

AN EFFICIENT VOTE COUNTING SYSTEM WITH AADHAR VERIFICATION THROUGH BLOCK CHAIN

¹ Dr.P.EPSIBA, ² KOLTUR RISHI, ³ ADURLA DIKSHITH REDDY, ⁴ GOLLA PAVAN KUMAR YADAV, ⁵ VISHWANADULA SAKETH

¹Associate Professor, Department of IT, Sri Indu College of Engineering & Technology, Hyderabad.

^{2,3,4,5} U.G. Scholor, Department of IT, Sri Indu College of Engineering & Technology, Hyderabad.

Abstract—Modern civilization is seeing an increase in the popularity of online voting. It has a tremendous chance of bringing down administrative expenses and raising voting turnout. Voting may be done everywhere there is an Internet connection, thus there is no need to waste a lot of money in the aspect of the setting up of voting places for people to vote in. Online voting options are considered with great suspicion despite these advantages because they pose new security risks. Vote has been rigged a lot of times on a grand scale and may result from a single vulnerability. Elections must use lawful, accurate, safe, and convenient electronic voting technology. But potential issues with electronic voting methods might prevent widespread implementation. These problems were addressed by the development of blockchain technology, which provides decentralised blockchain nodes for electronic voting and is utilised to construct digital voting.

Keywords – digital voting, security, blockchain-based digital voting, privacy, blockchain technology, vote, faith.

I. INTRODUCTION

Not only is electoral integrity crucial for democracies, but it is also crucial for state voter confidence and responsibility. Methods of political voting are essential in this regard. From a political perspective, electronic voting technology can increase voter turnout, trust, and enthusiasm for the electoral process. Elections have long been a social issue due to their effectiveness as a democratic decision-making process. Citizens are becoming the more conscious in the world of the voting system as more people vote in actual elections.

Judges decide who will present them in political and business governance via the voting system. Voters choose their representatives in a democratic system. The amount of trust that people have in the voting process largely determines how effective such a method will be. A well-known trend is the development of legislative institutions to represent public opinion. These political entities include constituencies and student unions, among others. Voting has evolved as the main method for expressing the preferences of the populace by making decisions from their choices over time.

People are the main concern about the changing world order and the world order can only be achieved by the only one way of achieving the democracy. The democratic system is better judged when we have the belief of the people. The better chances of the government that have been achieved is not only at the greater risk but also for the development work. The online voting system not only creates this belief on the people but also the government inherit trust. We have seen numerous times when the political parties complain about how their votes have been tampered and also the votes that have been hijacked. This been said this online voting system not only provides solution to the common people but also to the political parties. If this is better achieved the chances of the democracy increases and the world order sustains at better level.

A disseminated node for electronic or digitalized voting is provided by blockchain technology. Due to the advantages of end-to-end demonstration, distributed record technologies like blockchain have presently been employed to create electronic voting device [13]. With characteristics like decentralisation. Blockchain provides non-repudiation and security protection. offers an intriguing alternative to traditional electronic voting methods. Both boardroom and open voting take place there [8]. A blockchain is a growing list of blocks connected by cryptographic connections, which at first was just a chain of blocks. The blocks that are present have a hash of the previous block to be achieved at the end of the day. This hash not only have a better spectrum of the upcoming generation of voting. The blockchain was developed to withstand data loss. A novel application of Blockchain innovation is voting, where academics are attempting to make use of advantages including nonrepudiation, openness, and secrecy

Nonetheless, nations are pushing ahead with efforts to implement blockchain voting, like Brazil [13], which uses the Ethereum blockchain to store election data. It is a massive undertaking to gather and authenticate the information of over 145 million registered voters. As a result, certain obstacles must be addressed in order to perform entirely blockchain-based e-voting.

II. LITERATURE SURVEY

Dr. Jain, and Kriti Patidar et al.,2015 [1], Voter authentication: There are numerous alternative methods for voter authentication. Voters may be validated using private key cryptography, according to Kriti Patidar and Dr. Jain, but this must be done before the election.. Voters must be registered by a third party, who must then generate and distribute registration keys to each voter.

Cosmas Krisna Adiputra, et al.,2020 [2], The election system or the electoral of the dimension(or another election administration organisation) prepares a key pair for the election (PE; SE), which is then used to encrypt and decode voter communications. He also contends that a public and private key infrastructure is required. The next step is for each voter to create their own key pair. (PV X; SV X) stands for the voter X's key pair. Later, the voter's own message is signed with the help of this key pair. In order to be eligible to vote, the electoral commission requires voters to register their public key PV X. using an approved form of identification. After confirming each voter's identification, the electoral commission adds the associated public key PV X to a public list.

Friðrik Þ. Hjálmarsson, et al.,2021 [3], Fririk. Hjálmarsson has a different idea, he wants to utilise a 6-digit pin for voters to use for voter verification. Each individual is recognised and authenticated by the system by showing an electronic ID from Auokenni and the accompanying 6-digit CODE in the voting booth. An individual could vote for many individuals without monitoring if he knew the CODE for each associated electronic ID he had.

Roopak et al.,2020 [4], Roopak offered a novel idea of leveraging the Aadhar database to collect voter information. The proposed framework is an electronic voting system that uses a unique virtual ID given by the UIDAI. The Aadhar database is used to get demographic information, including fingerprint information, on voters/voters. The fingerprint is turned to a digital signature, which may be used to verify the security of the vote in the block while encrypting it, but we don't want anybody else to know what's going on because it doesn't help ensure the voting is reasonable.

Verifying voter identification is always challenging; several studies have attempted the chance that how you can have a

better check and balance system so that the government can then go on to the system of better chances of democracy to function properly. The idea of the biometrics and the other chances are also the main spectra of the democracy. Aadhar have been the majority of the part where the Indian have this as their identification part. This identification part is later being asymmetric to the part of the system.

However, we believe that using advanced, difficult to decipher algorithms is one way to protect the stolen biometric data. Rather than storing biometric data as binary data and then as a reference string, it may be hashed with any hashing algorithm. The sample model should be translated into a hash value and then compared to the reference value during the validation and identification step.

Mukesh Panigrahi, Ajay Nair, Kaif Patanwala, Z.A. Usmani [5] We argued that the foundation of every democracy and institution is its voting mechanism. Over the past few decades, the voting process has undergone numerous effective changes. Different voting methods are employed. Among these are the paper ballot voting system, the electronic voting system, the internet voting system, the SMS and Miss Calls Voting System, and others. In this article, we looked at several voting methods and their advantages and disadvantages. The primary goal of this research is to make voting multipurpose and platform-neutral across all operating systems.

Adrián Rodríguez-Pérez [6] In this system, we suggested When voters have the option to cast their ballots online, can the principle of secret voting be guaranteed? Since 2000, a variety of distant electronic voting methods have been steadily introduced, and it has become clear that internet voting cannot ensure the same level of anonymity as do on the contrast of the paper system of voting of the country. In opposition to this presumption, the current suggestion advises reevaluating how the principle of vote secrecy has traditionally been set up. In light of this, the proposal will (1) assess current accepted standards for voter anonymity in traditional and internet-based voting systems; (2) assess the fundamental components of legal relaxations of the principle of secret suffrage, particularly those typically associated with various forms of remote voting; and (3) assess the fundamental components of legal relaxations of the principle of secret suffrage, particularly those typically associated with various forms of remote voting. Examine how recent technological advancements in the electoral field can be utilised to internet voting (and more broadly, in the field of e-governance and edemocracy) may lead to greater easing of the secret suffrage concept in the future. The proposal's overall objective is to examine how particular ideas aimed at maintaining voter confidentiality in online voting correspond with the precise purpose that the concept of secret suffrage is intended to preserve, namely, voter freedom. This is done instead of analysing electronic voting systems using typical privacy and anonymity requirements for voters.

India's Online Voting System Based on Himanshu Agarwal and G. N. Pandey's AADHAR ID in 2013 [7],

Before voting is permitted, a high security password is validated in the main database. The voter will be able to verify whether or

not their vote was transferred to the proper candidate or party. A person from their assigned constituency may also vote. The votes can be counted manually, which saves the data.

Biometric voting method using Aadhar card in India in 2016 - S Chakraborty, S Mukherjee [8] The major purpose of this initiative is to construct a secure electronic voting machine that distinguishes evidence, so that we may use the Aadhar card database for particular marks. During the race voting season, the online-voting

confirmation procedure should be feasible utilising finger vein identification, which allows the electronic poll reset to allow voters to cast their ballots. In

2019, Basit Shahzad Raju and Jon Crowcroft will present Trustworthy Electronic Voting Using Adjusted Blockchain Technology. [9] To maintain data security, this study proposes a system that use appropriate hashing algorithms. The notion of block formation and sealing is introduced in this article. The use of a block sealing principle contributes to the blockchain's flexibility in meeting polling process needs. Kakali Chatterjee, Ashish Singh[10], We suggested that The voting process was changed from a paper-based to a computerised approach in today's digital environment.

III PROPOSED MODEL

The solution we offer is more accessible and secure as an Android application, owing to authentication, authorization, and verification. The voter or user must first register in this system by filling out a registration form accessible through the Android application, following which an entry is created in the central database. After registration, the user may log into the application and participate in the polling process. When a user has valid credentials, they may log in and validate them by entering a one-time password that is only valid for a limited period. When a user registers into their account, the dashboard displays all of the data that was retrieved from the centralised database. After login into the account, the user is authenticated using a fingerprint. Each account receives a single token that may be used to vote. The vote is cast by transferring the token from the user's account in question to the wallet of the contender. A web application providing information on the total number of voters, the number of votes cast, and the percentage of votes cast is being built to determine the majority of votes. A single account may only vote once, and once voted, the account is no longer useful.

IV. IMPLEMENTATION

A. BLOCKCHAIN

A distributed, decentralised public ledger is what blockchain is. There are three major forms of blockchain: consortium, private, and public. A public blockchain includes examples like Ethereum and Bitcoin. The sophisticated mathematical operations serve as proof for this. This study makes advantage of open blockchain (Ethereum). A block is the foundation of secure as compared to other solutions.

a blockchain, which is fundamentally made up of a chain of blocks. A block has a header and a body, and the body of the block is where the network transactions are written. The block information, including the previous hash, nonce value and difficulty, block timestamp, and transactions, is contained in the block header. The sophisticated mathematical operations serve as proof for this. This study makes advantage of open blockchain (Ethereum). [7] Each block also contains data on the party taking part in the transaction. The block length varies, but it's generally thought to be around.

Workings of Blockchain:-

Blockchain is a peer-to-peer technology that allows for open sharing of data. among the users to produce an immutable transaction record. A transaction must occur before a block can be formed, and the authenticity of that transaction must then be confirmed. The block must then be sealed with a hash value after

The attributes of a digital electronic voting system are transparency, decentralisation, irreversibility, and nonrepudiation. The expansion of electronic voting systems raises numerous security and transparency concerns. In this study, we used blockchain technology to address security concerns and meet system requirements in a digital e-voting system. It presents fresh chances to set up a safe e-voting system in any country or organisation. The system is decentralised, contains the outcomes in the form of bit-coins, and has many locations, making it considerably superior than other systems. We will also assess the safety of the voting system we've proposed, which shows our protocol is more

The person becomes eligible to vote after they've turned in their registration form. The authentication module will receive the user's login details and verify their credentials. The dashboard won't be accessible to them until the verification process is finished. The OTP Verification process on the dashboard is the first step. The voter wallet is produced and a token is given to the voter, who will use it to cast their vote, only when user

the transaction has been stored within. As a result, a block is formed and sealed.

B. ETHEREUM

Ethereum is an open platform that allows for the development and deployment of sophisticated legal and financial applications like smart contracts. With Ethereum, developers may create markets, shared ledgers, digital alliances, and an infinite number of other things involving constant data and agreements without the need for an intermediary. This is similar to how programmable Bitcoin allows developers to create these things. The brilliant Vitalik Buterin, creator of the 2015 cryptocurrency Ethereum, saw the potential for using Bitcoins with Blockchain technologies as the next step in advancing the development of the Blockchain culture. It is anticipated that Ethereum, which currently has the second highest coin market cap, will surpass Bitcoin as the most popular cryptocurrency worldwide and the most valuable investment.

C. HASHING

The process of converting an arbitrary and variable input size to a defined output size is known as hashing. There are numerous functions that have data at various levels. Using SHA-256, we have implemented security. SHA-256, one of the SHA-1 (also known as SHA-2) successor hash functions, is one of the most powerful hash algorithms available. SHA-256 is not considerably more difficult to code than SHA-1 and has not yet been corrupted. [3] AES is a symmetric key encryption cypher, which means it uses the same key for encryption and decoding. AES is a fantastic companion feature because to its 256-bit key. In contrast to all of them, the technique is more adaptable than its forefathers in that it accepts any input length and creates an arbitrary output length.

D. REGISTRARTION MODULE

Following the submission of the registration form, the individual is now eligible to vote. The user will submit their login information into the authentication module, which will then validate their credentials. They will be allowed to access the dashboard only after that. The dashboard's initial procedure is OTP verification. After the user has been vetted and authenticated using just their fingerprint, the voter wallet is created and a token is provided to the voter, who will use it to cast their vote. Votes are cast by shifting the token from the voter's wallet to the wallet of the right candidate.

E. LOGIN MODULE

authentication has been completed. To cast a vote, the token is transferred from the voter's wallet to the appropriate candidate's wallet. The login module is the most important part of the whole process and this can better be achieved in the case if you have better check and balance system, so that at the end of the day the proper people who are authenticated and have proper aspect are verified and given chance to vote for the democracy.

V. CONCLUSION

In this essay, we analyse and discuss the conventional voting process as the current system and the upcoming system is analysed and better expectation have been inspected on the part of the system. The system not only gives a better idea of how the technology can better be used but also the idea is achieved. Then, we witnessed a comparison between the currently in use traditional voting system and the blockchain-based electronic voting system. Blockchain is used in the implementation as a centralised voting system. The voter data or credentials that will be used for their authentication will be stored in this system's blockchain network and database. Details of the voter or candidate will be used by the system during the voting process.

In this project, we have implemented a blockchain-based online voting framework where smart contracts are employed to enable safe and affordable elections while maintaining the privacy of the voters. In contrast to the previous part of the research system, we have demonstrated that blockchain technology provides democratic nations with a new opportunity to transition from the pen and paper election system and the paperless direct-recording electronic voting machine (DRE) to a more cost- and time efficient election system, thereby enhancing the current system's security and providing new accessibility. The vast statics of the online voting system may help us to gain the support of people who might not be able to go to vote.

The system that we have proposed currently makes use of Ethereum, a public blockchain. There are no constraints on participation, anybody may join in the consensus method, scalability concerns have been detected, and throughput is only fairly strong.

To get over the concurrent issues that are prevailing over the time, consortium blockchain, which have always combined elements of both public and private blockchain, can be used. In the future, we would construct the project as a whole. Even though it is currently meant for local organisations, the national

VI. SYSTEM ARCHITECTURE

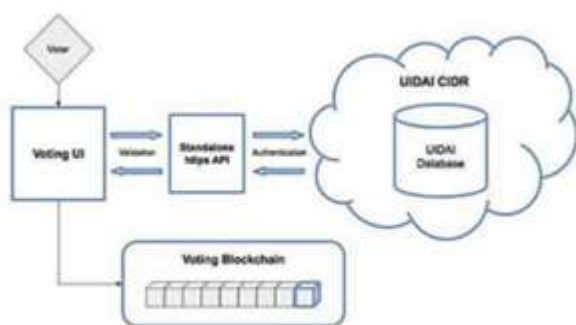


Figure 4: System architecture.

VII. FUTURE USAGE

voting system remains. In addition to the fingerprint module now used for authorization, a face recognition module would be introduced for increased security.

VIII. REFERENCES

- [1] F. P. Hjálmarsson, G. K. Hreiðarsson, M. Hamdaqa and G. Hjálmtýsson, "Blockchain-Based E-Voting System," 2018 IEEE 11th International Conference on Cloud Computing (CLOUD), San Francisco, CA, 2018, pp. 983-986, doi: 10.1109/CLOUD.2018.00151.
- [2] C. K. Adiputra, R. Hjort and H. Sato, "A Proposal of Blockchain-Based Electronic Voting System," 2018 Second World Conference on Smart Trends in Systems, Security and Sustainability (WorldS4), London, 2018, pp. 22-27, doi: 10.1109/WorldS4.2018.8611593..
- [3] . K. Garg, P. Saraswat, S. Bisht, S. K. Aggarwal, S. K. Kothuri and S. Gupta, "A Comparative Analysis on EVoting System Using Blockchain," 2019 4th International Conference on Internet of Things: Smart Innovation and Usages (IoT-SIU), Ghaziabad, India, 2019, pp. 1-4, doi: 10.1109/IoTSIU.2019.8777471.
- [4] R. Hanifatunnisa and B. Rahardjo, "Blockchain based evoting recording system design," 2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA), Lombok, 2017, pp. 1-6, doi: 10.1109/TSSA.2017.8272896.
- [5] . Xiao S., Wang X.A., Wang W., Wang H. (2020) Survey on Blockchain-Based Electronic Voting. In: Barolli L., Nishino H., Miwa H. (eds) *Advances in Intelligent Networking and Collaborative Systems. INCoS 2019. Advances in Intelligent Systems and Computing*, vol 1035. Springer, Cham. https://doi.org/10.1007/978-3-030-29035-1_54
- [6] Li, Y., Susilo, W., Yang, G., Yu, Y., Liu, D., Du, X., & Guizani, M. (2020). A Blockchain-based Self-tallying Voting Protocol in Decentralized IoT. *IEEE Transactions on Dependable and Secure Computing*, 1–1. doi:10.1109/tdsc.2020.2979856 .
- [7] K. Patidar and S. Jain, "Decentralized E-Voting Portal Using Blockchain," 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, 2019, pp. 1-4, doi: 10.1109/ICCCNT45670.2019.8944820.
- [8] Y. Zhang, Y. Li, L. Fang, P. Chen and X. Dong, "Privacyprotected Electronic Voting System Based on Blockchin and Trusted Execution Environment," 2019 IEEE 5th International Conference on Computer and Communications (ICCC), Chengdu, China, 2019, pp. 12521257, doi: 10.1109/ICCC47050.2019.9064387.
- [9] T. M. Roopak and R. Sumathi, "Electronic Voting based on Virtual ID of Aadhar using Blockchain Technology," 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), Bangalore, India, 2020, pp. 71-75, doi: 10.1109/ICIMIA48430.2020.9074942.

- [10] Y. Abuidris, A. Hassan, A. Hadabi and I. Elfadul, "Risks and Opportunities of Blockchain Based on E-Voting Systems," 2019 16th International Computer Conference on Wavelet Active Media Technology and Information Processing, Chengdu, China, 2019, pp. 365-368, doi: 10.1109/ICCWAMTIP47768.2019.9067529.
- [11] Himanshu Agarwal and GN Pandey. Online voting system for india basedon aadhaar id. In 2013 Eleventh International Conference on ICT and Knowledge Engineering, pages 1–4. IEEE, 2013.
- [12] Soumyajit Chakraborty, Siddhartha Mukherjee, Bhaswati Sadhukhan, and Kazi Tanvi Yasmin. Biometric voting system using aadhar card in india. *International journal of Innovative research in Computer and Communication Engineering*, 4(4), 2016.
- [13] Basit Shahzad and Jon Crowcroft. Trustworthy electronic voting using adjusted blockchain technology. *IEEE Access*, 7:24477–24488, 2019.
- [14] Scott Wolchok, Eric Wustrow, J Alex Halderman, Hari K Prasad, Arun Kankipati, Sai Krishna Sakhamuri, Vasavya Yagati, and Rop Gonggrijp. Security analysis of india's electronic voting machines. In *Proceedings of the 17th ACM conference on Computer and communications security*, pages 1–14, 2010.