International Journal of Future Generation Communication and Networking
Vol. 13, No. 2, 2020 pp.1206-1221

A Secured End to End E-Voting Using Ethereum Blockchain

N.Prasath,
Associate Professor,
Communication Networks Research Group, Department of Computer Science and Engineering,
KPR Institute of Engineering and Technology, Coimbatore, Tamilnadu, India

Abstract

The new approach for e-polling includes a centralized structure that regulates the whole voting process, to deliver returns and electoral supervision. In the meantime, the technology blockchain provides a decentralized system, opening the entire network of non-confident parties. Blockchain Technology can instill protections such as data secrecy, data honesty and data validity in the e-voting framework. The introduction of intelligent agreements, as in the Ethereum network, is a important method for decentralization. Intelligent contracts are significant codes which can be inserted into the blockchain and applied as expected in each blockchain upgrade stage. A program for e-voting should be safe, as duplicated votes are not enabled and entirely open while maintaining users' privacy. As a smart contract for an Ethereum network, we have deployed the e-voting program utilizing the Ethereum wallets and the language of solidity. Finally, after a poll, the blockchain in Ethereum can hold the polling and polling history. Users may send their votes from their Ethereum wallets directly and the consent of the Ethereum node is answered in these transaction requests. This agreement creates a transparent e-voting environment.

Keywords: *Blockchain, Ethereum, Smart contract, decentralized application*

I. INTRODUCTION:

Ethereum, with a market capitalization of $870 M in November 2016, is the second most used crypto currency. It depends on Bitcoin's [20] innovation: primarily Blockchain, a pioneer in relation. A decentralized, transparent peer-to-peer network is managed or established through the Blockchain. The Blockchain's aim was to evict banking's centralized position in keeping a financial record. Researchers are currently seeking to recreate Blockchain to address additional transparent problems such as the Internet of Things [12] and health [10]. This paper reflects on the usage of the Blockchain for open Web voting. E-voting mechanisms to support undisputed citizens typically acknowledge the existence of a transparent release board to gives all voters a steady vision. In fact, the regular elections of the International Association of Crypto-Logical Science (IACR) [22] are a case of incorporation of the public advisory council. We are not investigating the possibility of utilizing the Blockchain as a public notice board other than as a confidence statement. In fact, we find that the communication is a democratic election preparation function. In action, firms including The Blockchain Voting Machine and TIVI provide ways to store voting data using Blockchain as a polling tool. Such strategies shield citizens with a power-contained relationship. Ethereum, on the other side, calculates measurement and efficiency directly with a gas metric and as far as possible the gas which its customers will use. For e.g., the stakeholders will vote to hire a new director in the meetings hall. Select the voting protocol of the boardroom as an intelligent ethereal contract. These intelligent contracts provide an interactive programming language and are held on the Blockchain directly. Above all, the contract code is performed separately by both participants on the underlying peer-to-peer network in a agreement on its performance. This implies the electors cannot carry out the entire estimate to ensure whether the procedure is performed.

This chose truffle as production framework and network blockchain. Ethereum is one of the truffle frames. While Bitcoin is intended solely for validating coinage transactions, the Ethereum network offers the capacity of intelligently contractual commerce for a wider variety of applications. Our decentralized technology includes a database operation, which these smart contracts will carry out without a firewall.

All operations are operated on in real time in the Ethereum network, and all blocks in the final chain are written for certain Ethers. They are distributed to the miners who carry out the writing and testing research

ISSN: 2233-7857 IJFGCN

which is exorbitant in time and power measurement. The Ethereum ledger used to operate on a smart contract with the Ethereum Virtual Machine (EVM). The intellectual contract is the position of our lifelong corporate reasoning. The autonomous part of our software is designed with this intelligent contract. Intelligent contracts assume care of interpreting, writing and executing open program knowledge in the blockchain. Intelligent contracts are composed in robustness. Programming language. Throughout the following, the rise of the block chain was addressed.

TABLE 1: The evolution of Blockchain

	Exonum	**Quorum**	**Ethereum**
Consensus	Custom-built BFT algorithm	Quorum Chain, IBFT and Raft-based consensus	PoW, PoS and PoA
Transactions	up to 5000 transactions	Dozens to hundreds	Depends
Private support	Yes	Yes	Yes
Smart Contract Language	Rust	Solidity	Solidity
Programming Language	Rust	Go, C, Javascript	Go, C, Javascript
Decentralized	Yes	Partially	Optional

II. RELATED WORK

Review of various academic papers discussing related fields of study, i.e. electronic voting schemes.

Ahmed Ben Ayed, et. al, (2017) [26] Blockchain provides different opportunities for creating new forms of digital infrastructure. Although there is still work on the subject, the key emphasis is on the technological and legal problems rather than on the application of this modern paradigm and the development of innovative digital services. In this article, we will use the Blockchain open source technology to develop a new electronic voting system that could be used in local or national elections. Blockchain is a secure, trustworthy and anonymous system, which will increase the voting numbers and the confidence of the people in their governments.

Hjalmarsson, F. P., Hreioarsson, G. K., Hamdaqa, M., et.al, (2018) [27] It has for a long time been a struggle to build an online voting program that follows legislation. Significant technological advancement in the area of computation is the distributed ledger technology. Blockchain platforms provide an enormous range of application of open networks. Blockchain is discussed in this article as a method for the introduction of unified electronic voting schemes. The paper explains and analyzes the legal and technologically restricted application of blockchain in order to incorporate electronic voting schemes. The paper starts with an overview of some of the traditional blockchain structures provided by blockchain. We then suggest a new online voting method focused on blockchain that solves all the constraints found. More broadly, this paper explores the ability of distributed headline technologies, including the mechanism of election and deployment of applications centered on blockchains, which boost protection and cut the expense of hosting national elections, through a case study summary.

ISSN: 2233-7857 IJFGCN

Freya Sheer Hardwick, et.al, (2018) [28] In other facets of our daily life, technology has important impacts. The creation of a 24-hour network that is internationally connected enables quick access to a variety of outlets and resources. In fact, technologies such as the Internet became a fertile source for invention and imagination. Blockchain – a core feature in crypto currency – is one such technological breakthrough. The blockchain platform is viewed with several of the current and new innovations and utilities as a game changeover. It emphasizes on other markets as an equalizing force in the present equality between customer and big corporate governments, due to its immutability properties and decentralized architecture. The blockchain can be used in e-voting systems. A decentralized architecture to run and support an open, fair and independent voting scheme would be the aim of this scheme. In the present article, we propose a possible new protocol on e-voting using the blockchain as a transparent voting box. The protocol is structured to support fundamental e-voting properties and enable voters to change / modify their votes (within the permitted voting period) by providing some degree of decentralization. This paper discusses the benefits and drawbacks that blockchain requires in development / deployment and usage conditions for such a project from a realistic viewpoint. The paper is a potential roadmap that will support diverse implementations for blockchain technologies.

Gaby G. Dagher, Praneeth Babu Marella, Matea Milojkovic, et.al,(2018) [29] A voting system based on blockchain called Bronco Vote which preserves the privacy and transparency of voters while ensuring that the voting system is open, secure and cost-effective. Bronco Vote uses the University-scale Voters Platform to accomplish election administration and auditable voting records via Ethereum blockchain and smart contracts. Moreover, Bronco Vote uses a variety of holomorphic encryption methods to facilitate voters' safety. Our implementation was used for use ability, scalability and reliability on Ethereum Test net.
Hanifatunnisa, R., & Rahardjo, B. October (2017) [30] In the Bitcoin system known as the decentralized bank system, Blockchain itself was used. Through implementing blockchain, one of the cheating causes of database abuse can be the by dissemination of databases on e-voting platforms. This work explores the analysis of voting data from all polling places utilizing blockchain algorithms. This thesis suggested the approach focused on a pre-determined device switch on for each node in the built-in blockchain, as against Bitcoin's work proof.

III. BLOCKCHAIN

Blockchain has established a peer to wallet network, which allows online cash transactions without confidence or the need for a financial institution, first introduced by Satoshi Nakamoto [18]. By its design and a good Byzantine tolerance scheme, Blockchain is safe [19]. Bitcoin is the first use of Blockchain to create a currency that can be transmitted across the Internet using cryptography alone. Blockchain is a distributed data framework for the transaction block. Growing block of chain is linked to the last block of chain. Stack frame is the first component in the series. Any current block is placed above the previous block by a stack named Blockchain.

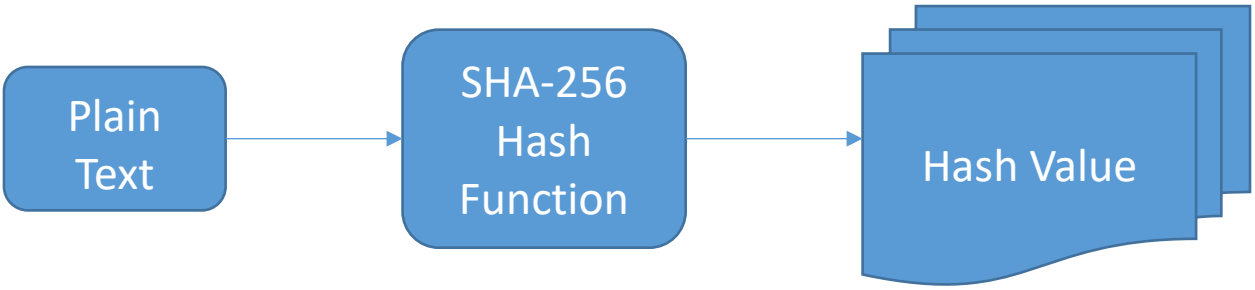

Fig. 1: The basic function of SHA-256

ISSN: 2233-7857 IJFGCN

Any of the blocks in a stack is identified by a hash put on the header. Figure 1 illustrates that this hash has been created using the stable hacking algorithm (SHA-256) to produce virtually fixed 256-bit hash, and the common algorithm was developed by the National Security Authority to protect all contact.

NEW BLOCK

- Hash value
- Vote count
- address

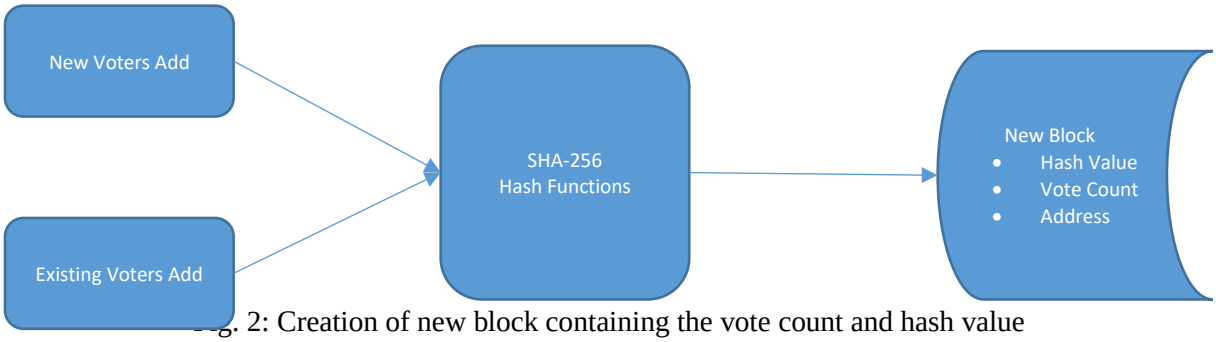

Fig. 2: Creation of new block containing the vote count and hash value

The frame is used to monitor how the blocks approach and continuously update the chain as new blocks emerge. As a block is formed. It should complete the frame feature as shown in the figure 2.

PROPOSED SYSTEM

The election is carried out more securely with the help of Ethereum Blockchain where the first phase is creation of election, followed by candidates registration phase, voting phase and the last phase is the voting and result declaration phase is proposed as shown in the figure 3 which shows the abstract view of an election process.

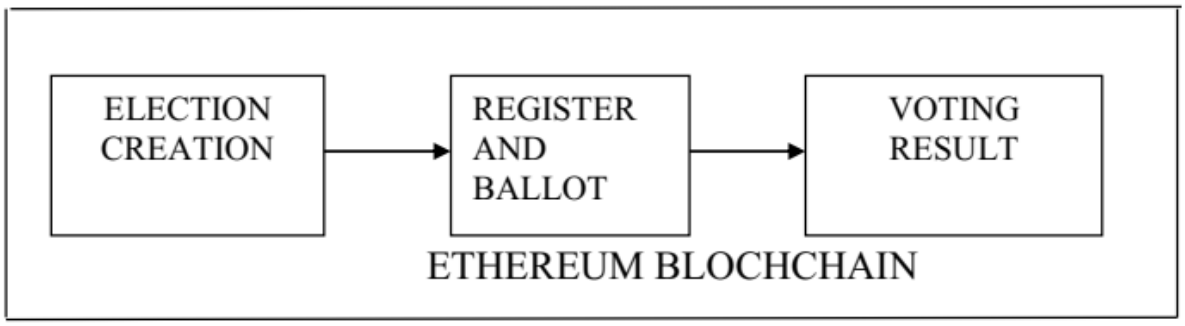

Fig. 3: The election process

Election modules

i. **Administrator** is accountable to set up the initial registration phase and also responsible for creating smart contracts as shown in figure 4. The administrator has the capability to grant and maintain ballot creation permission for registered voters.

ISSN: 2233-7857 IJFGCN

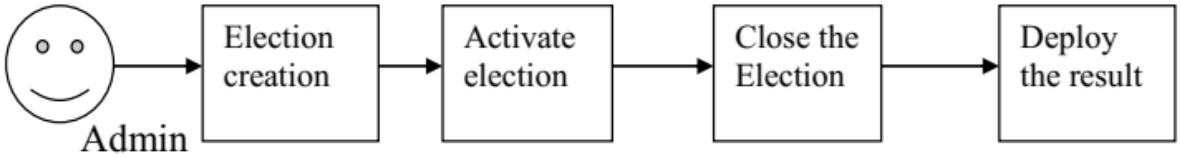

Fig. 4: Election timing module

ii. **Voting.js** gathers information initially and interacts with voting phase and to the Ethereum Blockchain. For each new request voting phase will be contacted which responds after communicating with server and Ethereum for verifying votes and to store vote information.

iii. **Index.html** page is the first interface for the users. This page allows new users also the registered candidates to give necessary information for each of the different use cases.

iv. **Voting.sol** this act a virtual ballot and carries out voting process on the ballot. The figure 5 shows the working of voting phase that how a voter is casting his vote in online starting from registration phase to vote counting.

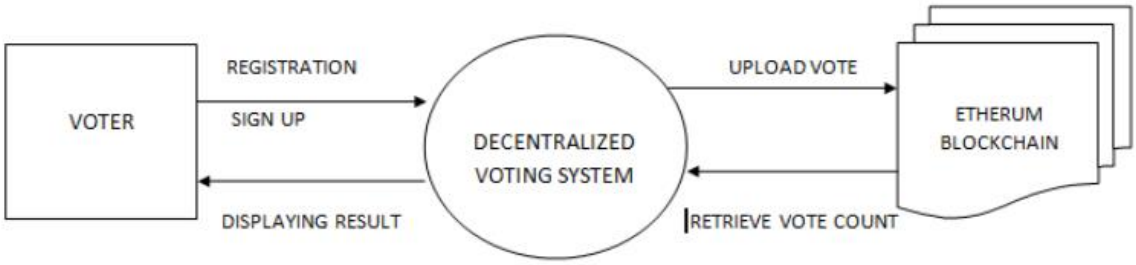

Fig. 5: Dataflow diagram for E-voting system

IV. **Registrar.sol** acts as the record and gate keeper. It keeps track of all registered voters and creators, ballot IDs, voting contract addresses.

IMPLEMENTATION AND DISCUSSION

Our voting method that is applied according to the following scheme.

Election method: Election phase consists of a series of intelligent contracts instantiated by election managers on the block chain. Figure 6 for increasing electoral division, the option of a smart contract is specified, thereby involving several smart contracts. The smart agreement with the respective place will be requested for each elector with his corresponding voting district, identified during the registration period for electors, after the person has authenticated him or herself while voting.

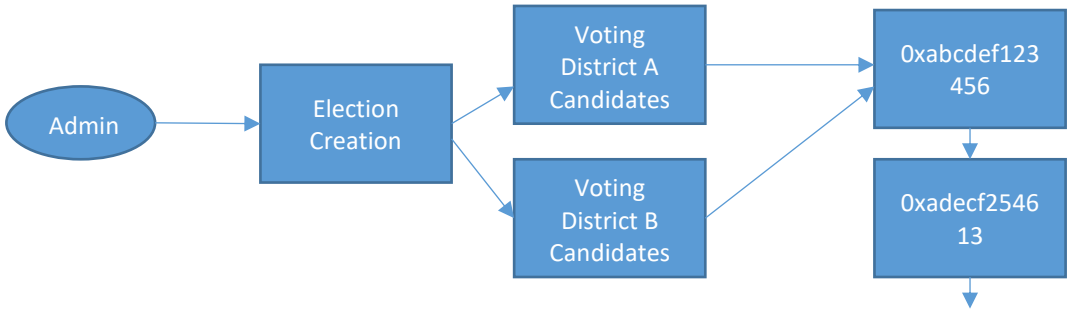

Fig 6: Role of admin in election process

ISSN: 2233-7857 IJFGCN

"Our proposed electronic voting criteria that include:

- System integrity.
- Data integrity and reliability.
- Voter anonymity and data confidentiality.
- Operator authentication".

Administrator: The liable for the execution of initial smart contracts with Registrar and Developer. Administrators do have the luxury of authorizing eligible voters / creators to build a ballot or cancel it.

Voter Register: Voting registers with a valid ID and voting name on the ballot ID numbers issued in our program. The figure 7 shows flow of voter to cast the vote to the prime minister candidate.

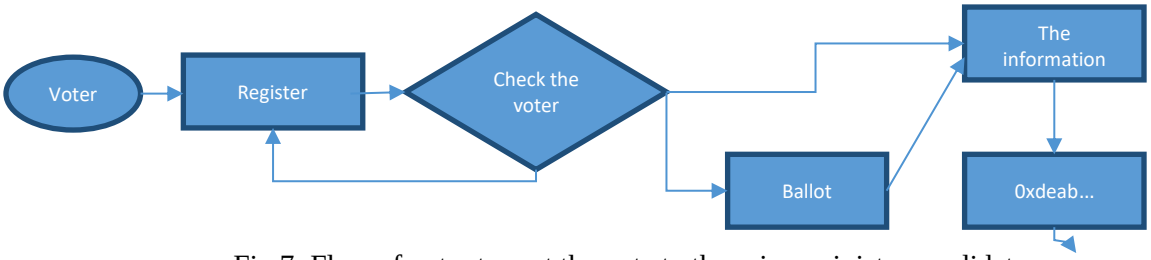

Fig 7: Flow of voter to cast the vote to the prime minister candidate

Creator: It is a elector with approval to construct a ballot. The front / back pages introduced in the Vote are briefly listed as follows:

Index.html: It's the UI for our men. It's website. Users should insert details appropriate for each of the various use cases on this list. When the consumer enters the details required, functions on App.js are activated in the corresponding click buttons.

App.js: It gathers VoteUI.html details and communicates with js file and Blockchain from Ethereum. Eth. calls, server call app.js and Ethereum transactions are used to verify, encrypt / decrypt votes and store the ballot-vote-information for each corresponding request from Index.html.

Registrar. Sol: He serves as the keeper of the ledger. It tracks both eligible voters and developers, voting Ides, and voting agreements. Voting details and different ballots are related in the deal. Figure 8, which allows the voting authentication, adjustment of authorization and the retrieval of the Voting. Sol address by the document. The contractor is the beneficiary of the deal.

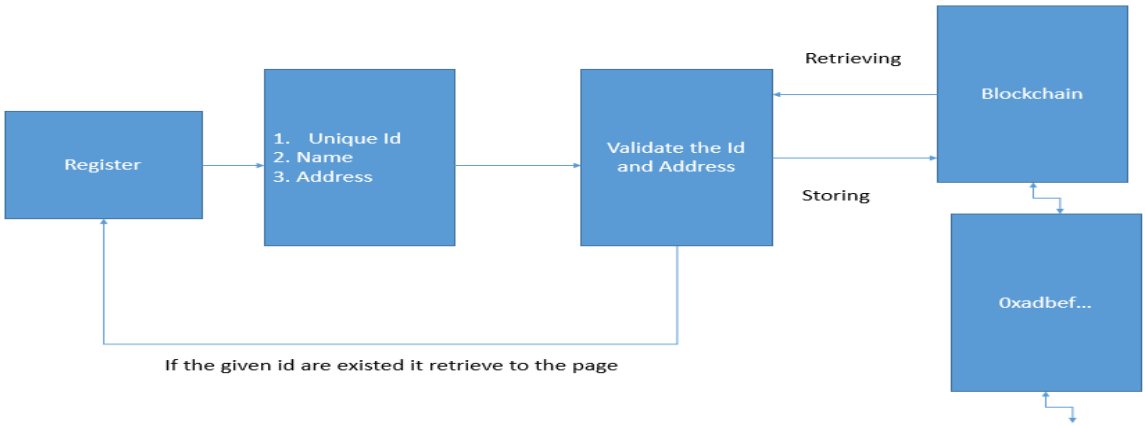

Fig 8: Registration Process

ISSN: 2233-7857 IJFGCN

Voting.sol: It functions as a computer ballot and controls the result. This deal also involves several collection of democratic verifications, including voting attempts and voting duration. The title of ballots and the collection of encrypted ballots are also kept there to enable us to locate them later. The contract owner is the author of the deal.

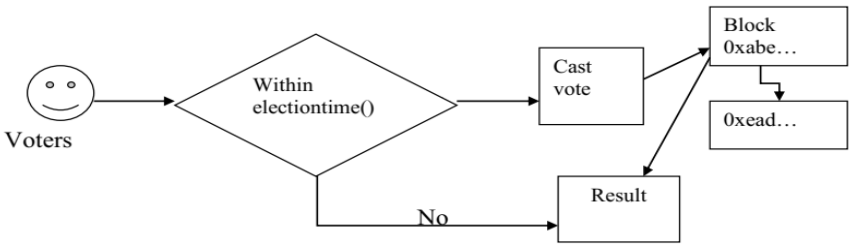

Fig 9: Voting Process

Upon the activation of intelligent contracts, the blockchain cannot be disposed of, figure 9 describes the retention of votes and citizens will observe whether or not the executions outcome of intelligent contracts are valid. No central authority has to supply the proof of work in the Ethereum network. Without interference, every peer node can calculate the results of contracts.

A. ***Designing a Blockchain Voting Mechanism***

The first element is the method of authentication, which involves an elector to validate the reliability of the program. Making sure that the identification of someone is not exploited for fraudulent purposes is critical, especially when voting matters. Such details from the Applicant is used to encourage the consumer to register to vote on our proposed program. This is the aadhar number of the knowledge. This knowledge forms an activity for the individual who identifies with our program to register and then generated this exchange on the voters' network, which vary significantly from the voting network. When everyone has signed in, they will continue voting. You pick your favorite nominee and begin the voting phase. If the candidate has been chosen, a transaction will be performed with the candidate details deposited on the blockchain as shown in the figure 10.

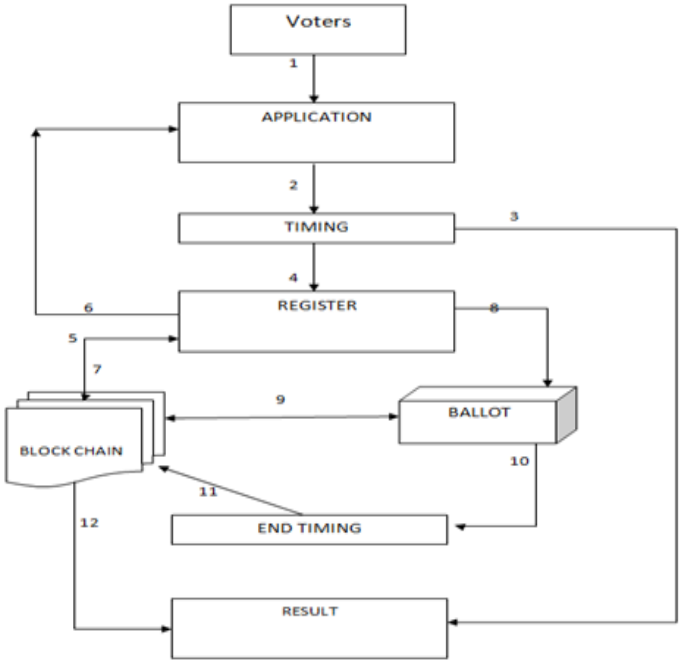

Fig. 10: Overall flow of e-voting system

ISSN: 2233-7857 IJFGCN

1. Interaction of voter
2. Election running time
3 .If election time end the voter won't be allowed to vote.
4. If there is available time the voter accepted to register.
5. Validate the information from the blockchain.
6. If information is invalid it return to main page.
7. If valid data get stored in blockchain.
8. After registration the voter permitted to cast.
9. The casted vote store in blockchain.
10. After the voter complete his vote he may wait until time end.
11. When the time gets end, this system request the blockchain to calculate the vote.
12. The calculated vote get displayed.

E-voting is a 2-round open system for small-scale board voting and much more. Both the electors declared their intention to vote in the first round, and both voters cast their ballots during the second round. The programs presume that all electors are willing to reach an authorized broadcast service.

Round 1. In order to display exponent xi information on the public newsletter floor, per voter Pi broadcasts their voting key g xi and Zero-knowledge proofs ZKP (xi). As proof of Schnorr[32], ZKP(xi) is applied using the heuristic Fiat Shamir[15], which has been rendered non- interactive. Finally, before computing a list of reconstructed keys, all voters will review the validity of all zero-knowledge evidence.

Round 2. The g^xiyi g^v and the (non-interactive) zero-kennt proof are transmitted by each elector in order to demonstrate that v is either no or yes (regarding 0 or 1) votes. The Cramer and Schoenmakers (CDS) development applies this one-of-two zero-knout proof [7]. 4 Before calculating the count, all facts must be checked in order to ensure properly shaped authenticated votes.

All voters who have broadcast in round 1 their voting keys shall transmit their encoded voting in round 2 if the election count is to be process able. In fact, the last voting to disperse the encrypted vote is able to determine the count until the encoded vote is shared in Round 2. He will adjust his option of vote according to the determined count. We address this problem in our implementation by requiring all voters to vote before they are revealed. This adds another compromise round to the protocol. The open design of the Open Vote Network allows Blockchain implementation. Bitcoin's blockchain can be used for store voting data for the free vote network as the public newsletter platform. It needs, though, that the polling process be applied manually by the electors. They plan then to use Ethereum to execute the implementation of the voting protocol. It can be used as a universal machine that can store and execute programs. Conceptually Ethereum. Such ventures are written as smart contracts, using the same network trust that secures the Ethereum blockchain in order to guarantee their accurate implementation. The central peer-to-peer network will also function as a documented medium for contact.

The following method is primarily taken into account in our e-voting program

B. The role of timers:

The poll administrator sets out a number of occasions that improves Ethereum's timely advancement. During the SETUP process there is a fixed time interval μ (in seconds), such that any step stays stable for no less than a duration period μ. The laws, particularly

TfinishCommit − TbeginElection > π and TfinishVote − TfinishCommit > π

We are obligated to allow electors ample time to register and approve. The whole process will be committed once the time is over and show candidates' results.

ISSN: 2233-7857 IJFGCN

C. Voter Registration

The code displayed in the chart. 1 shows the term's definitions. 'Voter' is a word in wellness education language. We named and grouped electors. Voters have those features and could have far more depending on the case of usage. The term "voted" is a marker that indicates whether or not electors have already cast their ballots. 'Vote' factor often stores the electoral choice for each of the candidates, which are called proposals in a more detailed sense (defined as the proposal structure). The ID is a wallet address for a voting account of the Ethereum network.

Algorithm 1: voter registration

1. **Procedure** ElectionRegisteration(_voterAdd,_name,_voted,true,_Id)
2. voterAddress ← _voterAdd
3. name ← _name
4. voted ← true
5. candidateId ← _Id
6. require (time now()>ElectionTime)
7. then return (result)

A genesis contract will be inserted in the blockchain after the authentication of an election (Algorithm 1). This contract of genesis provides all the material required for the validity and placing of ballots, to guarantee that no ballots are put after time, no token is put and no ballots are cast if the referendum prohibits these bales. The document frequently includes other details that anyone involved in the referendum will have free access to. This material comprises the number of individuals on whom a vote will be made and the order of the bulk of the judgment. Once the contract is formed, the customer in control of moving the contract into the blockchain must pass on this details. This is then placed in the condition of the arrangement.

D. Casting a vote:

The amount of votes is the sum of transfers sent to the account of a nominee. An individual who wants to take part in an election merely produces his or her private key and opens his or her address to cast his or her vote.

Algorithm 2: casting a vote

1**: Procedure**
Vote (unit _candidatedID,name,voterAdd)
2: **require** (ElctionEndtime()>timenow() and verify(voterAdd))
3: new vote (_candidateID)
4: procedure vote (_candidateID)
5: votecount++
6: vote←true

You will display the vote algorithm. At the election is held the beneficiary of the deal, which was once named during the creation of the contract. The owner of the agreement will fulfill this role. A fundamental reason can be given for this property. The registered Voter (wallet) address is then granted the voting privilege. The individual with the Ethereum address, which was decided by the referendum, is entitled to vote under this contract. The elector must also apply the election ID that is used exclusively to mark this vote along with the election they have voted for. This prohibits a candidate from putting many deals on the blockchain

ISSN: 2233-7857 IJFGCN

E. Vote transaction:

In a voting district, youth voters communicate with a smart polling arrangement for the same polling district as specified by each electorate. This logical agreement interacts with the blockchain via the corresponding district node like voting whether the plurality of district nodes approve. — Voting is registered as a transaction in the Blockchain, while each individual candidate obtains the Transaction ID for authentication. The details of who and the polling position are available for each blockchain transaction. Only when the corresponding geographic nodes decide to verify the results will the resulting voting smart contract attach any vote to the blockchain.

If the candidate casts his or her vote, his or her weight in his or her purse is reduced by 1. As can be seen in Table I, the transaction Name, the transfer row, the transaction date, the bill that sent and who got the transfer, the total sum sent and the expense of the transaction is shown on the public ledger of Ethereum. All of this information does not include a transaction in our proposed system; a single transaction just requires specifics on the Transaction ID which is the basis for the smart transaction.

This knowledge is accessible in French only. Therefore, no details on the actual voting elector in our scheme is given by a transaction, see table II and example for transaction is given in table III order to shield specific citizens from timing violence, a single transaction is omitted.

TABLE II: Example of a public transaction (Ethereum)

TxHash	Block	Age	From	To	Value	TxFee
0xabcd...	1337	33 sec	0xabbee...	Token	10 Ether	0.087
0xefff...	1337	33sec	0x42fe...	0x1234...	1 Ether	0.056

TABLE III: Example of a transaction in our system

TxHash	Block	To	Value
0xdeadbeef...	1337	N1SC	D
0xG1345edf...	1330	N2SC	P

F. VOTING RESULT:

Returns the winning candidate's ID in the get winning candidate vector introduced in algorithm 3. The election cycle will not resolve itself, but any time it is executed, it returns the winning nominee. This feature monitors will execution, counts the votes and returns the individual who is the winner in the overall voting cycle because the election does not end.

Algorithm 3: count the result

```
1:procedure countingvote
2:require(electiontimeend()<timenow())
3:if maxVote<voteCount[i] then
4:maxVote ← voteCount[i]
5:maxVoteCandidateid ← i
```


ISSN: 2233-7857 IJFGCN

6: **return**(candidateId,name,maxVote)

The following statistics was derived from our electronic e-voting program developed and applied. The unified e-voting program produces a mobile interface where you can use Java script, JS and solidity.

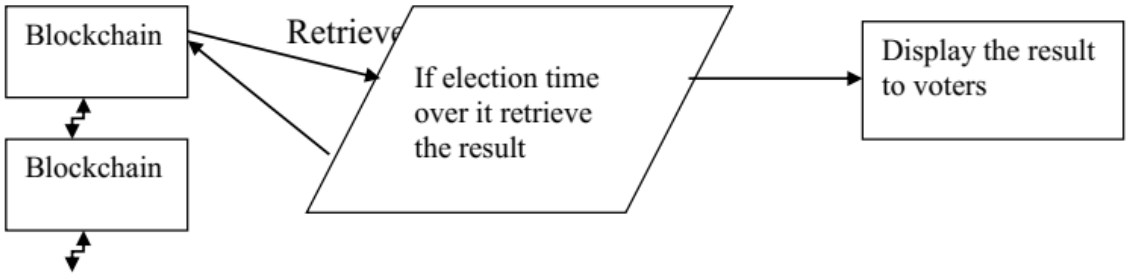

Fig. 11 **Result retrieve from Blockchain**

Figure 11 is used to insert relevant details, such as specific name and number, into this voter's registration process. It will save in blockchain after entering the details. This method is performed only after a given period has elapsed. If this page crosses time and displays the outcome of the decision automatically.

Registration Phase:
The voter has register his user credentials with any one of this identity proof and has to create his or her login credentials and once registration is completed the voter is eligible to vote as shown in the figure 12.

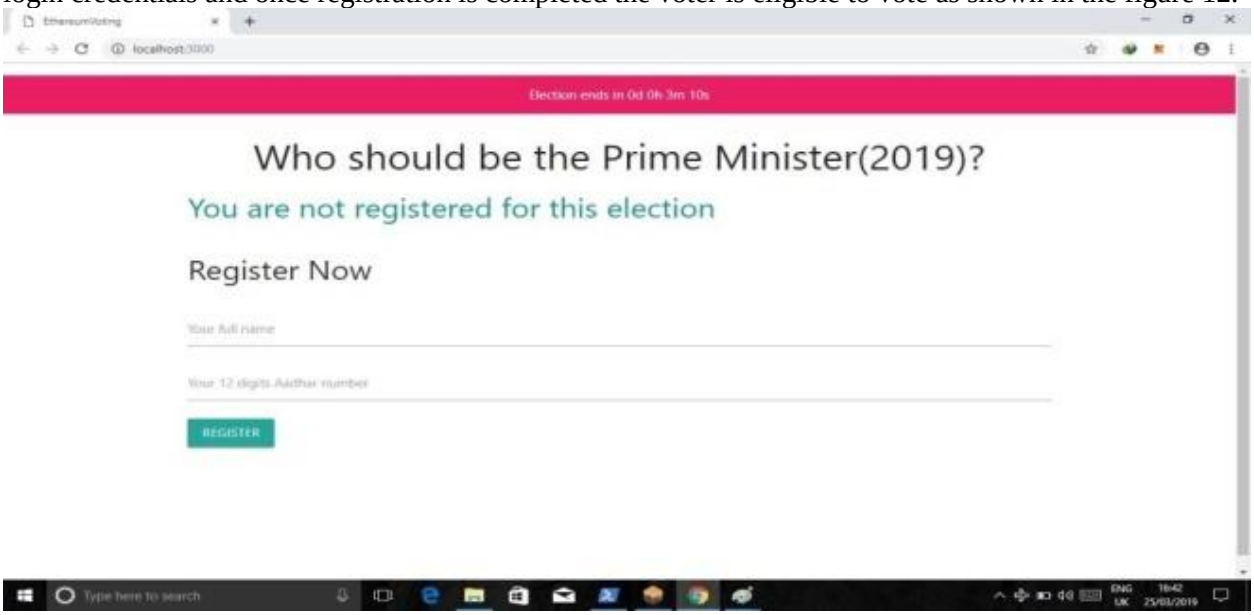

Fig. 12 New candidate registration process

Transaction Phase:

User proceeds with the transaction of ether to register profile in figure 13, User proceeds with the transaction of ether to register profile. As user profile is written into the Blockchain, ether crypto currency must be

ISSN: 2233-7857 IJFGCN

spent by the user.

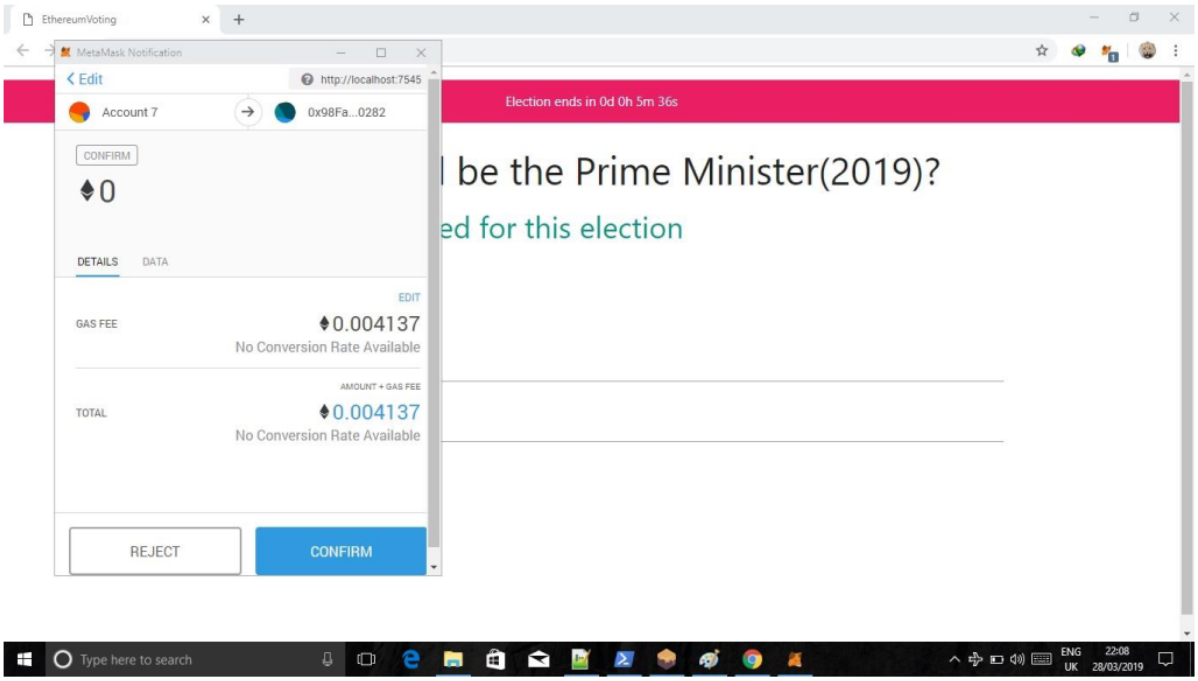

Fig.13: Transaction module

Voter is greeted with the voting page after the user is registered with our system figure 14.

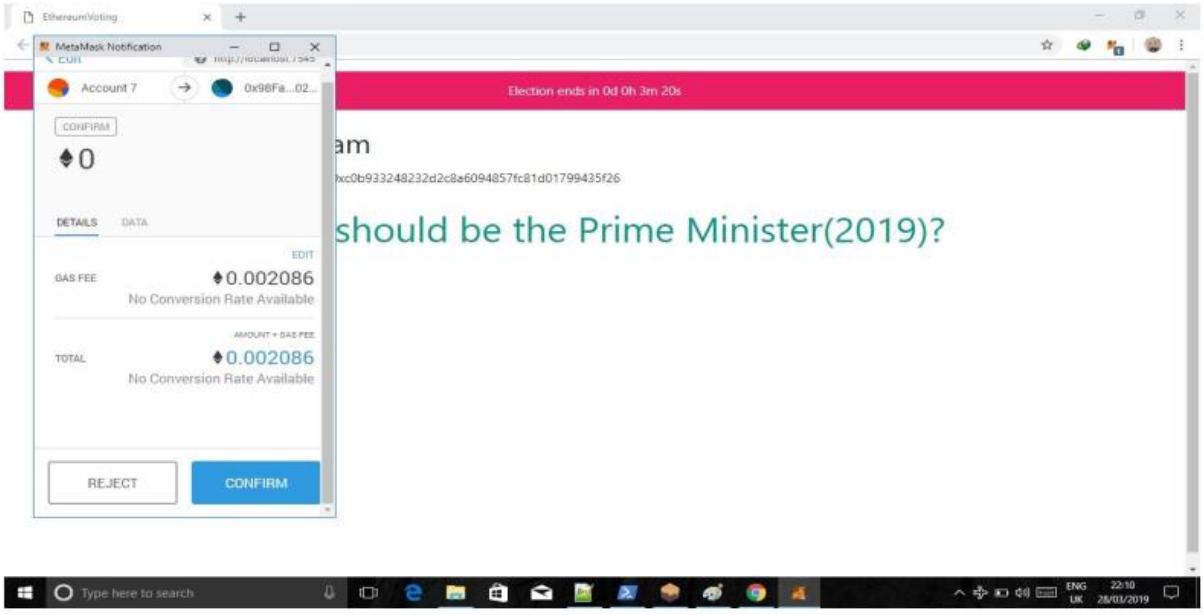

Fig. 14: Vote Transaction module

ISSN: 2233-7857 IJFGCN

Voting Phase:

This Section indicates the number of candidates that are both interested in the race as shown in figure 15. This page may only be accessed and voted by a registered voter. The elector should pick a favorite nominee and cannot vote by revealing any electors. The voter ID may be increased by one of the positive votes in the past and deposited in the Ethereum blockchain. It is difficult to alter their support until voted successfully.

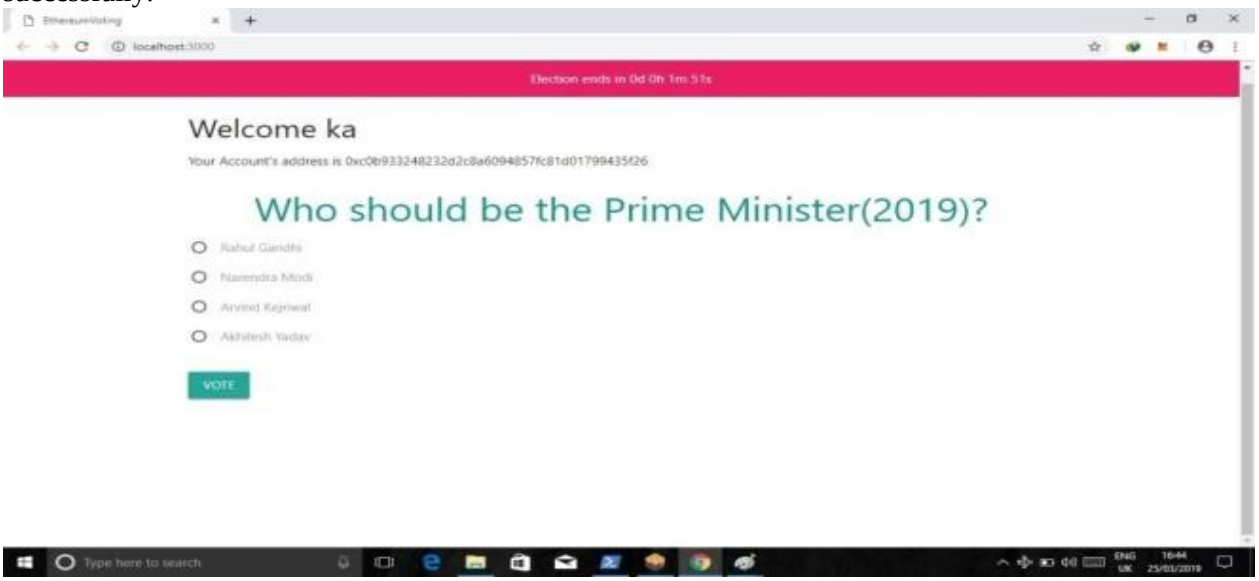

Fig. 15: Candidate participating in prime minister Election

Result Phase:

In Figure 16 the results list only occurs until time is completed. The cumulative count is collected from the ledger and the winner is declared and all the candidates received votes themselves are counted.

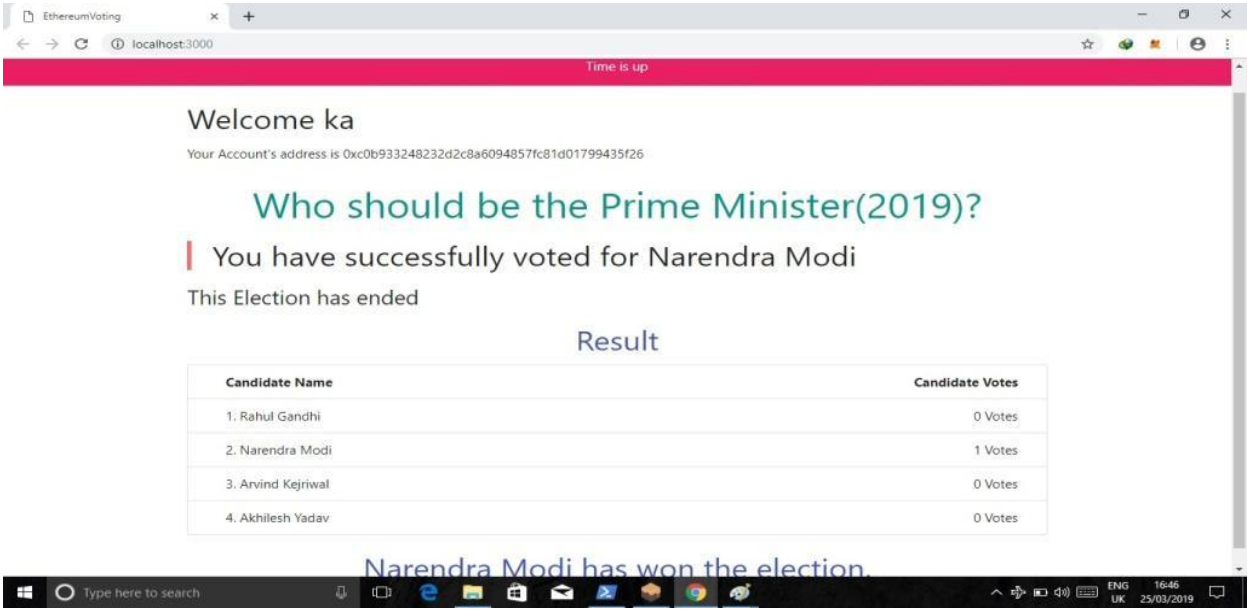

Fig. 16 Result of voting process

ISSN: 2233-7857 IJFGCN

G. Timing analysis:

The table explains measures of the pacing framework for e-voting activities. Both of the tests were carried out on the windows operating OS 10 fitted with 4 cores, 2.3GHz Intel Core i3 and 4 GB DDR3 RAM. We allow communicating between the web viewer and the Ethereum client simpler via the Web3 truffle System. All tasks are performed by RPC call which enables us to calculate the processing time of the code on the local network. The intelligent contract for cryptography shall provide the voters with the zero information proof. For the one-off-two zero-knowledge evidence the time needed for the research is 81 and 461 ms. such acts are only done with. Call), (as transactions can never be made on this deal. The smart voting contract shall follow the democratic procedure. Registering a vote includes verifying the certificate of zero knowledge which in turn needs 142 ms. Casting a vote entails testing the one-of-two zero-information evidence and needs 573 ms. Tiling requires a minimum of all the cast votes and brute-forces the distinct consequence logarithm, which takes an average of about 132 ms as shown in table IV. The programming of the elector's local application is much quicker to run than the usage of a different framework or Open SSL.

TABLE IV: A time analysis for actions that run on the Ethereum daemon.

Action Avg.	Time (ms)
Create ZKP(x)	81
Register voting key	142
Begin election	277
Create 1-out-of-2 ZKP	461
Cast vote	573
Tally	132

This slowness is mainly because the Elliptical Curve Mathematics is not supported by Ethereum's intelligent contracts. The Ethereum Foundation aims to provide indigenous funding and that will boost our reporting greatly.

V. CONCLUSION

The purpose of this paper is to reduce errors in election counting. It reduces the handling of Vote through paper and also secure. By using this voting system, people need not to wait a long time in queue for voting. The project provides the use case with the benefits of cost-effectiveness, Secure and portable. This project's main motto is make transparent, secure and secure the entire voting system Unchanging. The project offers the required features automatic voting updates for each applicant as soon as possible voting is cast, also offers the possibility to view votes of every candidate after immediate election results are declared. It saves a lot in counting the vote and declaring the results. It also contributes to the ratio of voting participation. This system can be implemented for a small locality by the election commission and further can be implemented through the country.

ISSN: 2233-7857 IJFGCN

REFERENCES

1. Hardwick, Freya Sheer, et al. "E-voting with blockchain: An e-voting protocol with decentralisation and voter privacy." *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. IEEE, 2018.
2. Hjálmarsson, Friðrik Þ., et al. "Blockchain-based e-voting system." *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*. IEEE, 2018.
3. Panja, Somnath, and Bimal Kumar Roy. "A secure end-to-end verifiable e-voting system using zero knowledge based blockchain." *IACR Cryptology ePrint Archive* 2018 (2018): 466.
4. Yavuz, Emre, et al. "Towards secure e-voting using ethereum blockchain." *2018 6th International Symposium on Digital Forensic and Security (ISDFS)*. IEEE, 2018.
5. Parycek, Peter, and Noella Edelmann, eds. *CeDEM14: Conference for E-Democracy an Open Government*. MV-Verlag, 2014.
6. Blum, Christian, and Christina Isabel Zuber. "Liquid democracy: Potentials, problems, and perspectives." *Journal of Political Philosophy* 24.2 (2016): 162-182.
7. Neumann, Peter G. "Security criteria for electronic voting." *16th National Computer Security Conference*. Vol. 29. 1993.
8. Rubin, A. D. (2002). Security Considerations for Remote Electronic Voting. Commun. ACM, 45(12), 39–44.
9. Kohno, T., Stubblefield, A., Rubin, A. D., & Wallach, D. S. (2004). Analysis of an electronic voting system (pp. 27–40).
10. Ekblaw, Ariel, et al. "A Case Study for Blockchain in Healthcare:"MedRec" prototype for electronic health records and medical research data." *Proceedings of IEEE open & big data conference*. Vol. 13. 2016.
11. Gramoli, Vincent. "On the danger of private blockchains." *Workshop on Distributed Cryptocurrencies and Consensus Ledgers (DCCL'16)*. 2016.
12. S. Higgins. IBM Invests $200 Million in Blockchain-Powered IoT. CoinDesk, Oct. 2016. http://www.coindesk.com/ibm-blockchain-iot-office/
13. Moura, Teogenes, and Alexandre Gomes. "Blockchain voting and its effects on election transparency and voter confidence." *Proceedings of the 18th annual international conference on digital government research*. 2017.
14. Ayed, Ahmed Ben. "A conceptual secure blockchain-based electronic voting system." *International Journal of Network Security & Its Applications* 9.3 (2017): 01-09.
15. Adida, Ben. "Helios: Web-based Open-Audit Voting." *USENIX security symposium*. Vol. 17. 2008.
16. Aradhya, P. "Distributed ledger visible to all? Ready for blockchain." *Huffington Post* (2016).
17. V. Buterin. Long-term gas cost changes for io-heavy operations to mitigate transaction spam attacks. Ethereum Blog, Oct. 2016. https://github.com/ethereum/EIPs/issues/150, Accessed on 01/11/2016.
18. Nakamoto, Satoshi, and A. Bitcoin. "A peer-to-peer electronic cash system." *Bitcoin.–URL: https://bitcoin. org/bitcoin. pdf* (2008).
19. Reid, Fergal, and Martin Harrigan. "An analysis of anonymity in the bitcoin system." *Security and privacy in social networks*. Springer, New York, NY, 2013. 197-223.
20. Nakamoto, Satoshi. "Bitcoin: A Peer-to-Peer Electronic Cash System. November 2008." *Announced on the cryptography mailing list. URL: http://www. bitcoin. org/bitcoin. pdf* (2015).
21. Ethereum. The mix Ethereum dapp development tool. GitHub, 2016.https://github.com/Ethereum/mix, Accessed on 10/10/2016.
22. International Association for Cryptologic Research. About the Helios system. Oct. 2016. http://www.iacr.org/elections/eVoting/about-helios.html.

ISSN: 2233-7857 IJFGCN

23. J. Groth. Ecient maximal privacy in boardroom voting and anonymous broadcast In International Conference on Financial Cryptography pages 90{104.Springer, 2004.
24. A. Hertig. The First Bitcoin Voting Machine Is On Its Way. Motherboard Vice, Nov. 2015. http://motherboard.vice.com/read/the-rst-bitcoin-voting-machine-ison-its-way.
25. Khader, Dalia, et al. "A fair and robust voting system by broadcast." *Lecture Notes in Informatics (LNI), Proceedings-Series of the Gesellschaft fur Informatik (GI)* (2012): 285-299.
26. Ayed, Ahmed Ben. "A conceptual secure blockchain-based electronic voting system." *International Journal of Network Security & Its Applications* 9.3 (2017): 01-09.
27. Hjalmarsson, F. P., Hreioarsson, G. K., Hamdaqa, M., & Hjalmtysson, G. (2018, July). Blockchain-Based E-Voting System. In *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)* (pp. 983-986). IEEE.
28. Hardwick, Freya Sheer, et al. "E-voting with blockchain: An e-voting protocol with decentralization and voter privacy." *2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData)*. IEEE, 2018.
29. Gaby G. Dagher , Praneeth Babu Marella , Matea Milojkovic and Jordan Mohler. BRONCO VOTE 4th International Conference on Information Systems Security and Privacy (ICISSP 2018), pages 96-107
30. Hanifatunnisa, Rifa, and Budi Rahardjo. "Blockchain based e-voting recording system design." *2017 11th International Conference on Telecommunication Systems Services and Applications (TSSA)*. IEEE, 2017.

ISSN: 2233-7857 IJFGCN