EMPOWERING DEMOCRACY THROUGH BLOCKCHAIN

Ms.Supriya B Rao
supriyab.cs@sahyadri.edu.in

Shailendra Shetty, Prasad V Bhat, M Vignesh Bhat and Rithwik V Shet
Computer Science Engineering, Sahyadri College of Engineering and Management, Mangaluru-575029, Karnataka, India;
shettyshailendra3@gmail.com, vbhat.prasad@gmail.com, vigneshbhat064@gmail.com , rithwikvshet@gmail.com

Abstract: Election is an important factor in choosing the government in any country and it is important to increase the security and to have the most secure way and it can be secured with the most convenient and secure way which gives the fair choice for the people of the country to choose the leader they need.
Building a protected blockchain based e-voting system that offers all the essential features in a straight forward way of current voting plans and giving the convenient way to use the system which has been test for quite a while. The paper focus on creating an interface which has a quite strong security interface which is easier and convenient for the user. The system designed should focus on the user and the security of the system as they are the most important factor in the e-voting process.

Blockchain is the most trusted and secure technology which is considered and has decentralized network of blocks called ledgers. Whenever any attacker makes changes in the ledger the transaction history data present on the other system will be inconsistent and can be easily trackable so it is considered as one of the secure way.

I. INTRODU CTION

Electronic voting systems has been one of the important topic of active research for many years, with the goal to increase the efficiency of the election system and ensuring the election integrity by fulfilling the safety, privacy and compliance requirements [1]. Replacing the primitive way with a replacement election system which has the potential and verifiable. This technology has important features like Immutability which means when any proposed new block to the ledger is referenced by the previous version of the ledger. This creates an immutability in the chain which is effective way of preventing tampering with the integrity of the previous entries. Verifiability of the system is when the ledger is decentralized, replicated and distributed over network in multiple locations. This ensures high availability and provides third-party verifiability as all nodes maintain the consensus version of the ledger. Distributed Consensus: A distributed consensus protocol to see who can append the following new transaction to the ledger. A majority of the network nodes must reach a consensus before any new proposed block of entries becomes a permanent a part of the ledger. These features are partially achieved through advanced cryptography, providing a security level greater than any previously known record-keeping system. Blockchain technology is therefore considered as one of the best way for securing and implementing a replacement to modern voting process.

The current Indian democratic election system follows the primitive way where people come to election centre where they are allowed to cast their vote using a printed paper and a seal which is not the best solution to secure a vote but what if we introduce blockchain into this system which is the most secure way that is considered till date. The Project idea starts with giving two different interfaces admin and the users where admin registers and monitors all the activities that is going on in the system and who will be responsible to whatever happens in the system. The project next focusses on the identification and the validation of the user which will further more enhances the security of the system and there will be some more security layers which will be implemented in the project. The block containing the vote details will be added to blockchain network which will be stored in the decentralized network so modification done by an unauthorized user will be blocked and can be easily identified so this ensures the advanced security in the voting process.

II. LITERATURE SURVEY

[1]
This paper gave how the system of blockchain can be used as a implementation like service in an electronic voting system.
The paper makes the following original contributions:
propose a blockchain-based e-voting system
that uses blockchain and the review of existing blockchain frameworks which fits in
constructing a blockchain based electronic voting system.
Electronic voting system have been the topic of active research with the goal of minimizing the cost of running an election, while making sure the election

integrity is maintained by fulfilling the security, privacy and compliance requirements [1].
and paper scheme with a new election system has the using potential method to limit fraud while making the voting
this process is traceable and verifiable [2]. Blockchain is a distributed network it is present over many devices and is non-mutable process, has incontrovertible design, and available for public use and works in the concept of using ledger. This new technology has three main features:
Immutability: Any proposed block to the
ledger must reference the earlier version of the ledger recorded. This creates an immutable chain, which is when the blockchain gets its name from, and prevents from tampering with the integrity of the entries recorded earlier.
Verifiability: The ledger is decentralized, replicated and distributed over the blockchain network in different locations. This ensures high availability and eliminates the single point of failure of the system.
Distributed Consensus: The distributed consensus protocol to determine who will and can append the new transaction to the ledger

Secure Electronic Voting System Using Blockchain Technology(2018 International Conference on Computing, Power and Communication Technologies (GUCON)) [2] This paper gives us insights about todays digital environment and how the voting system has moved from paper based to a digital system. A digital e-voting system that have many properties such as transparency, decentralization, irreversibility and non-repudiation. The growth in digital e-voting system will arise many security and transparency issues which can be clearly seen.

Pomares [3] Even though having the knowledge about e-voting had taken place in an established
Democratic way and later as an under developed countries the speed of this system and implementation of the e-voting has been higher in the developing countries, especially in the countries of Latin America with countries such as Brazil, Argentina, Venezuela, and Ecuador. This paper talks about the experience of Salta which is the first Argentine district to implement e-voting in the year 2013. Process is analysed and their feed back is taken which is used to improve the system. Furthermore this paper talks about the e-voting system used and how the election process conducted in the different countries and what are the challenges faced by them in implementing the e-voting system successfully in their democratic environment.

Aruna [4] The voting system has evolved and substituted the system of voting using the old ways
And decreased redundancies and inconsistencies. Many privacy and security vulnerabilities
experienced over time had been the resolved with the help of e-voting system. All the cryptocurrencies are based on block chain. Block chain depends on the
principle of distribution and decentralization.

Volkamer [5] One common way of ensuring the security of The two different entities or trustees. Whereas in the most election process election authority
complete the task of entities and elections of the places where small number of people involved such as board elections is implemented in such a way that all the voters in the system are considered as entities. This is basically taken as the actual idea for an election process that is carried out.

Goodman [6] Development in the internet voting process that has taken place in Canada are growing up faster with activity focused on local election processes, political party its leadership and its votes and its union. In some cases federal structure of the
canada state made possible for the process of Internet voting while in others it inhibits the process.

Stein [7] This mainly talks about the electronic voting system implemented in the Europe. The challenges faced when implementing the electronic voting system in the Europe. And after implementation what are the challenges faced by them how they solved it and what are the consequences of implementing the evoting system in their country. What are the patchwork they have done in the different period of times and what are the flaws and negative impact of the system.

Goré [8] This shows how a modern technology can be used to do complex work by elemenating the human intervention within the system and making the system more reliable and trustworthy. This can be created by the combination of the technology like blockchain and machine learning. The machine learning process can be used in the electronc voting system in the process like vote counting and hence by elemenating human intervention making it more reliable.

Kulyk [9] This paper mainly talks about enhancing the security of the voting system and proposes that the one of the best way to ensure the security in voting system is by distributing critical tasks between
different entities named here trustees. Whereas in the most election process election authorities does the job of trustee. This actually is the case for an election in this process of distributed system.

III. METHODOLOGY

The implementing process in the system initially provides a better interface for the user while using the system. When the press on the given button on the initial page the page will redirect them in to the new page where the users have to select the login phase. This is the step which makes the normal users of the system different from the admin of the system. The users will be having the limited access to the system whereas the admin will be having some special access in to the system.

In selecting the user phase the users also have to give the password along with the unique id provided to them which make the system secure and trustworthy. The normal users will be able to vote for the candidates by making the transaction but the admin will be able to monitor the complete activity going on inside the system. He also has the access in changing the phase from voting phase to count vote once the election process is over and then result phase.

There are two parts in the Blockchain system. Admin login and User login. Each Node is connected with the blockchain based database. The each of the node has its own separate functionality and has different access to the system. The user performs voting by making a transaction with the help of the cryptocurrency separately provided to the users. The admin manages and monitors the overall activity going on in the system and will be having the special access to the system. On successful transaction, the transaction details are maintained in a ledger which can be used for authorization of transaction in the future.

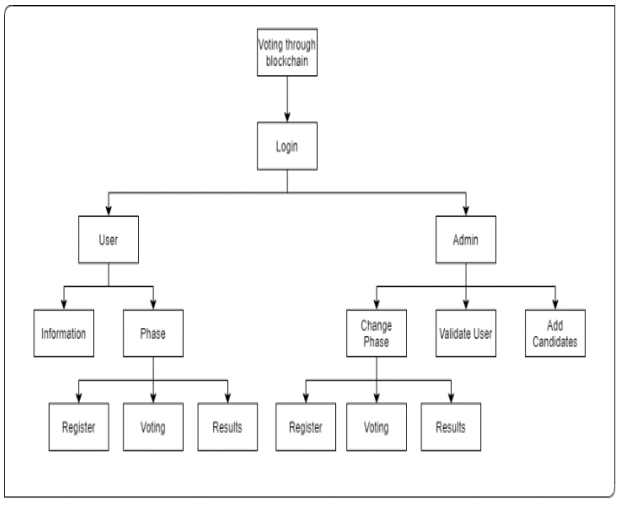

Fig 1: Implementation of the proposed e-voting system

IV. RESULTS AND DISCUSSION

The detailed analysis on the topic is carried out and

The sign in for admin interface is used to sign in the admin to the systen with his user id and password. The admin needs to submit same and he will be given special access to the system like changing the phase registering the voters and validating the voters.

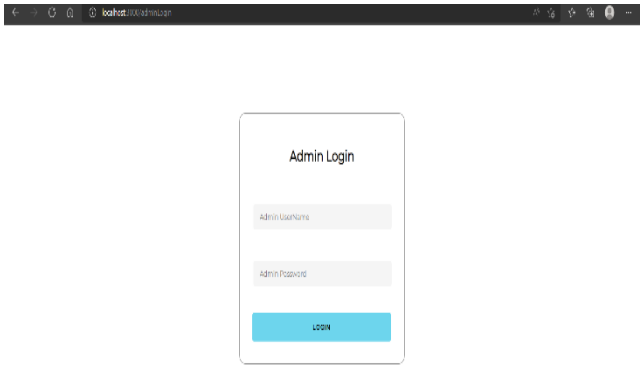

Fig 2: Admin login interface in the e-voting system

Initially whenever any user log in to the system they will be provided with the interface of the system to guide them and make the concept of using the system easier and understandable.

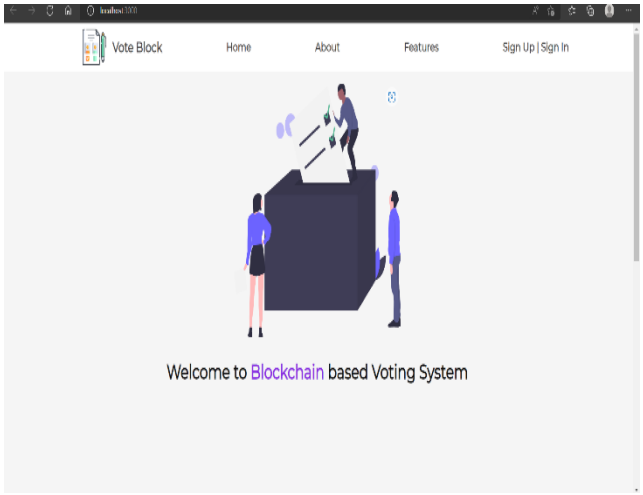

Fig 3: The initial interface provided in the system

In the initial phase the users of both the phase admin and normal user will be given a login window where users have to enter their username and password to log into their

dashboard where they will be given access to different resources and will be able to vote.

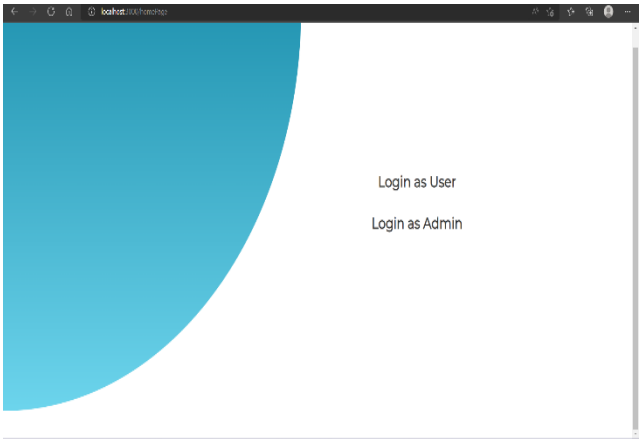

Fig 4: The two different interfaces provided in the system

The admin dash board is an interface for admin to do all the operations which has higher responsibility. Admin operations include adding the candidates who have registered and second responsibility that admin has got is to validate the voters that is to verify if he is an eligible voter or not . We have third admin feature as to change the voting phases and we can also get details of all registered candidates. Last option is to logout from admin panel.

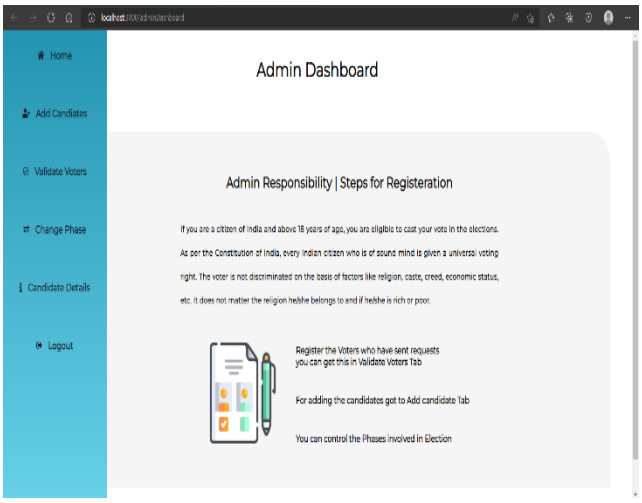

Fig 5: The admin dashboard in the system

In the add candidates section admin can add the eligible candidate for the elections which is also considered as a transaction and Matamask gets activated and gas fee is cut. Before adding the candidate admin needs to take all the details such as candidate name, his party name, candidates age and his expirence, by taking all these factors candidate is added. This also gets displayed in other section candiate details where all the candidate overview can be seen.

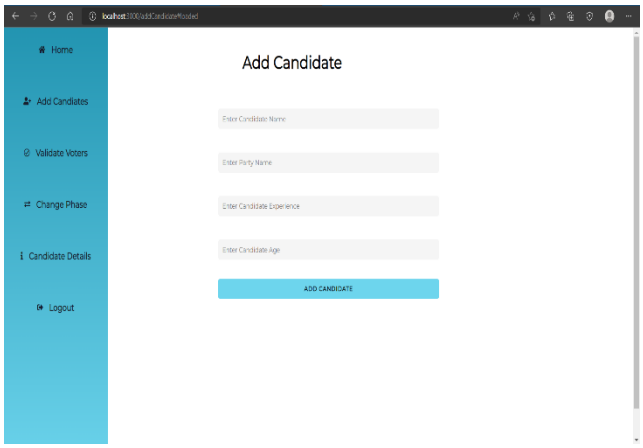

Fig 6: Add candidates in the system

Validate voter interface is used to verify the voter that he is eligible or not. Here whenever user registers in the user section the public id of the user gets displayed in the validate voters section. In metamask as we know we use private id but here to verify admin don't have right to see users private id. After typing that id which was previously used in metamask and clicking on add voters ,the candidate gets validated as a voter.

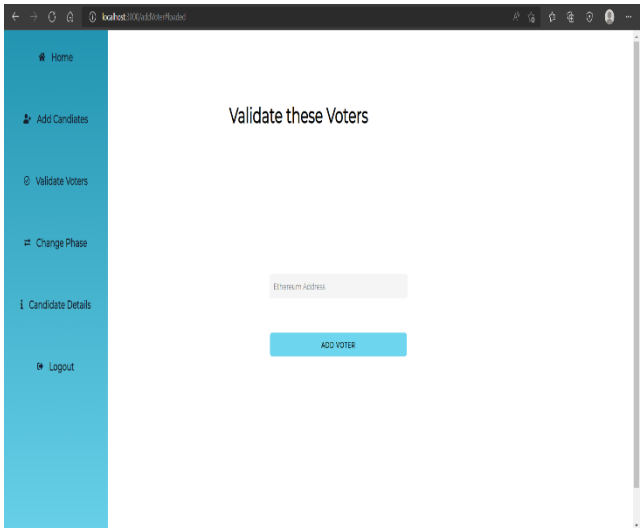

Fig 7: Validate voters in the system

The change phase interface is used to change the phase that is progress of the election. In our voting system we have three types of phases. The first phase is registration phase where voter is registered and validated. Second phase is voting where user can caste his vote. Last phase is result phase where we can see who won and how many votes did each candidate got. Changing the phases is also a transaction and it too cost some gas.

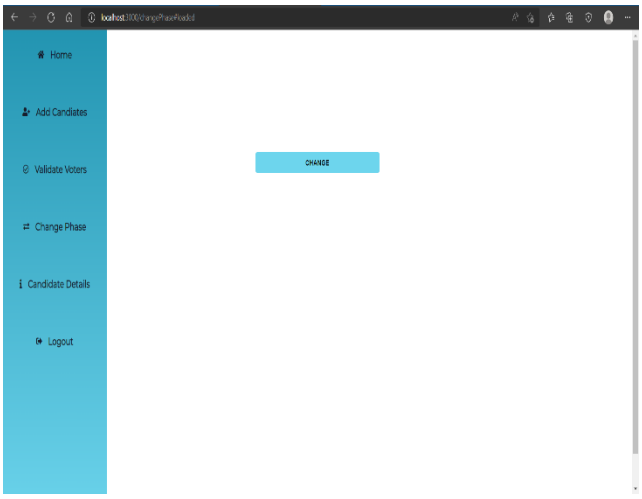

Fig 8: Change Phase in the system

In the candidate details interface we can see details of all candidates who got added by the admin in candidate add section. The details include name of candidate, party of candidate, his experience, candidate age and number of votes that candidate got in real time to analyze which candidate is in majority and can form the government.

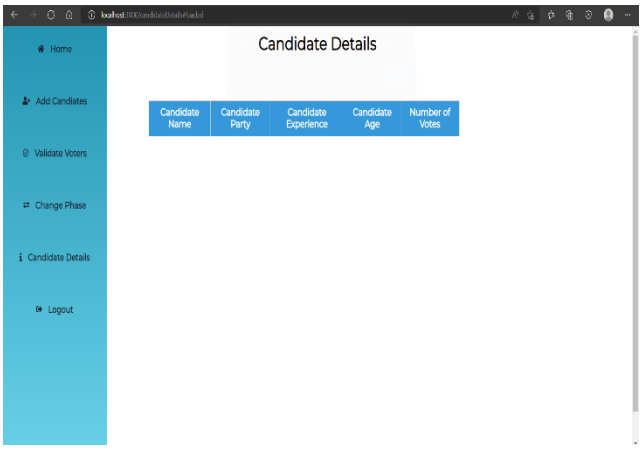

Fig 9: Candidate details in the system

The sign in sign up interface is used to either register the candidate or sign in with his user id and password. If the user do not have any account he needs to type his name mail id and password. After this user will be sent an otp to his mail address which he has already given before . User needs to submit same otp and if that otp matches user gets registered and then can login as a voter. This gives us extra layer of security before verifying he is eligible voter or not.

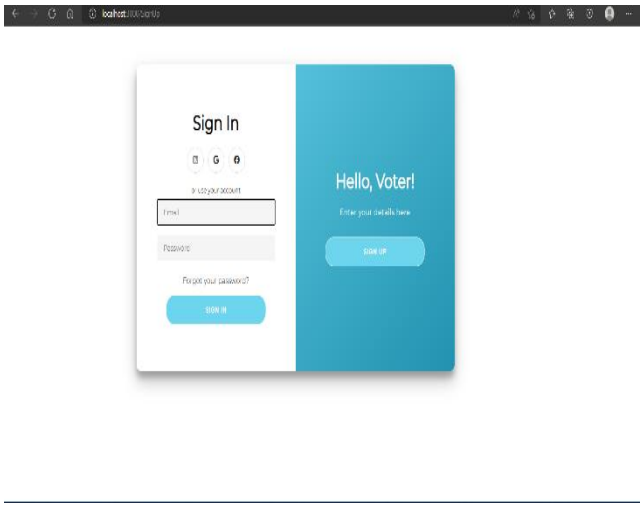

Fig 10: Sign in and signup in the system

This is the interface for voter where he can do all his activities. Features given to user includes registering himself, casting his vote to his party and also observing results. This all depends on which phase is user. These phases are controlled by admin. These are the only three activates that user is allowed do.

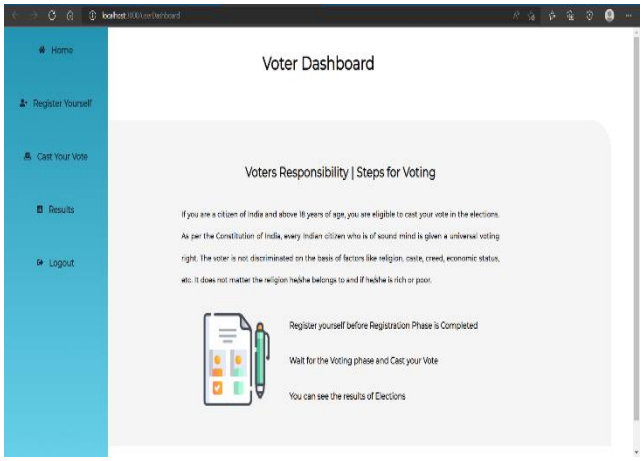

Fig 11: The user interface in the system

In the registering interface we can register ourselves by giving 2 detalis. The to be provided includes voterid number which is issued by government of India. Second thing is o enter Ethereum address which is the public id of the private id which has already being used in meta mask for all the operations ,after this user is registered for voting. These all things should be done within registration phase itself.

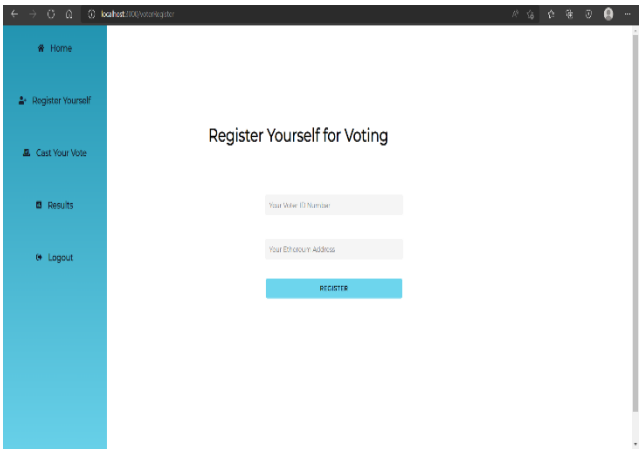

Fig 12: Register yourself in the system

In this section after registration user can choose from the drop down menu which candidate he wants to vote, this is a transcation which happens through metamask wallet. After confirming gas fees his vote is successfully casted. The voting process only happens only if admin has changed the phase to voting else it cannot be done.

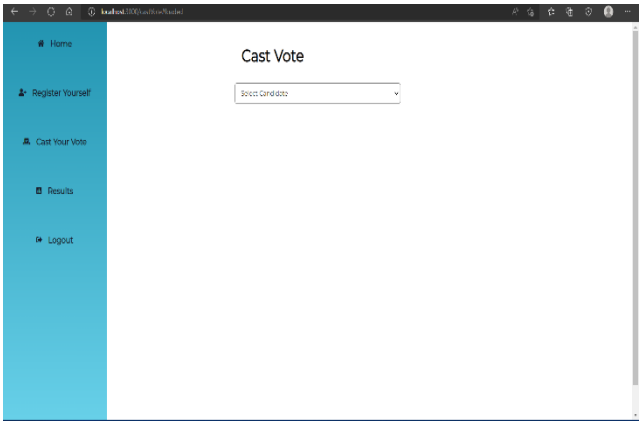

Fig 13: Cast your vote in the system

In this section, voter can see the number of votes which has been casted for each and every candidate after certain time , that is after all the registration and voting is completed by using this voting system becomes highly secure and transparent. Voter can only see all the results only if admin has enabled results phase.

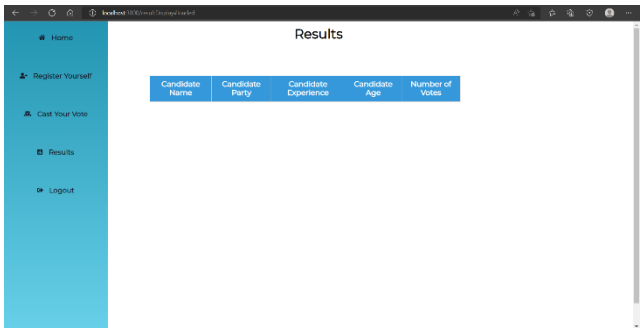

Fig 14: Results of the voting in the system

The utility constructed could be useful in the field of democratic election system in securing their vote via way of means of getting the vote through the platform and securing it in the blockchain end result of the of the system also provides a very good secure election system. This platform is the one of the simplest way of casting vote. Hence, the utility might be very useful and powerful in its operation as soon as it is implemented in this field. Developing a system in blockchain to securely vote is a way of building a better society by giving a good interface between the system and the people.

V. CONCLUSION

Blockchain works as the shared or distributed network. the distinctive cryptographic methods are used in securing the data on the ledger of the distributed blockchain network. Blockchain assures decentralization, tamper information, scalability and additionally provides immutability to the data stored on the network so it will likely be successfully used for securing votes. It can reduce the overall frauds and tampering of the vote and voter details. Here for implementation purposes we make use of solidity language which is used for connecting the data with blockchain network. The currency we make use is ethereum which is used to make transaction and thereby successfully vote.

VI. REFERENCES

[1] Hjálmarsson, Friðrik Þ., Gunnlaugur K. Hreiðarsson, Mohammad Hamdaqa, and Gísli Hjálmtýsson. "Blockchain-based e-voting system." In *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, pp. 983-986. IEEE, 2018.

[2] Kumar, D. Dwijesh, D. V. Chandini, Dinesh Reddy, Debnath Bhattacharyya, and Tai-hoon Kim. "Secure electronic voting system using blockchain technology." *International Journal of Smart Home* 14, no. 2 (2020): 31-38.

[3] Pomares, Julia, Ines Levin, R. Michael Alvarez, Guillermo Lopez Mirau, and Teresa
Ovejero. "From piloting to roll-out: voting experience and trust in the first full e-election
in argentina." In 2014 6th International Conference on Electronic Voting: Verifying the
Vote (EVOTE), pp. 1-10. IEEE, 2014.

Aruna, S., M. Maheswari, and A. Saranya. "Highly Secured Blockchain Based Electronic
Voting System Using SHA3 and Merkle Root." In IOP Conference Series: Materials Science
and Engineering, vol. 993, no. 1, p. 012103. IOP Publishing, 2020.

[5] Volkamer, Melanie, and Margaret McGaley. "Requirements and evaluation procedures for
eVoting." In The Second International Conference on Availability, Reliability and Security
(ARES'07), pp. 895-902. IEEE, 2007.

[6] Goodman, Nicole J., and Jon H. Pammett. "The patchwork of internet voting in Canada."
In 2014 6th International Conference on Electronic Voting: Verifying the Vote (EVOTE),
pp. 1-6. IEEE, 2014.

[7] Stein, Robert, and Gregor Wenda. "The Council of Europe and e-voting: History and
impact of Rec (2004) 11." In 2014 6th International Conference on Electronic Voting:
Verifying the Vote (EVOTE), pp. 1-6. IEEE, 2014.

[8] Goré, Rajeev, and Thomas Meumann. "Proving the monotonicity criterion for a plurality vote-
counting program as a step towards verified vote-counting." In 2014 6th International Conference on Electronic Voting: Verifying the Vote (EVOTE), pp. 1-7. IEEE, 2014.

[9] Sos.ca.gov. (2007). Top-to-Bottom Review | California Secretary of State. Available at: http://www.sos.ca.gov/elections/voting-systems/oversight/ top-bottom-review/.

[10] Nicholas Weaver. (2016). Secure the Vote Today Available at:https:// www.lawfareblog.com/secure-vote-today.

[11] TechCrunch, (2018). Liquid democracy uses blockchain to fix politics, and now you can vote for it. Available at: https://techcrunch.com/2018/ 02/24/liquid-democracy-uses-blockchain/

[12] Ajit Kulkarni, (2018), "How To Choose Between Public And Permissioned Blockchain For Your Project", Chronicled, 2018.

[13] "What Are Smart Contracts? A Beginner's Guide to Smart Contracts", Blockgeeks, 2016. Available at: https://blockgeeks.com/guides/ smart-contracts/

[14] Salanfe, Setup your own private Proof-of-Authority Ethereum network with Geth, Hacker Noon, 2018. Available at: https://tinyurl.com/ y7g362kd.

[15] Geth.ethereum.org. (2018). Go Ethereum. Available at: https://geth. ethereum.org/

[16] Vitalik Buterin. (2015). Ethereum White Paper Available at: https: //github.com/ethereum/wiki/wiki/White-Paper.

[17] Ethdocs.org. (2018). What is Ethereum? — Ethereum Homestead 0.1 documentation. [online] Available at: http://ethdocs.org/en/latest/ introduction/what-is-ethereum.html

[18] Agora (2017). Agora: Bringing our voting systems into the 21st century Available at: https://agora.vote/Agora_Whitepaper_v0.1.pdf

[19] Patrick McCorry, Siamak F. Shahandashti and Feng Hao. (2017). A Smart Contract for Boardroom Voting with Maximum Voter Privacy Available at: https://eprint.iacr.org/2017/110.pdf.

[20] Andrew Barnes, Christopher Brake and Thomas Perry. (2016). Digital Voting with the use of Blockchain Technology Available at: https://www. economist.com/sites/default/files/plymouth.pdf

[21] Jonathan Alexander, Steven Landers and Ben Howerton (2018). Netvote: A Decentralized Voting Network Available at: https://netvote. io/wp-content/uploads/2018/02/Netvote-White-Paper-v7.pdf

[22] Jelurida, "Jelurida", 2017. Available at: https://www.jelurida.com/sites/
default/files/JeluridaWhitepaper.pdf

[23] 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.

[24] 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.

[25] 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.

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

[27] 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 Evoting and Identity, ser. VOTE-ID'07. Berlin, Heidelberg: Springer-Verlag, 2007, pp. 111-124.

[28] 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.

[29] 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.

[30] Chaum, D. (2004)."Secret-ballot receipts: True voter-verifiable elections." , IEEE Security Privacy, vol. 2, no. 1, pp. 38-47, Jan 2004.

[31] Chaum, D. (1981)."Untraceable electronic mail, return addresses, and digital pseudonym.", Commun. ACM, vol. 24, no. 2, pp. 84-90, Feb.

[32] Douglas W Jones. Threats to voting systems. In NIST workshop on threats to voting systems, 2005.

[33] Yi Liu and Qi Wang. An e-voting protocol based on blockchain.

[34] Taher ElGamal. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE transactions on information theory, 31(4):469–472, 1985.

[35] Tadayoshi Kohno, Adam Stubblefield, Aviel D Rubin, and Dan S Wallach. Analysis of an electronic voting system. In Security and Privacy, 2004. Proceedings. 2004 IEEE Symposium on, pages 27–40. IEEE, 2004.

[36] Rifa Hanifatunnisa and Budi Rahardjo. Blockchain based e-voting recording system design. In Telecommunication 866 Systems Services and Applications (TSSA), 2017 11th International Conference on, pages 1–6. IEEE, 2017.