International Journal of Emerging Research in Engineering, Science, and Management
Vol. 2, Issue 1, pp.13-19, Jan-Mar 2023.
www.ijeresm.com eISSN – 2583-4894

General Voting System for Democratic Countries Using Blockchain and Computer Technology

[1]Vandanababu Talakayala, [2]Dr. Prashant Dahiwale, [3]Sanjay Mate

[1,2,3]Lecturer in Computer Engineering, Government Polytechnic, Daman

Abstract: Secret voting in democratic countries using computational intelligence and Blockchain Technology, the vote is a fundamental right in democracy to elect people's representatives at various levels. Manual voting is tedious and error prone. E-voting systems replaced the manual voting systems to overcome illegal voting and malpractices. Due to growing cybercrimes, the existing e-voting systems are not ideal and face many challenges like authentication, privacy, data integrity, etc. This paper presents computational intelligence and Blockchain technology in developing secret e-voting systems. This paper addresses various issues not addressed by traditional and e-voting systems and proposes new voting using computational intelligence techniques and blockchain technology.

Keywords: Blockchain, EVM, Paper Ballot, Information Security.

1 INTRODUCTION

Considering a country like India, anyone who is a citizen of India and is 18 years or older is eligible to vote in the elections. However, before doing so, the applicant is required to register themselves. There are two ways for voter registration activity online and offline based. In the offline method, a citizen has to apply for inclusion of name for first-time voter or on shifting from one constituency to another, by submitting Form 6, which is an application form for including a name in the electoral roll designed by the Election Commission of India (ECI) with valid identification proof like an Aadhar card issued by the Unique Identification Authority of India (UIDAI). After verification and approval, authorities will give a voter identity. Form 6A is available for overseasor Non-Resident Indians (NRIs) people to register as voter in the country. With proper approval of authorities, Form 8 can be used by the election commission to update voter information like age, address of current residency, name, and photo. Form 6, Form 6A, and Form8 are available on the NVSP website [1].

In the process of elections in democratic countries like (India), there is an Election Commission (EC), it frames all election rules starting from forming constituencies, voter registrations, polling dates declarations, taking nominations from the contesting candidates, arrangements for polling process, conducting good training to polling staff, conducting polling, and finally declaring the results. The election process seems like a simple, but in countries like India, to conduct the election there are more than 60 crores of eligible voters, almost 50 lack polling staff, and 20 lakh protection or police forces are required. Not only is this, but a good amount of budget also needed. The election commission introduced and had been using an Electronic Voting Machine (EVM) for the last 15 years, before this paper-based polling voting system had used for conducting the elections. In paper based voting system, there is paper called ballot on which all the names and their political party symbols were printed and used by the election commission, voters exercised their votes in a secret compartment in the polling station.

Some of the major drawbacks in this method are vote rejection because many voters due to lack of knowledge might select multiple symbols on a single ballot; the amount of time required or allocated for a voter to cast vote; not only these there are so many drawbacks present in this method. So the election commission introduced EVM based elections to eliminate some the drawbacks like rejected votes issue completely addressed, time required to cast a single vote significantly improved, by this, number of voters to cast vote in a polling booth increased by 30 to 40%. EVM consists of one control unit, ballot units, it is used to collect votes and avoid rigging with technical time delays; it also produces results in less time than traditional polling ballots. The election commission recently introduced a device to print voter's responses named as Voter Verifiable Paper Audit Trail (VVPAT), which provides immediate feedback to voters and feels that he cast his as per his choice, it brought confidence to voters, they can see the vote symbol for a while through a glass window and stored in a sealed ballot box, can be used during counting time for counter verification of results with the same EVM and that print will be stored in sealed box, It is used during counting time for counter verification of results with the same EVM.

A Software will be loaded into the EVM according to the constituency in which it will be used in polling by the election commission, the software generally includes polling station numbers within that constituency, the number of contesting candidates, storing votes cast by voters, and set system date time. If any EVM is not working correctly during polling, then it will be replaced by the concerned authority. A voter enrolled for a particular ward is supposed to exercise his vote at a designated polling booth only, sometimes this may lead to less voting percentage because, if a voter is in travel or another polling station near him within the same constituency, a voter cannot cast his vote other than the polling booth assigned to him.

https://doi.org/10.58482/ijeresm.v2i1.3

If a voter can be identified as valid by the polling officials in a polling station within the same constituency, he can cast his vote in that polling station near him on election day; the existing system is not designed to manage voters' identity at any polling stations within the same election constituency. With Blockchain technologies, we can manage a voter identity across all polling stations within the constituency, allowing the voter to cast his vote at any nearest polling booth on election day. It will help to increase the voting exercise and overall percentage.

The Blockchain technology has evolved since 1991, starting with Stuart Haber and W Scott. Blockchain has many definitions, but Blockchain is a simple database mechanism that stores the data with high security [2]. In 2008, this technology gained relevance by a group of people named Satoshi Nakamoto. Satoshi Nakamoto is the accredited brain behind digital ledger technology. The new concepts and approaches evolved into the Blockchain mechanism for transformation towards digital data utilization in the year 2009 [3]. There is no way to change that data once data is stored; there is transparency in data storage. Recently using of this technology increased in banks, stock markets, and recent government sectors in the registration of properties like lands, houses, etc between parties.

The Block-chain creates a chain that initiates and manages the ledger state through transactions submitted by applications. This ledger with the data performs secure, tamper-proof transactions and can be easily accessible by the system users. Like the internet, the Blockchain has no central authority; instead, it is a network of transactions shared over a vast network of users. Blocks are added one after another to the Blockchain, where each block contains a header, timestamp, the previous block's hash, and data of the current block. If data on any block is changed, then its hash code changes, by this next block no longer points to the last block; hence the newly modified data will not fit into the chain of data and this is the main objective of the technology to bring transparency in the data. Blockchain data will be stored in encryption form as Hash code; even if a hacker accesses the data node, he cannot change that data. This technology can be used by all two-party agreed transactions [2].

This technology can be applied to the voting process so that the public can cast their votes through a mobile device like cell phone, tablet, or within premises offered by the election commission. In [4], the possibilities and challenges in designing a Blockchain-based voting system were discussed. In elections, if the technology is used by the election commission and found that there is a significant impact in decreasing organizational cost and increasing voter turnout, then it will be a big step towards democracy. It eliminates the need to print ballot papers or open polling stations—voters can vote from wherever there is an Internet connection. Despite these benefits, online voting solutions are viewed with a great deal of caution because they may introduce new threats. Each vote is added to the chain of data blocks in the Blockchain with the header, the previous block's hash code, voter identity, election officer identity, timestamp. Once a block of information known as the node is attached to the Blockchain list, further cannot be changed. It puts a solid control to resist malpractices possible in the election process like casting another person's vote.

Counting is a technical platform-based task, and it is straightforward to follow. It accesses all symbols marked from each Voter and consolidates constituency-wise, candidates-wise, total votes cast and verified, and it uploads results statistics into the election commission server. In a paper-based ballot, counting took place full day for one constituency, votes from two or three polling stations were mixed and separated candidate-wise marked ballots into a bundle of 25 each, this is repeated for all booths in that constituency, and these bundles are counted for each candidate and the candidate who got a greater number of votes declared as winner in that constituency by the election commission. In this process, many possible errors may take place in bundle making process, method of mixing candidate ballot into other by human error, this will become a big drawback for a very narrow margin wins if it happens in 10 to 20 percent of total bundles.

In EVM-based elections counting time required for a constituency reduced drastically in 2 or 3 hours compared to the traditional ballot paper-based method, rest of the process for conducting the election is almost the same like paper-based elections. Sometimes EVM may not work during counting time due to technical errors. The results were declared based on the majority votes among the two contesting candidates. A drawback is that it reveals ward-wise people's majority choice; it may lead to some opinion on the political parties on that ward. Suppose in some wards, if a more significant number of votes are cast to NOTA (none of the above), i.e., most of the public not interested in any candidate, once results announced the ruling party might neglect this ward in granting government schemes.

Voatz established a smartphone-based voting system based on Blockchain technology to cast votes remotely and anonymously and verify that the vote was counted correctly [5]. Voters confirm their application with the voting system themselves by giving identification proofs, including biometric confirmation such as fingerprints or retinal scans. However, this is not suitable for countries like India, where many people do not have good smartphones, internet connectivity, and literacy to operate and use App.

1.1 Causes for Developing Online and Intelligent Voting System

Eligibility and Availability: The objective is to avail the voting facility to every eligible citizen of the country from any corner of town or village. This system reduces travel time in the traditional allotment of the booth to exercise the vote. It is more helpful for old age people and physically disabled people too.

One Citizen One Vote: An eligible citizen can cast their vote once in each election; ease of casting a vote increase the voting percentage. The rise in voting percentage is a moral victory of democracy.

Privacy: A voter can also see a vote log for any election post declaration of elections, with proper login authentications and verification.

Fairness and Completeness: No one knows the results in the middle of the election process. All eligible voterchoices should be tally correctly and were included in the final results.

1.2 Existing and Previous System

Voters are categorized based onward the number. An election constituency has several ward voters. Ward number is the number assigned by the local authorities to identify the population count in each town, village, and district, usually for electoral purposes or to extract property and locality details [6].

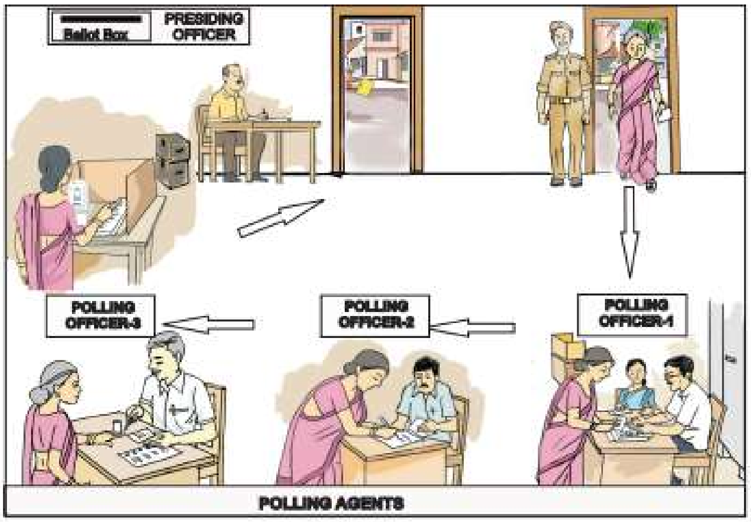

Fig. 1. A ballot paper-based voting system at a polling station [7]

The ballot paper-based voting system at polling station [8] as shown in Fig. 1, voter proceeds on successful voter verification as per data present with Polling Officer I. If a voter belongs to the assigned polling booth, then Polling Officer II records the list of voters who utilized their vote in that booth. Polling Officer III provides a paper ballot where a voter executes their choice on the ballot in a secret compartment provided, then the voter folds the ballot and puts it in the pre-locked ballot box. All ballot boxes were transported with high security to the designated place to store, and finally, on counting day, those boxes were opened and counted as directed.

The EVM-based polling replaced the traditional paper ballot unit, and it is a set of devices (EVM) like Control Unit, ballot unit, and VVPAT, as shown in Fig. 2. In EVM-based elections, Polling Officer I and II have the same job roles as specified in figure 1, and Polling Officer III has the control over the key/button of a control unit that initiates a session for one vote exercise for a single time as the voter cast his vote session ends.

The Control unit stores all voters' responses, handled by Polling officer III during polling. Voter comes in interaction with ballot unit to where a list of Election contesting candidates and symbols are given, and voter responds by pressing a button in front of the name and logo of that candidate. VVPAT (Voter Verifiable Paper Audit Trail) is a pre-locked will be placed in a compartment with privacy where the voter casts his vote and verifies the symbol of his choice on the VVPAT screen 7 seconds. This vote displayed on VVPAT will be stored for counting if needed. The ballot unit is associated with light and beep sound that confirms response to VVPAT.

In both Paper Ballot-based and EVM-based models, the amount of time for the election process is the same, during the counting process EVM based works far better than the first one. Before the poll day, one or two polling officers need to do a lot of preparatory work like writing addresses on the envelopes, filling various judicial and non-judicial forms to be submitted to the election commission. After polling, all the items should be sealed as per directions given by the election commission and transported with tight security to a specified location and kept under surveillance up to counting day.

The only difference between paper-ballot-based and EVM-based elections is storing of the votes and amount of time for declaring results, the remaining election activities are the same. Here we are proposing an intelligent voting system where it can transform the entire election process.

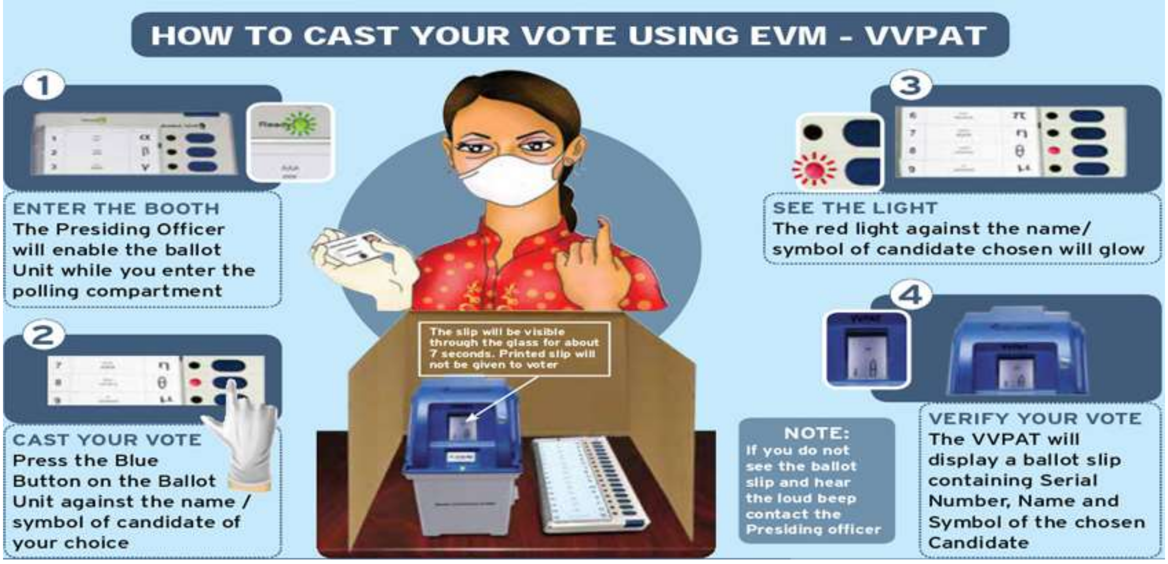
HOW TO CAST YOUR VOTE USING EVM - VVPAT
1
ENTER THE BOOTH
The Presiding Officer will enable the ballot Unit while you enter the polling compartment
2
CAST YOUR VOTE
Press the Blue Button on the Ballot Unit against the name / symbol of candidate of your choice
The slip will be visible through the glass for about 7 seconds. Printed slip will not be given to voter
3
SEE THE LIGHT
The red light against the name/ symbol of candidate chosen will glow
4
NOTE:
If you do not see the ballot slip and hear the loud beep contact the Presiding officer
VERIFY YOUR VOTE
The VVPAT will display a ballot slip containing Serial Number, Name and Symbol of the chosen Candidate

Fig. 2. An EVM based voting system at polling station [9]

2 PROPOSED SYSTEM DESIGN

In this process, Voter Registration, Conducting Election, Counting, and Declaring Results are the three typical stages present. All these stages are continuous, completely computerized, any single event happens will be stored by the new voting system in permanently, this typical design is main advantage of this voting system, where as in previous voting methods with help of computers and spreadsheets software the stages were executed, these stages are discrete, and independent with each other, if any error in previous stage is may be ignored in later stage or handled separately by the election commission.

1. Voter Registration: This is the first stage or also called pre-process of election process, voter registration is mandatory to all eligible citizens to be a member on voter list to cast their votes. The system allows only voters who register with the system in the stipulated time given by the election commission.
2. Election Process: This is the crucial stage where the actual election process takes place by following protocols and guidelines specified by the election commission.
3. Declaring Results: Final stage is counting the polled votes and result declaration by the election commission.

Once a voter casts a vote, it cannot be verified or identified by the voter in the existing system. In the proposed Blockchain-based system, every voter can verify their vote with the system before result declaration, which doubles the faithfulness of the system.

2.1 Voter Registration

Every voter has to register within the new system with details such as voter identity number given by the election commission along with identification proofs issued by respective governments which consist of the date of birth, address details, photo, etc. Ward Numbers designated by the election commission [6], the identity of the ERO (Electoral Register Officer), timestamp. Figure 3 shows the model of a node or a block in the Blockchain voting system.

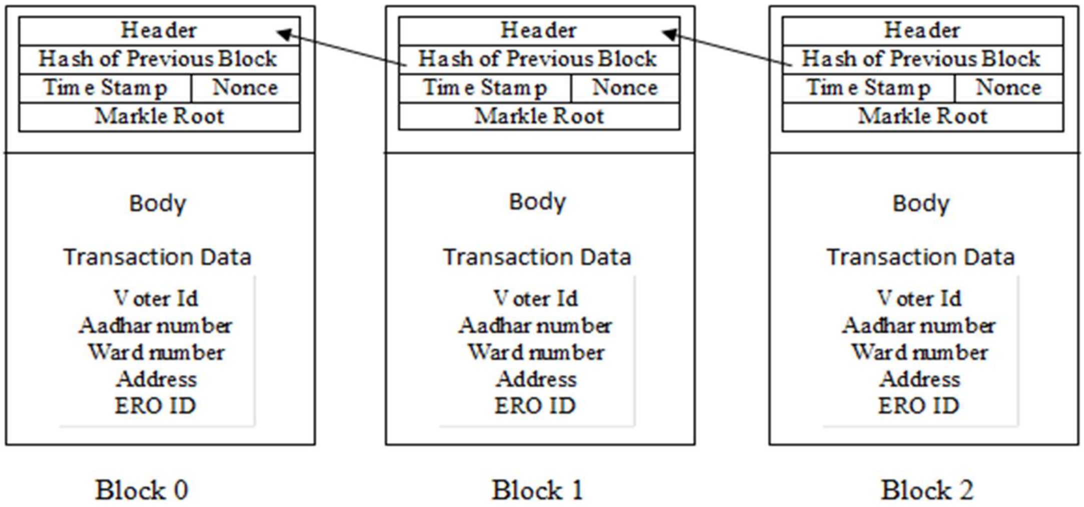

Fig. 3. Model of Node in the Blockchain

Initially, if voter registration is completed with the new system, then a new node with all the information related to voters will be added to the voting system once it is added to the system will never be deleted or tampered with. This technology eliminates false voter enrolment by the election commission. If any voter tries to register in more than one place can be recognized by this new technology, and duplications can be avoided countrywide by the new voting system. Every eligible citizen can register as a voter by themself online by uploading all relevant documents, for the people who are not having an online facility to register can complete registration at specified offices arranged by the election commission. Voter data like identity numbers, ward number, address, and ERO identifying combination becomes a body of transaction data, as shown in figure 3. As new voter registers into the system, a new node is created and is added to the system as shown in figure 4. All the computing processors within this system will verify the new node by comparing its hash value with the previously added node; if it matches, then only this new node will be added by the voting system. This process can be done in parallel and decentralized within a constituency. The system will follow an intelligent contract mechanism like Ethereum [8], which is a platform to facilitate decentralized smart contracts via Ether.

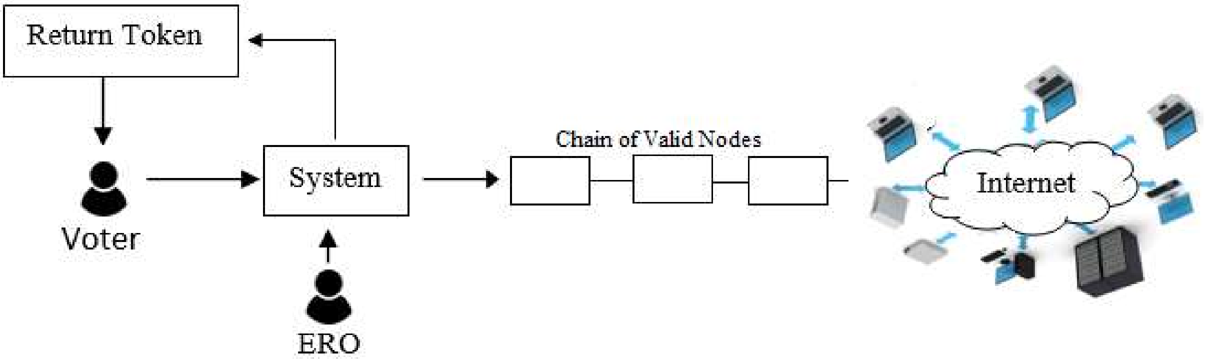

Fig. 4. Registration of voters for electoral roll

Smart contract [11] refers to the idea that legal agreements can be notarized and executed automatically. The rule followed in the systems is that every node should contain valid data, including ERO identity and a hash of the previous node then only the new node will automatically add into the voting system. Finally, the voter list can be generated based on the constituency, district, and state levels.

2.2 Election Process

In two ways election process can be conducted by the election commission: Mobile App-based and another uses a polling booth-based voting system. First approach needs a robust technical infrastructure in terms of data security, network, the internet, server response time, etc. It is more suitable for a few voter elections or picking someone from elected members like elections in the assembly hall or conference hall-based polling. In a framework with good technology and infrastructure, if elections are not conducted in free and fair, and if it is influenced by political people may lead to unfair practices; there are more chances for unfair practices in the first approach. Second approach is recommended for the general election in a country like India, where a few crore voters exercise their votes. In the second approach polling booth-based voting system, each registered voter has to go to a designated polling booth or any polling station within the same constituency premises. Then the following steps will be executed during this entire process by the election team.

1. Each Voter needs to produce a voter identity or token details generated at the time of voter registration or any valid identity or can use scanners for biometric-based identification to initiate the voting process.
2. The Polling officer will enter details after the duly verification, the system generates a unique token; the same token will be stored in it for future reference.
3. The system will generate an e-ballot and send it to the ballet unit with polling officer identity, voter identity, and a list of symbols of contesting candidates.
4. In a privacy-maintained cabin, a voter can execute his vote by choosing one of the symbols on that e-ballot. If required, the symbol on the ballot can be printed and collected directly into a pre-locked box.
5. A new node with e-ballot, previous e-ballot hash value, the system timestamp will be stored as a node by the voting system.
6. Every voter can be given a post-vote receipt; with this receipt, the voter can verify his vote with the system even after polling up to some days before or after counting to ensure his or her vote remains in the system and brings full faith on with a single mouse click, the counting process can be processed, and results can be declared with the voting system by the election commission.

This process is repeated for all eligible voters at that polling station as per the time guidelines provided by the election commission. The chain of nodes looks like as shown in Fig. 5.

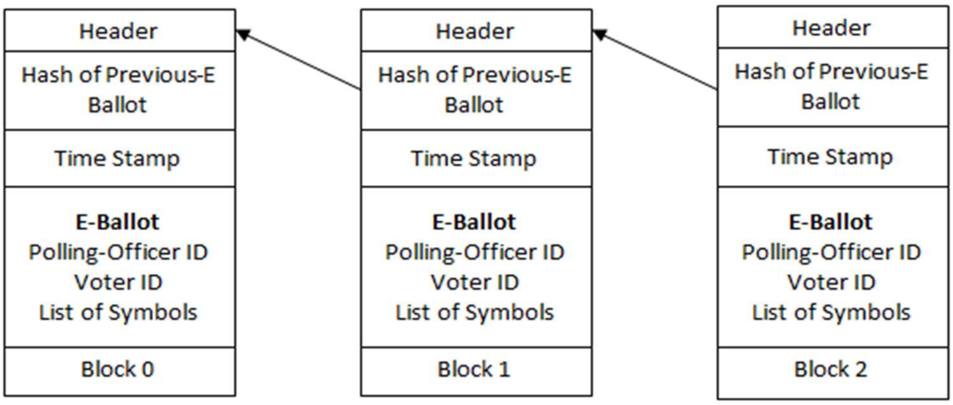

Fig. 5. A chain of nodes in a proposed Blockchain-based polling system

Every time a new node is created by the voting system as above said, it must be stored in the Blockchain voting system by the process of “Smart Contract”. Ethereum acts as a smart contract, is a decentralized blockchain platform that establishes a peer-to-peer network that securely executes and verifies application code [12]. These smart contracts are also used in logistic systems to bring greater trust [13], [9] discussed how to use Solidity and Ethereum in developing smart contracts. Here the rules for a smart contract will be a valid token of a voter, polling officer identity, valid timestamps, and a hash of the previous node, after some time if anyone tries to change the node’s e-ballot symbol of the existing node the system automatically detects and discards those nodes. Anyone trying to intrude from another system can be discarded by simply checking their systems identities. The exact process, similar to Fig. 4 polling, will be conducted in a parallel and decentralized way. Every block, as shown in Fig. 5 transmitted to the system and verified by innovative contract programs then stored into the system. Before adding an e-ballot into the system, which will be encrypted with any Public-Private Key algorithms [14] so that others cannot see the data present in the e-ballot.

This model will be best suited for countries like India, as most of the complexity in preparation and verification of voter lists, ballot boxes transport, collecting hourly based poll percentages, and many other things will be done automatically by the voting system; half of the polling staff can be reduced, human errors can be reduced to 100% in the election process. Polling booths usually schools/colleges/offices, where a good number of computers are equipped, we can use them wisely.

2.3 Declaring Results

Blockchain technology allows voters to cast their votes from any booth in a designated constituency, and these votes are stored in the voting system constituency-wise. The counting process can be processed with a single mouse click, and results can be declared with the voting system by the election commission. When compared with results of paper-based polling, EVM-based polling conducted by the election commission, these results are 100% acceptable because there is no single person involved in calculating these results.

A voter can verify vote pre and post result declaration for up to a few days to ensure the correctness of the system, and the data on the system tampers proof. Counter verification can bring full faith on results by verifying printing the results from the Blockchain system to the voter slips already printed and stored in pre-locked boxes at the time of Election. Any 15 to 20 percent booths can be selected randomly for counter verification in a constituency to ensure the effectives of the system.

3 IMPLEMENTATION, TESTING AND LIMITATIONS

The proposed Block-Chain based voting will address this problem by correctly identifying voters, and there is no need to fill in a voter-marked list. Need not write addresses on covers because everything is programmed and stored concerning constituency. Even polling staff can be reduced to 2 to 3 instead of 5 to 6 members by the election commission. There is no need to worry about the transportation of ballot boxes EVM machines because each vote when cast, is automatically stored in the distribution chain of systems across the constituency and to the election commission networks.

The process will be as follows:

```
1. Go to polling station XYZ
2. A Recognized Voter of that constituency AND not cast a vote in any other
polling booth within the constituency
        Voters are allowed to cast a vote.
        It is marked as Voter as cast in polling booth XYZ.
        A new node will be generated with voter id, booth id, the symbol chosen
        as a vote by the voting system. All are encrypted and added to the chain
        of Nodes with the previous node hash and time stamp.
Else
        Not allowed to cast
```

4 CONCLUSIONS

This paper presented a solution for a transparent and more responsible and tampered proof system for the election from beginning to end. Even the election commission of the democratic countries is looking for these types of systems. There were issues in implantations like initial budget, lack of professional expertise, technical infrastructure covered on the requirement of setting up for the state or countries. This paper will contribute as knowledge for those willing to design or develop a system for polling-based activities with recent technologies.

REFERENCES

[1] National Service portal of India https://www.nvsp.in/

[2] M. R. Manu, Namya Musthafa, B. Balamurugan, and Rahul Chauhan, "Blockchain Components and Concept', Pg 21-50, Blockchain Technology and Applications, CRC Press, ISBN: 978-0-367-53340

[3] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," 2008. [Online]. Available at https://bitcoin.org/bitcoin.pdf.

[4] Jafar, U.; Aziz, M.J.A.; Shukur, Z., "Blockchain for Electronic Voting System—Review and Open Research Challenges," *Sensors* 2021, 21, 5874. https://doi.org/10.3390/s21175874

[5] Voatz. Voatz—Voting Redefined ®®. 2020. Available online: https://voatz.com

[6] Local government directory of India https://lgdirectory.gov.in/welcome.do?OWASP_CSRFTOKEN=HLJ6-WTC2-1069-R7GA-L1QN-UGOI-KJP8-LPPC)

[7] https://ceomanipur.nic.in/documents/elc/Chunav%20Pathshala.pdf

[8] Election commission of India, resource guide, Chunav Pathshala https://ceomanipur.nic.in/documents/elc/Chunav%20Pathshala.pdf

[9] https://cdn.s3waas.gov.in/s32b44928ae11fb9384c4cf38708677c48/uploads/2021/11/2021110849.jpg

[10] C. Dannen, "Introducing Ethereum and Solidity foundations of cryptocurrency and blockchain programming for beginners," in *Proceedings of the 1st International Conference on Internet of Things and Machine Learning*, IML '17, New York, NY, USA, pp. 73:1–73:8, ACM, 2017.

[11] Public-Key Cryptosystems Ronald L. Rivest, Adi Shamir, and Leonard M. Adleman. Communications of the ACM 21, 2 (Feb. 1978). *Communications of the ACM*, *21*, p.2.

[12] V. Buterin, "Ethereum white paper: a next-generation smart contract & decentralized application platform," https://github.com/ethereum/wiki/wiki/White-Paper, 2013.

[13] N. Álvarez Díaz, J. Herrera-Joancomartí, and P. Caballero-Gil, "Smart contracts based on blockchain for logistics management," in *Proceedings of the 1st International Conference on Internet of Things and Machine Learning*, IML '17, New York, NY, USA, pp. 73:1–73:8, ACM, 2017.

[14] B.H.Linganna, G. Dedeepya, Sk. Ayesha Sultana, T. V. V. Satyanarayana, "ALO Based Robust Cryptographic Scheme," International Journal of Advanced Research in Computer and Communication Engineering, Vol. 5, Issue 5, May 2016, pp. 830-833.