, V., Jasinski, M., Vinogradov, A., Leonowicz, Z. and Jasiński, M., 2021. Blockchain: Future of e-overnance in Smart Cities. Sustainability, 13(21), p.11840.

