"Bodh", BPIT's International Journal of Technology & Management
ISSN: 2454-8421, Volume 7, Issue 2, July- Dec 2021, Page 38-45

BBIJTM

Smart Secured Voting Tool Using Block-chain Technology in Peer-to-Peer Network

Bhawna Suri[1], Shweta Taneja[2], Rohan Sharma[3], Muskaan Dua[4], Rajneesh Dubey[5]
[1]*Department of Computer Science and Engineering, Bhagwan Parshuram Institute of Technology, Delhi, India,*
[1]bhawnasuri@bpitindia.com, [2]shwetataneja@bpitindia.com, [3]rohan01101999@gmail.com,
[4]muskaan.dua1999@gmail.com, [5]rkrajnees3@gmail.com

Abstract- Electronic Voting (e-voting) is the well-known method of casting and/or counting votes electronically. This is a cost-effective and efficient approach for handling a voting procedure, which has the feature of being benevolent as well as presenting data and soliciting high safety. Procuring e-voting is the need of the day and can be accomplished using only by the domains of communications and net-working. The major concerns are the data privacy for e-voting. We have proposed a tool- E-Matdan using block chain for safe and reliable of e-voting. It is a three-step process, in step the mapping of a synchronized model of voting records based on Distributed Ledger Technology (DLT) is done to avoid fabrication of the votes. Secondly, on the using Elliptic Curve Cryptography (ECC), user credential model is made for validation of votes. Thirdly, a withdrawal model is made that allows the voters to change their vote before a preliminary to the decided deadline. By amalgamating the above constructions of different designs, we have proposed a block chain based e-voting scheme in P2P network. To showcase the work, using block chain an e-voting system is implemented on Linux platforms in the P2P network for sundry candidates.
Keywords--- E- voting(Electronic voting), blockchain, DLT(Distributed ledger technology), , ECC(Elliptic curve cryptograph), ECDSA(Elliptic curve digital signature algorithm)

I. INTRODUCTION

Democratic voting is the necessity of every Democratic country. The most familiar and easy voting technique was paper-based but now with so much advancement in technology, this casting of votes would save paper and minimize the cost of conducting elections. Another advantage of get ridding of this traditional paper based scheme with a new election system is to reduce forgery, booth capturing and other unfair means to clean and fair elections [1]. Voting is the modus operandi to make a collaborative resolution or communicate an opinion among an assembly or a meeting or constituency [2]. Voting usually follows debates and discussions, controversies and election crusades. Since the 17th century, voting has been the accustomed technique by which contemporary exemplary democracy has set off. During voting, the individual to be elected is the one contesting the election, also known as the candidate of the election and the one who casts a referendum for their selected contestant is the voter. Customarily, the voter can vote in obedience to the list of candidate/contestant or vote for any other individual(s) he/she favors.

Voting plebiscites must be anonymous and stamped by the voters in private kiosks so that no one else can discover out for [whom an individual is voting. Voting is also used in various other distinct privatized establishments and brackets, such as clubs, corporations, and volitional consortiums.

With the expeditious evolution of the Internet and information technologies, many run-of-the-mill offline amenities such as casting votes, sending/receiving mails, payments, are hiking up to the online ones. Online voting is also well known as electronic voting (e-voting). E-Voting is an electronic means for registering and enumerating votes. E-voting helps us save time and endeavor with high productivity and pliability. Users of e-voting are balloters and election officials. The balloter/voter can proffer his/her votes in a computerized manner (electronically) to the election officialdom from any placement through the way of e-voting. The election administration is accountable for accumulating the votes from the balloters/voters. It is surely getting more and more recognition instead of the traditional method of voting. With the development of the Internet, e-voting became a crucial means of countless corporations.

A. E-Voting

Electronic voting machines (EVMs) are generally considered as weak machines for security concerns. Anyone who captures the machine or has access to it can interfere with it and can change the vote casts through that machine. Hence, there is a need to move one step ahead for this fair voting which is digital voting.

In digital voting the electronic devices, such as voting machines or an internet browser, are used to cast votes. The voting done through EVMs, which are at the polling stations, is also called e-voting. When the voting is done using a web browser is known as i-voting. Every mechanism has their pros and cons; the main concern in i-voting is the security issues. To handle the security the safest track is blockchain technology.

Blockchain technology was primarily designed for cryptocurrency- bitcoin. It uses the distributed architecture, and every transaction is stored as a block chain. It is a secure and robust system and can be used for digital voting.

B. Role of Blockchain in E-voting

A blockchain is a distributed, immutable, incontrovertible, public ledger with 4 main features – storage at many different locations, no single point of failure in the maintenance, every new block holds the reference the previous version of the ledger, creating an immutable chain and lastly every new block becomes a permanent part of the ledger. The first block in the blockchain is known as the 'Genesis block' or 'Block 0'. [3] All this is based on the cryptography techniques, providing a more secure database than the previous databases. The blockchain technology can therefore be considered as the ideal tool for the voting process.

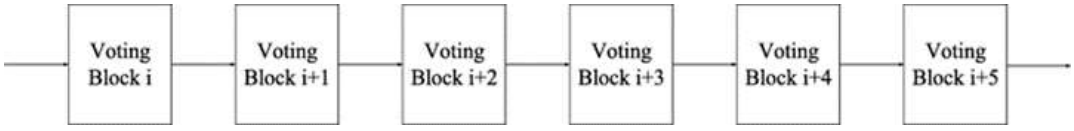

Fig. 1: E-Voting blockchain

The design of blockchain in e-voting is based on DLT which is a list of blocks It is represented as a series of voting blocks chained sequentially chained to each other. The first block is known as the Genesis block. This is shown in Fig 1. In each block, there is a voter's ID, voter's signature, timestamp, vote and a digest (hash) as shown in fig 2.

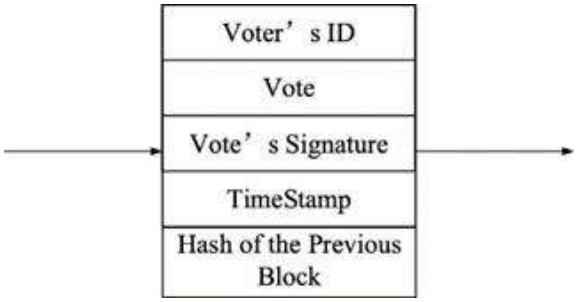

Fig. 2: A voting block

(1) Voter's ID: Voter is the person who casts a vote to his/her chosen candidate. ID is assigned randomly to the person who has the right to vote.
(2) Vote: A ballot is assigned to the chosen candidate of the voter.
(3) Voter's signature: A voter uses his/her private key to assign the vote in an encrypted manner. This encryption is done with the help of private key and hash generation. No one else can find out to whom the ballot is assigned.
(4) Timestamp: Submission of ballot is tracked by a timestamp. If two or more blocks have the same timestamp, the one with higher value of signature is preferred over others.
(5) Hash of the previous block: SHA-256 algorithm is used to compute the previous block hash value.
Thus, the blockchain-based e-voting scheme is immune to data modification and is non-repudiation.

C. Our Contribution

In our work, blockchain technology is used to improve the security of e-voting. Following are our contributions:
(1) A synchronized model of voting records has been designed based on DLT to avoid forgery of votes.
(2) A user credential model has been designed based on ECC to provide authentication and non-repudiation.
(3) A withdrawal model has been developed that enables voters to change their vote before a preset deadline.
By integrating the above designs, we propose a blockchain-based e-voting scheme, which meets the essential requirements of the e-voting process.
Following are the features of our blockchain-based e-voting scheme as follows:
(1) The blockchain-based e-voting scheme is public, distributed, and decentralized. Votes can be recorded from voters across the world using mobile or computers
(2) In blockchain-based e-voting schemes voters are allowed to audit and verify the votes inexpensively.

(3) The management of the database of votes is done autonomously and uses a distributed server of the timestamp on a peer-to-peer network.
(4) Process of voting on the blockchain is a workflow where voters regarding data security are marginal, which removes the characteristic of infinite reproducibility from e-voting.

The paper is organized as follows. Section1 deals with introduction. Section 2 deals with the related work. Problem formulation is described in the Section 3, Section 4 and its subsection deals with the estimation of the context information. Mathematical model for context estimation comes in Section 5. Section 6 deals with result and discussion .Section 7 deals with conclusion and future scope. Section 8 contains the reference part.

II. RELATED WORK

Block chain technology can be applied in many applications; here we have discussed its applications done in different manners and in different domains. Anonymous voting by two-round public discussion, proposed an addition of a self-tallying function to the 2-Round Anonymous Veto Proto-col (called AV-net). The AV-net provided exceptional efficiency compared to related techniques, the paper was focused on the dining cryptographers network (DC-net) and its weaknesses and proposed the AV-net as a new way to tackle that problem [4].The new protocol, like the AV-net requires no trusted third party or private channel. Participants execute the protocol by sending two-round public messages, but are significantly more efficient in terms of the number of rounds, computational cost and bandwidth usage. In general, the new protocol divided electronic voting into to two classes:
1) Decentralized elections where the protocol is essentially run by the voters.
2) Centralized elections where trusted authorities are employed to administer the process.

The goal there-fore was to eliminate the use of a trusted third party altogether. The first round in the two-round protocol consisted of every participant to publish his public key and a zero knowledge proof (ZKP) for his private key. When the round finished, each participant checks the validity of the ZKPs and computes. In the second round, each participant needs to demonstrate that the encrypted vote was one of the valid voting choices without revealing which one. The authors in [5] have proposed the first implementation of a decentralized and self-tallying internet voting protocol with maximum voter privacy using the Block chain, called The Open Vote Network (OVN). The OVN is written as a smart contract for the Ethereum block chain. It is costing 0.73$ per voter. In this system the voting is conducted in an unsupervised environment. The OVN is also vulnerable to denial-of-service The implementation is feasible only for small boardroom voting, with the disadvantage that each voter has to download the full Ethereum block chain to confirm the voting protocol is being executed correctly.

A multi authority secret-ballot election scheme which would guarantee privacy, universal verifiability and robustness, where voters would participate using a PC, where the main consideration is the effort required of a voter [8]. In this model, voters cast their vote by posting ballots to a bulletin board. The bulletin board works as a broadcast channel with memory to the extent that any party can access its content but no party can erase anything from the bulletin board. The ballot does not reveal any information on the vote itself but is ensured by an accompanying proof that the ballot contains a valid vote. The final tally, the sum of all votes, which occurs when the deadline is reached, can then be obtained and verified, by any observer, against the product of all submitted ballots. Which would ensure

universal verifiability, due to the homomorphic properties of the encryption method used? While this proposal can scale up to large elections better than the previous ones, it does have limitations.

Netvote[9] is a decentralized block chain-based voting network on the Ethereum block-chain. Netvote utilizes decentralized apps for the user interface of the system. The Admin dApp allows election administrators to set election policies, create ballots, establish registration rules and open and close voting. The Voter dApp is used by individual voters for registration, voting and can be integrated with other devices (such as biometric readers) for voter identification. The Tally dApp is then used to tally and verify election results.

Netvote supports the three main types of elections as:
1) Open Election: Anyone may vote
2) Private Election: Only authenticated and authorized individuals may vote
3) Token-Holder Elections:

Another approach that only voters who operate accounts that have a balance of a designated compliant token may vote is implemented on Ethereum network. Here the people who do not even have an Ethereum wallet are allowed to vote. Users can give votes through their Android device or directly from their Ethereum wallets, and these transaction requests are handled with the consensus of every single Ethereum node for e-voting [10]. In [11], the Block-chain-enabled e-voting (BEV) is implemented to reduce voter frauds. Eligible voters can cast their vote through a computer or smartphone. BEV uses an encrypted key and tamper-proof personal IDs for e-voting. Block chain is offering new opportunities to develop new types of digital services. In [12], block chain technology is used for electronic voting that could be used in local or national elections and help to increase the trust of voters as well as governments.

III. PROPOSED METHODOLOGY

The objective of this paper is to develop a safe and secure tool for voting over the internet and this tool is E-Matdaan. The step by step execution of the framework of the E-voting is, Firstly the user registers for an electronic ID, a user chooses a PIN number for its corresponding ID consisting of 6 numbers. A user will therefore identify himself in the voting booth by scanning his ID and providing his corresponding PIN number to authenticate himself to the system.

Using the following methods:

1) Any computer in any voting district can be used by any eligible voter to vote, by checking its authentication. As the wallet for the corresponding voter has information about the voter.
2) On successful authentication, the corresponding smart contract which is a ballot is prompted for choosing the candidate to which the user wishes to vote.
3) Voter now must re-enter the corresponding PIN number for his electronic ID for casting vote. 4) Once the vote is signed the data is verified by the district node. If the node accepts the vote data, the vote data must be agreed upon by the majority corresponding district node.
5) If the majority of district nodes agree upon the vote data, consensus for the particular vote has been reached. The user then receives the transaction ID for the corresponding transaction of his vote in the form of a QR-code and the option to print the transaction ID. After this,

smart contract adds one vote to the party for which the user has voted for. This functionality is used for voting and displaying results at district level.
6) Now all the received and verified transactions are added as blocks in the block chain after the threshold time is reached. The block chain is then updated with the entry of every new block and each district node updates this copy of the ledger as in fig3.

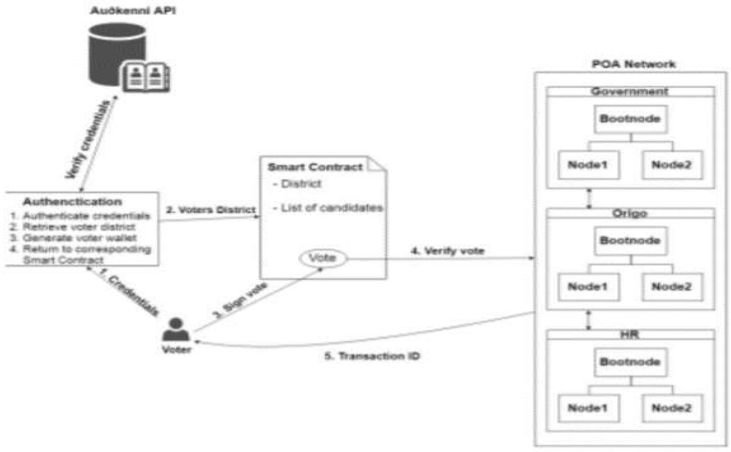

Fig. 3: E- voting proposed Methodology

IV. IMPLEMENTATION AND RESULTS

This section illustrates the design and functional phase of our application E-Matdan are shown in Fig. 4, 5, 6 and 7.

The different phases of the tool are discussed below:
1. **Registration Phase:** The Voter has to register itself first with its unique id and attributes such as name and mobile number. All this data is stored in the database.
2. **Login:** The voter after registration tries to login using password. After successful login, to cast their vote voter has to authenticate themselves using OTP authenticity.
3. **Blockchain Technology**: Blockchain encrypts the vote casted using Asymmetric encryption algo-rithm. A public key is provided by Blockchain, and private key is with the host. Public key is used for verification purposes by the ledger.
5. **Ethereum Network:** Ethereum network provides a framework for blockchain creation and stor-age. Every block is created and its details are stored in an encrypted ledger using Solidity. These created blocks are distributed among nodes which provide high fault tolerance to the system.

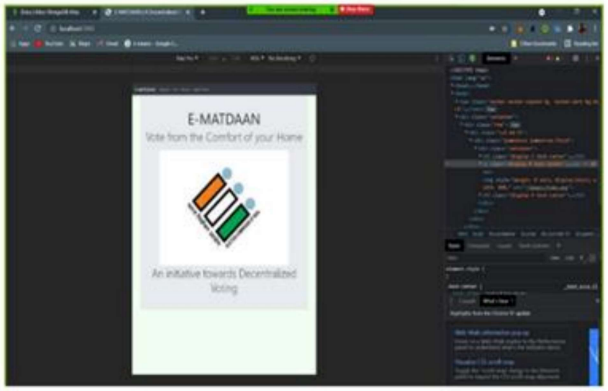

Fig. 4: Home Page of E-Matdaan

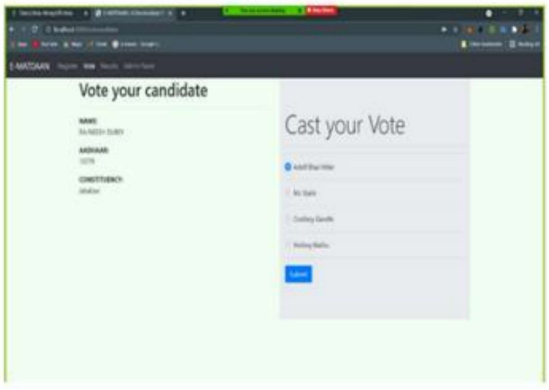

Fig. 5: Voting Page of E-Matdaan

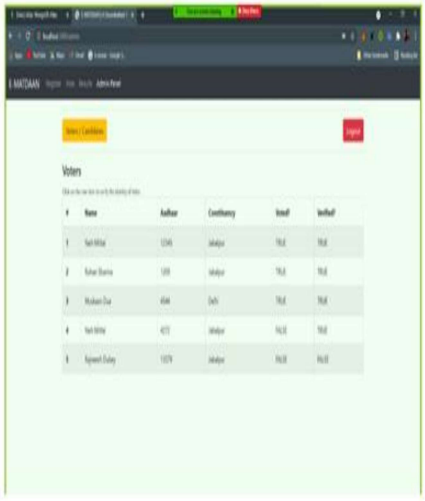

Fig. 6: Admin section of E-Matdaan

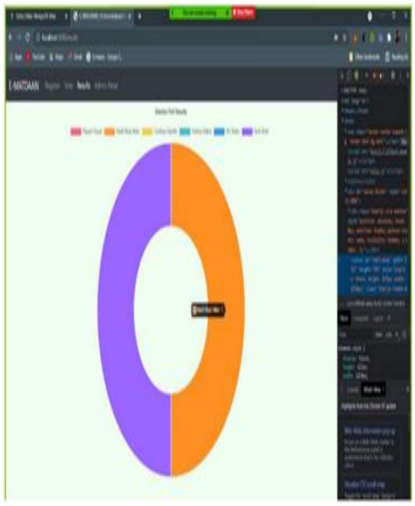

Fig. 7: Results Section of E-Matdaan

V. CONCLUSION AND FUTURE DIRECTIONS

In this research paper a smart and secured tool – E-Matdaan for safe and secure voting using block-chain has been proposed. The block chain has been implemented using the Ethereum network. The idea of adapting digital voting systems to make the public electoral process cheaper, faster and easier, is a compelling one in modern society. Making the electoral process cheap and quick, normalizes it in the eyes of the voters, removes a certain power barrier between the voter and the elected official and puts a certain amount of pressure on the elected official. It also opens the door for a more direct form of democracy, allowing voters to express their will on individual bills and propositions.

We have outlined the systems architecture, the design, and a security analysis of the system. By comparison to previous work, we have shown that blockchain technology offers a new possibility for democratic countries to advance from the pen and paper election scheme, to a more cost- and time-efficient election scheme, while increasing the security measures of

today's scheme and offering new possibilities of transparency. Using an Ethereum private block chain, it is possible to send hundreds of transactions per second onto the block chain, utilizing every aspect of the smart contract to ease the load on the block chain. For countries of greater size, some measures must be taken to withhold greater throughput of transactions per second, for example the parent & child architecture [28] which reduces the number of transactions stored on the block chain at 1:100 ratio without com-promising the network's security. Our election scheme allows individual voters to vote at a voting district of their choosing while guaranteeing that each individual voters vote is counted from the correct district, which could potentially increase voter turnout.

REFERENCES

[1].Van der Elst, C., & Lafarre, A. (2017). Bringing the AGM to the 21st century: Blockchain and smart contracting tech for shareholder involvement. European Corporate Governance Institute (ECGI)-Law working Paper, (358).
[2].Jonéus, C. (2017). Analysis of Scalable Blockchain Technology in the Capital Market.
[3].Gupta, A., Patel, J., Gupta, M., & Gupta, H. (2017). Issues and Effectiveness of Blockchain Technology on Digital Voting. International Journal of Engineering and Manufacturing Science, 7(1), 20-21.
[4].Henning, J., & Schreiber, R. (2014). The Bitcoin Protocol. Technische Berichte des Hasso-Plattner-Instituts für Softwaresystemtechnik an der Universität Potsdam, 18.
[5].Saad, M., Spaulding, J., Njilla, L., Kamhoua, C., Shetty, S., Nyang, D., & Mohaisen, D. (2020), Exploring the attack surface of blockchain: A comprehensive survey. IEEE Communications Surveys & Tutorials, 22(3), 1977-2008.
[6].Lazarenko, A., & Avdoshin, S. (2018, November). Financial risks of the blockchain industry: A survey of cyberattacks. In Proceedings of the Future Technologies Conference (pp. 368-384). Springer, Cham.
[7].Springall, D., Finkenauer, T., Durumeric, Z., Kitcat, J., Hursti, H., MacAlpine, M., & Halderman, J. A. (2014, November). Security analysis of the Estonian internet voting system. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (pp. 703-715).
[8].Eze, P., Eziokwu, T., & Okpara, C. (2017). A triplicate smart contract model using blockchain technology. Circulation in Computer Science-Special Issue, 1-10.
[9].Mus, K., Kiraz, M. S., Cenk, M., & Sertkaya, I. (2016). Estonian voting verification mechanism revisited. CoRR, abs, 1612.
[10].E. Yavuz, A. K. Koç, U. C. Çabuk and G. Dalkılıç, "Towards secure e-voting using ethereum block-chain," 2018 6th International Symposium on Digital Forensic and Security (ISDFS), 2018, pp. 1-7, doi: 10.1109/ISDFS.2018.8355340.
[11].N. Kshetri and J. Voas, "Blockchain-Enabled E-Voting," in IEEE Software, vol. 35, no. 4, pp. 95-99, Ju-ly/August 2018, doi: 10.1109/MS.2018.2801546.
[12]. Ayed, A. B. (2017). A Conceptual Secure Block chain-based Electronic Voting System. International Journal of Network Security & Its Applications, 9(3), 01-09.

