E voting System using Decentralized, Immutable and Transparent Blockchain Technology with Privacy Protocols, Ring Signature and Simulation.

[1]Mr.Nikhil Patare, [2]Mr.Shubham Adsul, [3]Ms.Dhanashri Durge, [4]Prof.Monali Mohite
[1]Student,Dept. of Computer Engineering, BSIOTR, Wagholi , SPPU , India , [2]Student,Dept. of Computer Engineering, BSIOTR, Wagholi , SPPU , India , [3] Student,Dept. of Computer Engineering, BSIOTR, Wagholi , SPPU , India, [4]Professor,Dept. of Computer Engineering, BSIOTR, Wagholi , SPPU , India.

Abstract : This system is an attempt to suggest blockchain technology for digital voting system. Elections and voting are important factors of a democratic country; however the voting process is increasingly challenged by the power of the internet. There are security problems around electronic voting booths, which analyzers have warned are vulnerable and easy for hacking. Such weak system could be used to undermine trust in an election system. The blockchain technology is presented as a game changer for many of the available technologies. With its immutability and transparent property and decentralized and unique architecture, it is taking important platform in many services as an equalization factor to the current parity between consumers and large corporate companies. This paper presents an effort to advantage of blockchain such as cryptographic foundations and transparent system to achieve an effective scheme for e-voting. The proposed scheme conforms to the fundamental requirements for e-voting schemes and achieves end-to-end verification.

IndexTerms **- Blockchain, Voting booths, Vulnerable, Decentralized, Immutable.**

I. INTRODUCTION

In every democracy, the security of an election is a matter of national security. The computer security field has for a decade studied the possibilities of electronic voting systems [1], with the goal of minimizing the cost of having a national election, while fulfilling and increasing the security conditions of an election. From the dawn of democratically electing candidates, the voting system has been based on pen and paper. Replacing the traditional pen and paper scheme with a new election system is critical to limit fraud and having the voting process traceable and verifiable [2]. Electronic voting machines have been viewed as flawed, by the security community, primarily based on physical security concerns. Anyone with physical access to such machine can sabotage the machine, thereby affecting all votes cast on the aforementioned machine. Enter blockchain technology. A blockchain is a distributed, immutable, incontrovertible, public ledger. This new technology works through four main features:
(i)The ledger exists in many different locations: No single point of failure in the maintenance of the distributed ledger.
(ii)There is distributed control over who can append new transactions to the ledger.
(iii)Any proposed "new block" to the ledger must reference the previous version of the ledger, creating an immutable chain from where the blockchain gets its name, and thus preventing tampering with the integrity of previous entries.

II. PRILIMINARIES OF EVOTING AND BLOCKCHAIN

This section explains the liquid democracy and its design consideration. We then provide an overview of blockchain and smart contract technology and its capabilities as a service for implementing an e-voting system for liquid democracy along with an overview of Zero-Knowledge proofs and their use cases in such systems use.

1)Liquid Democracy- Liquid Democracy, a part of authorized democracy, is a powerful voting method for collective decision making in large communities. Liquid Democracy adds the effective advantages of Democracy and Representative Democracy and creates a most effective democratic voting system that empowers voters to either vote on issues directly, or to authorize ones voting power to a trusted third party. Through authorization, people with domain-specific data are able to better influence the output of decisions, which in leads to an overall good governance of the state. Because of the knowlwdge, liquid democracy naturally progress into a Meritocracy, where decisions are mainly made by those who have such kind of knowledge and experience required to make well-informed.

2)Blockchain Service- Individuals and businesses are increasingly willing to adapt to blockchain technology. However, the technical complex data and operational overhead involved in creating and operating the blockchain, and maintaining its structure, often act as deterrents to its huge adoption. Along with leading tech giants, many startups are now offering a good solution to this problem through the Blockchain-as-a-Service model.

III. RELATED WORK

SHA-256 Cryptographic Hash Algorithm-
SHA-256 (secure hash algorithm, FIPS 182-2) is a cryptographic hash function with digest length of 256

bits. It is a keyless hash function; that is, an MDC (Manipulation Detection Code).
A message is processed by blocks of 512 = 16 × 32 bits, each block requiring 64 rounds.
Basic operations

- Boolean operations AND, XOR and OR, denoted by $\wedge$, $\oplus$ and $\vee$, respectively.
- Bitwise complement, denoted by $\bar{}$.
- Integer addition modulo 232, denoted by A + B.

Each of them operates on 32-bit words. For the last operation, binary words are interpreted as integers written in base 2.

- RotR(A, n) denotes the circular right shift of n bits of the binary word A.
- ShR(A, n) denotes the right shift of n bits of the binary word A.
- AkB denotes the concatenation of the binary words A and B.

The algorithm uses the functions:

$Ch(X, Y, Z) = (X \wedge Y) \oplus (X \wedge Z)$,
$Maj(X, Y, Z) = (X \wedge Y) \oplus (X \wedge Z) \oplus (Y \wedge Z)$,
$\Sigma 0(X) = RotR(X, 2) \oplus RotR(X, 13) \oplus RotR(X, 22)$,
$\Sigma 1(X) = RotR(X, 6) \oplus RotR(X, 11) \oplus RotR(X, 25)$,
$\sigma 0(X) = RotR(X, 7) \oplus RotR(X, 18) \oplus ShR(X, 3)$,
$\sigma 1(X) = RotR(X, 17) \oplus RotR(X, 19) \oplus ShR(X, 10)$,

Ring Signature- Ring signature technology to protect a user's privacy in the input side of a transaction. A ring signature is a type of digital signature in which a group of possible signers are merged together to produce a distinctive signature that can authorize a transaction. Ring signature is composed of the actual signer, who is then combined with non-signers to form a ring. The original signer and non-signers in this ring are all considered to be equal . The original signer is a one-time spend key that corresponds with an output being sent from the sender's wallet. The non-signers are past transaction outputs that are drawn from the blockchain. These past transaction outputs function as bait in the ring signature transaction, by forming part of the inputs of a transaction. From the perspective of an outside party, all of the inputs appear equally likely to be the output being spent in a transaction. It utilizes ring signature technology to help the original sender mask the origin of a transaction by ensuring that all data inputs are indistinguishable from each other.

3.1 Proposed Voting System

3.1.1 Registration of Voter

The first feature of our design is the registration process, verifying a voter is crucial in set up security within the system. Making sure that someone's identity isn't being misused for cheating purposes is main factor, mostly when voting is considered, where every vote have value.
1. Initially, a transaction is created when a voter 'registers'.
2. The next transaction is generated when a government miner permit that user's right to vote.

3.1.2 System Architecture- When determining on the architecture we took powerful inspiration from both the distributed an acquirability of the Bitcoin network and the gatherin g process of traditional voting. The network is a Multi-tiered, decentralized infrastructure which having the two definite blockchains. A local node is setup to only be in contact with the other local nodes under the connected constituency node and the constituency node itself.

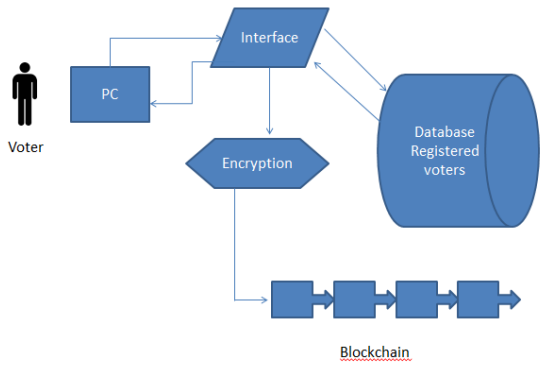

Fig 2.Architecture of E-voting System

3.1.3 Voting Process

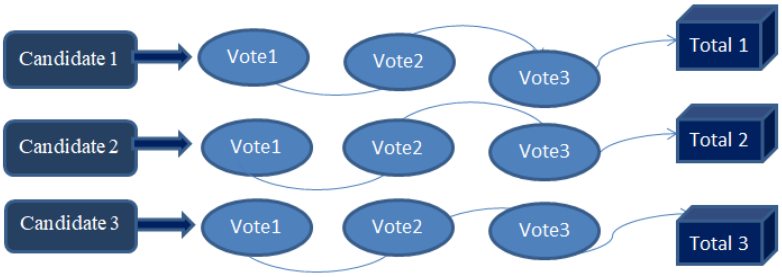

Fig 3.Additing vote into blockchain of E-voting System

(1)Requesting user to vote: The user will have to log in to the voting system using his credentials in this case, the e-Voting system will use his Social Security Number his address, and the voting confirmation numbers suggested to registered voters by the local authorities.
(2) Casting a vote: Voters will have to select to either vote for one of the candidates or cast a protest vote. Casting the vote will be proceeds through a user friendly interface.
(3) Encrypting votes: After successful execution of casting vote, the system will create an input that consist of the voter identification number came after the complete name of the voter and the hash code of the earlier vote. This way each input will be unique and make sure that the encrypted output will be unique as well.
(4) Adding the vote to the Blockchain : Choose the information is recorded in the particular Blockchain. Each block gets attached to the previously cast vote.

IV. Conclusion

These blockchains are held completely separately to remove any threat to link votes for certain parties back to individual voters while maintaining the ability to track who has voted and how many votes are actually present .
Also, due to the encryption mechanism we are using it would be close to impossible for any person(s) to gain access to all the votes without first taking control of the entire service network.

V. Acknowledgment

The authors wish to thank Prof. Monali Mohite Project Guide, Prof. G.M. Bhandari Head of Computer Department for supporting this research study through survey sessions.

References

[1] Sos.ca.gov. (2007). Top-to-Bottom Review | California Secretary 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] F. Reid and M.Harrigan, "An Analysis of Anonymity in the Bitcoin System", Security and Privacy in Social Networks. (2013), pp. 1-27.
[4]Genesis block (2015) Available at: https://en.bitcoin.it/wiki/Genesis_block (Accessed 27 September 2016)

[5] J. R. Douceur, "The Sybil Attack", International Workshop on Peer-to-Peer Systems, (2002), pp. 251-260.

[6]bitcoin/src/chainparams.cpp,https://github.com/bitcoin/bitcoin/blob/3955c3940eff83518c186facfec6f 50545b5aab5/src/chainparams.cpp#L123

[7]Bitcoin Block Explorer, https://blockexplorer.com

[8] Why Use Bitcoin? http://www.coindesk.com/information/why-usebitcoin/

[9] How to Set Up a Bitcoin Miner, http://www.coindesk.com/information/how-to-set-up-a-miner

[10]Elliptic-curve digital signatures, http://davidederosa.com/basicblockchain-programming/elliptic-curve-digital-signatures/