STRUCTURE AND DEVELOPMENT OF AN E-VOTING SYSTEM UTILIZING BLOCKCHAIN TECHNIQUE

Muralidhara S,
Assistant Professor,
Computer Science and Engineering,
NHCE, Bengaluru, India

Abstract: In recent years voter apathy has been increasing, especially among the younger computer/tech generation. For a robust e-voting scheme, a number of functional and security requirements are specified including transparency, accuracy, auditability, system and data integrity, secrecy/privacy, availability and distribution of authority. The idea in blockchain-enabled e-voting is to use a digital-currency analogy; BEV issues each voter a "wallet" containing a user credential. Candidates need to register themselves for the election process before the deadline. After the deadline, smart contract which is a set of rules that governs the interaction of users on the blockchain will be deployed containing the candidate list. Private keys will be sent to the voters a week prior to the Election Day through the registered mail. A confirmation sms will also be sent about the mail. Voter should not disclose the private key to anyone. On the day of election, the voter needs to login to system using their private keys through metamask which is a front end application for connecting to the Ethereum blockchain. After successful login, a voting page will be displayed containing the list of candidates standing in the election. The voter can cast the vote by selecting the desired candidate from the list and clicking the vote button.

IndexTerms **– Blockchain, Cryptography.**

I. INTRODUCTION

Voting, whether traditional ballet based or electronic voting (e-voting), is what modern democracies are built upon. In recent years voter apathy has been increasing, especially among the younger computer/tech generation. For a robust e-voting scheme, a number of functional and security requirements are specified including transparency, accuracy, auditability, system and data integrity, secrecy/privacy, availability and distribution of authority. Blockchain technology is supported by a distributed network consisting of a large number of interconnected nodes.

The cost of expenditure on the paper ballot is way higher. Electronic voting machines are vulnerable to malicious programming and if it gets affected then any hacker can hack the machine and can tamper the vote counts easily. Security of digital voting is always the biggest concern when considering implementing a digital voting system. With such monumental decisions at stake, there can be no doubt about the system's ability to secure data and defend against potential attacks. One way the security issues can be potentially solved is through the technology of blockchains.

II. PROPOSED SYSTEM

Blockchain technology is supported by a distributed network consisting of a large number of interconnected nodes. Each of these nodes has their own copy of the distributed ledger that contains the full history of all transactions the network has processed. A basic analysis of the blockchain technology suggests that it is a suitable basis for e-voting and moreover it could have the potential to make e-voting more acceptable and reliable. These technological features operate through advanced cryptography, providing a security level equal and/or greater than any previously known database. The blockchain technology is therefore considered by many, including us, to be the ideal tool, to be used to create the new modern democratic voting process.

III. LITERATURE REVIEW

In Paper [1], the author described that the Electronic Voting Machine (EVM) as a simple electronic device used to record votes in place of ballot papers and boxes which were used earlier in conventional voting system. All earlier elections be it state elections or centre elections a voter used to cast his/her favourite candidate by putting the stamp against his/her name and then folding the ballot paper as per a prescribed method before putting it in the Ballot Box. Paper [2] described that the Blockchain technology originates from the underlying architectural design of the cryptocurrency bitcoin. It is a form of distributed database where records take the form of transactions; a block is a collection of these transactions. With the use of blockchains a secure and efficient system for digital voting can be designed. Paper [3] discussed about Cryptocurrency, and its underlying technologies, that has been gaining popularity for transaction management beyond financial transactions. Transaction information is maintained in the block- chain, which can be used to audit the integrity of the transaction. The focus on this paper is the potential availability of blockchain technology of other transactional uses.

Using blind signature and blockchain, Paper [4] proposed an e-voting protocol, which introduces a lot of desirable properties from blockchain. Transparency might be reduced due to the tradeoff. It would be nice if some details of this e-voting protocol could be further optimized and implemented. In this protocol, manipulated ballots will be rejected by the network due to wrong signatures

and incorrect formats of ballots. Meanwhile, for potential dishonest organizer and inspectors, it is impossible to return a wrong signature with the purpose of invalidating voters' ballots, since wrong signatures associated with the original messages can be detected on blockchain. When the attack aims to forge ballots, it could not succeed if there exists at least one honest organizer or inspector.

For example, because of intentional transparency of blockchain, it seems difficult to satisfy coercion-resistance (Voters should not be able to prove how they voted.) unless implement access control using permissioned blockchain. Meanwhile, transparency might be reduced due to the tradeoff. To balance the two properties: transparency and coercion résistance better may constitute a possible direction of future work. Paper [5] said that the E-voting is among the key public sectors that can be disrupted by blockchain technology. The idea in blockchain-enabled e-voting (BEV) is simple. To use a digital-currency analogy, BEV issues each voter a "wallet" containing a user credential. Each voter gets a single "coin" representing one opportunity to vote. Casting a vote transfers the voter's coin to a candidate's wallet.

Paper [6] proposed smart contracts that succeeded in moving e-voting to the blockchain platform. Some of the fundamental issues that legacy e-voting systems have, by using the power of the Ethereum network and the blockchain structure are addressed. Ethereum and the smart contracts, which made one of the most revolutionary breakthroughs since the blockchain itself, helped to overturn the limited perception of blockchain as a cryptocurrency (coin), and turned it into a broader solution-base for many Internet-related issues of the modern world, and may enable the global use of blockchain. In Paper [7] it described about the use of hash values in recording the voting results of each polling station linked to each other makes this recording system more secure and the use of digital signatures makes the system more reliable. The use of the sequence proposed in the blockchain creation process in this system considers that in an electoral system not required for mining as in the Bitcoin system because the voter data and numbers are clear and are not allowed to select more than once, the proposed sequence ensures that all nodes Which is legally connected and can avoid collision in transportation.

IV. METHODOLOGY

The idea in Blockchain-Enabled e-Voting (BEV) is simple. To use a digital currency analogy, BEV issues each voter a "wallet" containing a user credential. Each voter gets a single "coin" representing one opportunity to vote. Casting a vote transfers the voter's coin to a candidate's wallet. A voter can spend his or her coin only once. To address voter tampering, blockchains generate cryptographically secure voting records. Votes are recorded accurately, permanently, securely, and transparently.

Using Distributed Ledger (Blockchain) to issue digital voting tokens to a poll station. Then the poll station issues tokens to individual voters and records voting on a sidechain. At the end of the voting, the entire side chain is committed to the main voting Blockchain. The specific Blockchain would be Ethereum. Right now there are a handful of blockchains who support smart contracts, but the biggest one is Ethereum. It was specifically created and designed to support smart contracts. A special programming language called Solidity, which was specifically created for Ethereum.

Polling stations are capable of keeping the votes off the main Blockchain for the purposes of keeping the totals hidden until their release. Every vote is validated in a smart contract before being sent to the candidate or ballot records.

In this system, the smart contract is that a "vote" is given to a candidate if it satisfies certain conditions, such as the amount being cast is equal to exactly one vote, verification that the polling station concurs that the voter wallet is valid, and that the vote occurred in a valid date range. The smart contract includes multisignature element, meaning that both the polling station and voter need to sign before release to the Blockchain. By combining elements of the cryptographic hashes, Blockchain, smart contracts, multisignature, and sidechains, it is possible to build an open, verifiable, and anonymous voting system for the modern world.

E-voting is among the key public sectors that can be disrupted by blockchain technology. The idea in blockchain-enabled e-voting (BEV) is simple. To use a digital currency analogy, BEV issues each voter a "wallet" containing a user credential. Each voter gets a single "coin" representing one opportunity to vote. Casting a vote transfers the CHAPTER 3 SYSTEM ANALYSIS Dept. of ISE, RNSIT 2018-19 Page 21 voter's coin to a candidate's wallet. A voter can spend his or her coin only once. However, voters can change their vote before a preset deadline. Here, argue that blockchains might address two of the most prevalent concerns in voting today: voter access and voter fraud.

The idea is as follows. Eligible voters cast a ballot anonymously using a computer or smartphone. BEV employs an encrypted key and tamper- proof personal IDs. For example, the mobile e-voting platform of the Boston-based startup Voatz employs smart biometrics and real-time ID verification. The public ledger ties each cast ballot to an individual voter and establishes a permanent, immutable record.

V. CONCLUSIONS AND FUTURE WORK

E-voting is proposed using blockchain in order to overcome the drawbacks of the traditional ballot system and EVM which are generally used for voting. The proposed system reduces the cost of expenditure and the time required for conducting an election and makes it possible to participate in elections and vote independent of current location. Also the people don't necessarily have to go to the booth and vote i.e they can vote from anywhere

Enhancements can be added to this project by adding better design and new features. Face detection can be used for authentication of the voter's identity to prevent a user from acquiring private keys of other people. Biometrics can be used for checking voter's authenticity. These can further boost the security. Better user friendly interfaces can be designed for providing

good user experience. Instructions can also be given regarding the procedure of voting and also regarding the cases if any emergency situations occur. Currently e-voting is applicable only on web interfaces. Further technique can be implemented on android to vote in Smartphone's using developed application.

REFERENCES

[1] Ali D. A. Kumar and T. U. S. Begum, " Electronic voting machine - A review", 2012.
[2] J. Hall, "Can Blockchain Technology Solve Voting Issues?" Bitcoin Magazine, 7 Mar 2018.
[3] Kibin Lee, Joshua I. James, Tekache Gobena Ejet "Electronic voting service using block-Chain",2016.
[4] Yi Liu and Qi Wang, "An E-voting Protocol Based on Blockchain", 12 Oct 2017. [5] Phillip laplant, Giuliano Antoniol, Steve Counsell "Blockchain enabled e-voting". 2017.
[7] Ali Kaan Koç, Emre Yavuz, "Towards Secure E-Voting Using Ethereum Blockchain",2015. [8] Rifa Hanifatunnisa and Budi Rahardjo, "Blockchain Based E-Voting Recording System Design",2013.