A PROPOSAL OF BLOCKCHAIN-BASED E-VOTING SYSTEM

Dr. B T Prasanna[1], Amogh Mahesh[2], Dakshath K M[3], Nirmal Kuttappa N[4]
[1]Prof., [1,2,3,4]Dept. of Computer Science, JSSSTU, Mysuru, India

Abstract: Designing a secure Electronic Voting Platform that offers reliability and privacy that is necessary to conduct elections and providing convenience and flexibility of online services. In this paper we will discuss the design to build an application for Electronic Voting based on Blockchain technology. We ad-dress important limitations in existing methods such as Voter Anonymity, Data Integrity, etc.. In particular , the main aim of our Blockchain based E Voting System is to improve the security,speed,convenience and decrease the cost of hosting a nationwide election.

Index Terms: E-Voting, Blockchain, Security, Convenience.

I. INTRODUCTION

Electronic voting systems have been the subject of active research for decades, with the goal to minimize the cost of running an election, while ensuring the election integrity by fulfilling the security, privacy and compliance requirements
Replacing the traditional pen and paper scheme with a new election system has the potential to limit fraud while making the voting process traceable and verifiable [2].
A blockchain is a decentralized, distributed, digital ledger that is used to record transactions across many computers so that any involved record cannot be altered retroactively, without the alteration of all subsequent blocks.

- Immutability: Any proposed "new block" to the ledger must reference the previous version of the ledger. This creates an immutable chain, which is where the blockchain gets its name from and prevents tampering with the integrity of the previous entries.
- Verifiability: The ledger is decentralized, replicated, and distributed over multiple locations. This ensures high availability (by eliminating a single point of failure) and provides third-party verifiability as all nodes maintain the consensus version of the ledger.
- Distributed Consensus: A distributed consensus proto-col to determine who can append the next new transaction to the ledger. A majority of the network nodes must reach a consensus before any new proposed block of entries becomes a permanent part of the ledger.[3]

Thus, this paper evaluates the use of blockchain as a service to implement an electronic voting (e-voting) system making the original contributions of Embedding the Blockchain system with email capabilities Sending the private key to the voter's registered email id
to login and vote.

II. RELATED WORK

There has been a lot of work on remote e-voting protocols using cryptographic tools, such as [4,5], etc. In some cases, a trusted third party (TTP) is involved to make e-voting systems more easily implemented and controlled. However, a powerful TTP may also become the vulnerable spot of the whole system. A few efforts have been made to combine an e-voting protocol with the blockchain paradigm to design a voting protocol without a TTP, which provides anonymity and verifiability as well [6]. Zhao and Chan proposed a voting protocol [7] in 2015, which introduces a reward/penalty scheme for correct or incorrect behaviors of voters. Although the protocol has some limitations, this is the first attempt to combine e-voting with blockchain. Later in 2016, Lee, James, Ejeta, and Kim proposed an e-voting protocol [8], which involves a TTP into the blockchain to preserve voters' choices. Very recently, using Bitcoin [9], Bistarelli, Mantilacci, Santancini, and Santini proposed another e-voting protocol
This protocol divides the organizer of elections into two different parts - the Authentication Server (AS) and the Token Distribution Server (TDS), to protect voters' privacy. However, there remain some problems in this protocol, for example, it is difficult to inspect these two parts' behaviors, and it limits the extension of the voting scheme.

III. SYSTEM DESIGN

We have designed the client of the system as follows Fig(1).

- Start the process
- The Voter registers himself using his email address and aadhar number
- Upon validation of the voters' registration details he is navigated to the login page.
- The voter receives a secret pass key to his registered email address
- The user enters the pass key and if it matches with the key sent to the voter's email, he is navigating to the voting page

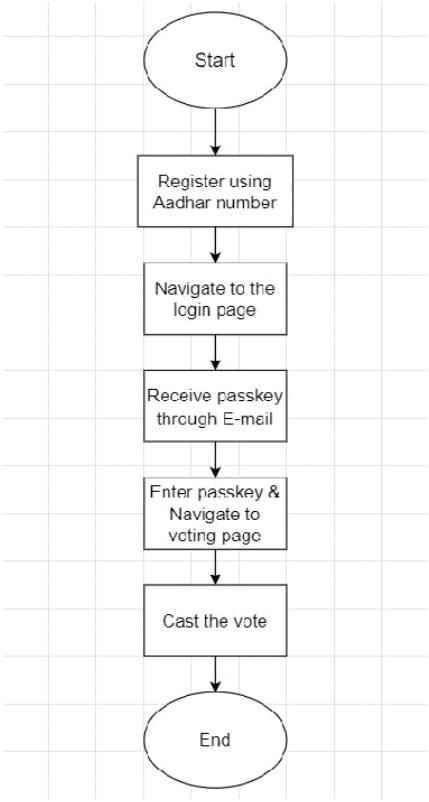

Fig. 1. Client side of the system

- The voter casts his valid vote
- End of the process

The server side of the system is designed as follows:
Fig(2)

- Start the process
- Model the candidates contesting for the election by taking in their credentials such as name, id, election symbols, etc..
- Store the collected information of the candidates
- Store the count of the candidates contesting for the election Voting phase:
- Check for the existence of the voter
    - If he is not present in the database then end the process
    - If he is present the fetch the details of the voter
- Verify the voter's credentials
    - If it appears to be invalid then the voter is not allowed to vote and the process is ended
    - If the voter is valid then further steps are continued
- Check if the voter has already voted.
    - End the process if the result is positive
    - Send the secret pass key to the voter's email address if the result is negative.
- Update the vote count after the voting phase
- End of the process

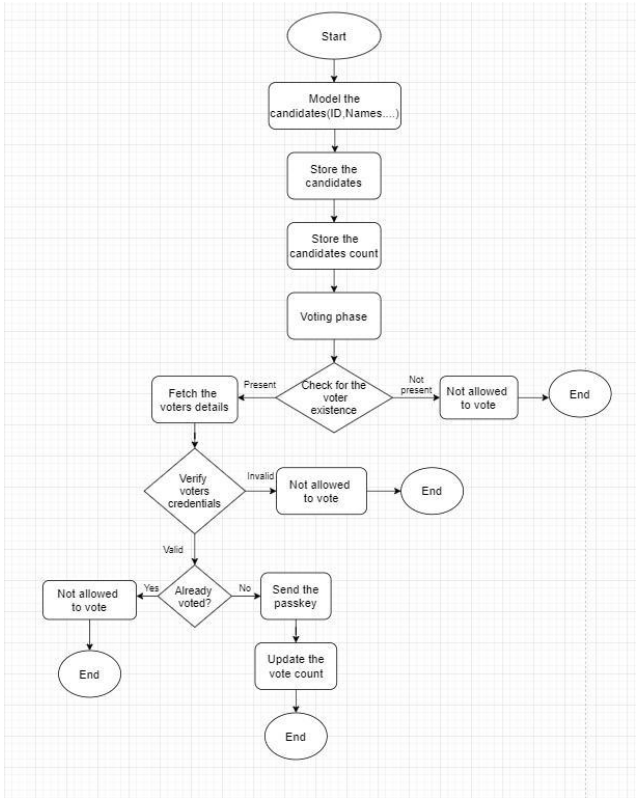

Fig. 2. Server side of the system

The User Authentication of the system is designed as follows: Fig(3)

First, the voter has to open the link of the registration page and register himself by providing his valid credentials such as aadhar card and email id and also a password of his choice.

If any of the credentials is wrong or missing the voter's name will not be enrolled in the voting list and he/she will not be allowed to vote and a relevant message will be displayed on the screen.

If all the credentials are right and matches with the backend credentials then he is navigated to the login page.

The voter must provide the email id and the password in the login page which he had given during the registration process.

By entering the email id and the password the voter will receive a pass key to the same email id. The voter must copy the pass key which was sent to the mail and paste it in the metamask page where the voter will be navigated to. Then the list of the candidates along with their details such as logo, manifesto and so on will be displayed. The voter must vote to the desired candidate within the specified time.

As the voter votes for his desired candidate the voting execution takes place instantly and the page will disable all the buttons immediately such that the voter shall not be able to vote again. At the same time the number of votes of the candidate increases thus ending the voting process from the voter's side.

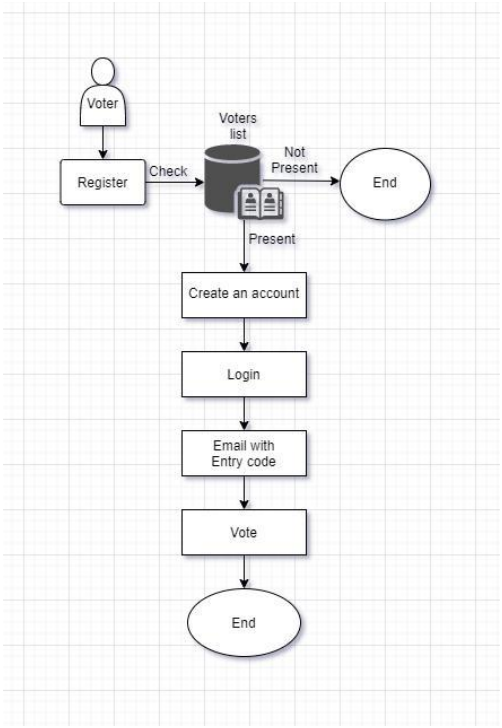

Fig. 3. User Authentication

IV. CURRENT IMPLEMENTATION

In our system we will create a front-end client that is written in HTML, CSS, and Javascript. Instead of talking to a centralized back-end server, this client will connect to a local Ethereum blockchain. We'll code all the business logic in an Election smart contract with the Solidity programming language. We'll deploy this smart contract to our Ethereum blockchain, and allow accounts to start voting.

The Smart contracts are immutable, the business logic once coded and deployed on the network cannot be changed without the consensus of the nodes on the Network.

Every single interaction with the smart contract will be consid-ered as a transaction which will be hashed to provide security. The transactions are stored on the blocks which are mined by special nodes called miners.

Client-side application will have a table of candidates that lists each candidate's id, name, and vote count. It will have a form where we can cast a vote for our desired candidate. It also shows the account we're connected to the blockchain with under "your account". The dependencies used here are Ganache, truffle, metamask,web3js, and npm node packages.

The password which the user enters at the time of registration and login is encrypted using Bcrypt hash. The bcrypt hash has a significant advantage over a simply salted SHA-256 hash: bcrypt uses a modified key setup algorithm which is timely quite expensive. This is called key strengthening, and makes a password more secure against brute force attacks, since the attacker now needs a lot more time to test each possible key.

V. RESULT

The current working model has a smart contract successfully deployed and a front end client that is capable of contacting the business logic. Each voter can register if he/she is in the voter's list and then proceed to enter the network and successfully cast their vote to the Candidate of their choice. The vote once cast will be stored on a distributed network in the form of a block after mining and hence will be nearly impossible to tamper with, without the consensus. Once the vote has been cast, the voter cannot perform any other transaction on the network, that is they cannot cast another vote, only the results of the election will be visible.

The below graphs give an idea of how our method of voting will be much more effecient.

Duration graph (Fig.4)

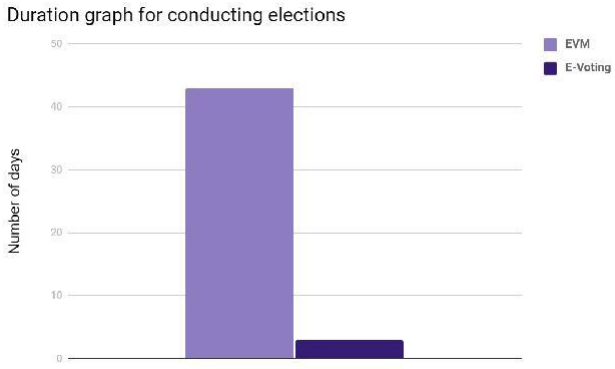

Fig. 4. Duration Graph

The above bar graph depicts the duration for conducting elections.

We can notice that the number of days taken to complete the election process using EVM is over a month, whereas by deploying E-Voting system it can be reduced to 2 days.

One entire day can be given to the voters to cast their votes followed by the second day for result announce-ment.

Thus, we can notice a huge improvement in the duration using this method.

Expenditure graph (Fig.5)

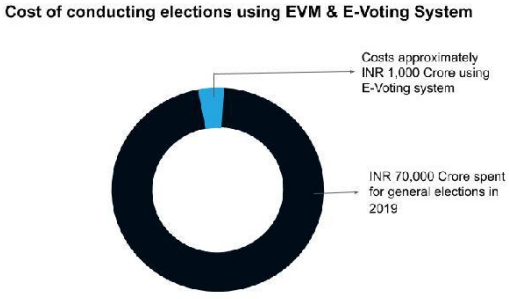

Fig. 5. Expenditure Graph

The Pie Chart shows the cost of conducting elections using EVM and E-Voting System.

We can notice that the region of the chart colored black shows the cost which was spent conducting elections in the year 2019 which was Rs.70,000 crores.

The region of the chart colored blue shows the approxi-mate cost required to conduct an election using E-Voting System.

Cr.1000 System Hardware + Private Blockchain + Proprietary Software + System Maintenance

Thus, we can substantially reduce the expenditure and use it in other sectors.

Comparison between Electors,Voters polled and the Smartphone users.(Fig.6)

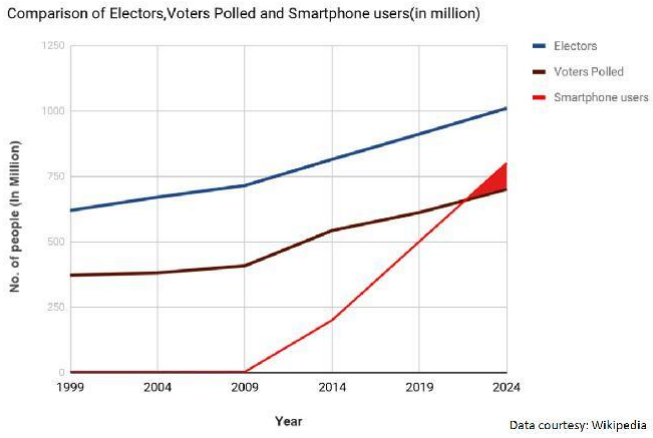

Fig. 6. Line graph to compare Electors,Turnout votes & Smartphone users

The above line graph illustrates the comparison between Electors,Voters polled and the Smartphone users.

We can notice that there is a constant increase in the rate of Electors.

The rate of Voters polled was increased over the period of 2009 to 2014 but the curve flattened there after.

Next, we can see the rapid increase in smartphone users from the year 2009 which is in constant rise till date and will continue to increase at a higher rate in the future according to the analysis.

We can now focus on the intersected region (colored red) between the smartphone users and the voters polled and notice that if the voting system was deployed to be on hands reach this gap can be covered and the voters polled line can be merged with the line of smartphone users and the number of votes casted can be increased by approximately two million.

Thus, the idea of E-Voting System is to cover this growing gap.

VI. CONCLUSION AND FUTURE WORK

In this paper, we introduced a blockchain-based electronic voting system that utilizes smart contracts to enable secure and cost-efficient elections while guaranteeing voters' privacy. We have shown that blockchain technology offers a new possibility to overcome the limitations and adoption barriers of electronic voting systems which ensures election security and integrity and lays the ground for transparency. Using an Ethereum blockchain, it is possible to utilize every aspect of the smart contract to ease the load on the blockchain. And we can also notice how the voters can vote without traveling to an election booth. For countries of greater size, some additional measures would be needed to support greater throughput of transactions per second. Note that, the blockchain technology such as Ethereum is still at its early stages of development and therefore another piece of future work would be the application of the appropriate version of blockchain technology in public sectors to meet and increase the security and privacy of individual's data.

REFERENCES

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

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

[3] Blockchain-Based E-Voting System Friorik P. Hjalmarsson, Gunnlaugur K. Hreiearsson, Mohammad Hamdaqa, Gisli Hjalmtysson School of Computer Science Reykjavik University, Iceland

[4] Adida, B.: Helios: Web-based open-audit voting. In van Oorschot, P.C.,ed.: Proceedings of the 17th USENIX Security Symposium, July 28-August 1, 2008, San Jose, CA, USA, USENIX Association (2008) 335–348

[5] Ryan, M., Grewal, G.S., Chen, L.: Du-vote: Remote electronic voting with un- trusted computers. In Cortier, V., Robbana, R., eds.: Proceed-ings of the Formal Methods for Security Workshop co-located with the PetriNets-2014 Conference , Tunis, Tunisia, June 23rd, 2014. Volume 1158 of CEUR Workshop Proceedings., CEUR-WS.org (2014) 4

[6] Zou, X., Li, H., Sui, Y., Peng, W., Li, F.: Assurable, transparent, and mutual restraining e-voting involving multiple conflicting parties. In: 2014 IEEE Conference on Computer Communications, INFOCOM 2014, Toronto, Canada, April 27- May 2, 2014, IEEE (2014) 136–144

[7] Zhao, Z., Chan, T.H.: How to vote privately using bitcoin. In Qing, S., Okamoto, E., Kim, K., Liu, D., eds.: Information and Communications Security - 17th Inter- national Conference, ICICS 2015, Beijing, China, December 9-11, 2015, Revised Selected Papers. Volume 9543 of Lecture Notes in Computer Science., Springer (2015) 82–96

[8] Lee, K., James, J.I., Ejeta, T.G., Kim, H.J.: Electronic voting service using block- chain. JDFSL 11(2) (2016) 123–136

[9] Nakamoto, S.: Bitcoin: A peer-to-peer electronic cash system (2008)

[10] Bistarelli, S., Mantilacci, M., Santancini, P., Santini, F.: An end-to-end voting- system based on bitcoin. In Seffah, A., Penzenstadler, B., Alves, C., Peng, X., eds.: Proceedings of the Symposium on Applied Computing, SAC 2017, Marrakech, Morocco, April 3-7, 2017, ACM (2017) 1836–1841

[11] A framework of blockchain-based secure and privacy-preserving E-government system Noe Elisa 1 • Longzhi Yang 1 • Fei Chao 2 • Yi´Cao 3 O The Author(s) 2018

