IOSR Journal of Engineering (IOSR JEN) **www.iosrjen.org**
ISSN (e): 2250-3021, ISSN (p): 2278-8719
PP 10-12

A Secure Blockchain- Based Electronic Voting System

Neel Patel*, Ruchir Mumbarkar*, Jay Desai*, Amruta Pokhare**
*(Information Technology, Mumbai University, Mumbai
Email: neelpat96@gmail.com , mumbarkarruchir@gmail.com , jayd409@gmail.com)
**(Department of Information Technology, Mumbai University, Mumbai Email: amrutapokhare09@gmail.com)

Abstract: *Blockchain is offering new opportunities to develop new types of digital services. While research on the topic is still emerging, it has mostly focused on the technical and legal issues instead of taking advantage of this novel concept and creating advanced digital services. We are going to leverage the open source. Blockchain technology to propose a design for a new electronic voting system that could be used in local or national elections. The Blockchain-based system will be secure, reliable, and anonymous, and will help increase the number of voters as well as the trust of people in their governments.*
Keywords *- Blockchain, Electronic Voting System, e-Voting, I-Voting, iVote.*

I. Introduction

A Secure Blockchain Based Electronic Voting System is required as this system uses existing technology such as a client server architecture integrated with a blockchain system to ensure aspects such as transparency, security and auditability are achieved without sacrificing privacy for voters.Estonia was the first in the world to adopt an electronic voting system for its national elections.Soon after, electronic voting was adopted by Switzerland for its state-wide elections, and by Norway for its council election. Blockchain has a wide area of applications for increasing the security of digital transactions. The security offered by blockchain could be used on an E-voting system to further increase the trust of voters. The system that will be designed will be easy and accessible by all.

II. System Analysis

a. PresentSystem

First E-Voting System

David Shaumintroduced the first-ever electronic voting system. Public key cryptography was used to cast votes and keep voters anonymous. The Blind Signature Theorem was used to make sure there were no links between voters and ballots [1].

Estonian I-Voting System

Estonia was the first in the world to adopt an electronic voting system for its national elections. Citizens were able to cast their vote using only the Internet and an electronic national identification card. The ID card used in the elections was designed to run on an integrated circuit, a chip Java chip platform, and protected with 2048bit PIN [2].The card is able to create signatures using SHA1/SHA2 [3]. The card is used for authentication, encryption, and signatures. The voter has to download the voting application, authenticate using the electronic ID, and if the voter is eligible to vote a list of candidates will be displayed and a vote could be cast.The vote will be encrypted using the election's public key and signed with the voter private key. As soon as the vote is cast it will be sent to a vote storage server controlled by the Estonian government [4].Voters could vote multiple times, and only the last vote will be considered valid.This is done to prevent vote buying.

Norwegian I-Voting System

Norway used an electronic remote voting system for the country council elections in 2011.Scytl developed this system. This system was very similar to the Estonian electronic voting system. In 2014, the country has discontinued its I-Voting project due to security concerns [5]. One of the main critics Norwegian I-Voting system faced was the fear of votes going public in case of a cyber-attack.

b. ProposedSystem

The proposed system consists of two steps registration where both candidate and user need to register and the process of registering itself. In this proposed system the user logs into the system with valid username and password. Once the user is logged in user can view the candidates and give vote respectively. The system then verifies the given vote using blockchain method and user then get a confirmation of their given vote.

A. Block Diagram:

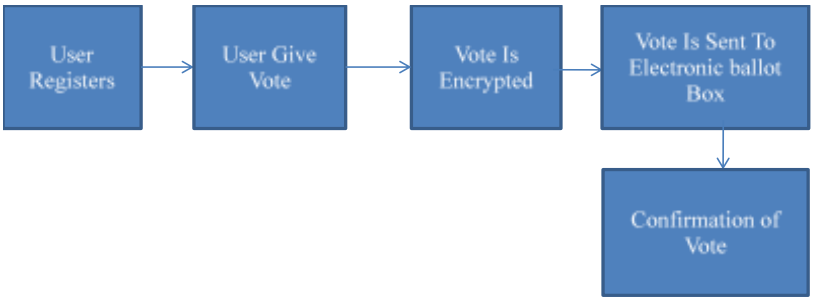

Figure II-A: System Block Diagram

III. Methodology

- Voter logs into the Electronic Voting Portal. (Voter needs to be registered and authorized to vote)
- Then the voter can view a list of candidates for the elections.
- The voter casts their vote and confirms.
- The vote is encrypted using SHA-256 and stored in the blockchain.
- Once the voting period ends, all votes are counted using a simple counting algorithm.
- The winner for the election is declared on the portal.

IV. Design

The voter starts by logging into the website with user credentials. Any registered and authorized voter will have their unique user name and password which they will use to access the portal. Once the voter is verified by the system, they will have complete voter access to the portal. The voter can then view the list of candidates for the ongoing elections and then cast their vote. System will prompt and ask for voter's confirmation after which the vote will be encrypted and saved in a block in the blockchain. As the blockchain uses a decentralized network the possibility of the votes being lost due to hardware or software failure would be zero. Hashing algorithm SHA-256 will be used for encrypting the blocks hence there would be no chance of security breach. Once the voting period has ended the votes will be counted and the winner will be declared on the Voting Portal.

V. Conclusion

The project will mainly focus on designing and developing an electronic voting system based on the Blockchain technology. The system will be decentralized and does not rely on trust. Any registered voter will have the ability to vote using any device connected to the Internet. The Blockchain will be publicly verifiable and distributed in a way that no one will be able to corrupt it.

Acknowledgment

We would like to express immense gratefulness to our guide Prof. Amruta Pokhare for her motivation and guidance throughout. We would also like to thank the faculty of Information Technology Department who greatly assisted our research and for their valuable help.

References

[1]. D. L. Chaum, "Untraceable Electronic Mail, Return Addresses, and Digital Pseudonyms", Communication of the ACM. Vol. 24(2). (1981), pp. 84-90.
[2]. Madise, Ü. Madise and T. Martens, "E-voting in Estonia 2005. The first practice of country-wide binding Internet voting in the world."Electronic voting,2nd International Workshop, Bregenz, Austria, (2006) August 2-4.
[3]. Trueb Baltic, "Estonian Electronic ID – Card Application Specification Prerequisites to the Smart Card Differentiation to previous Version of EstEID Card Application." http://www.id.ee/public/TBSPEC-EstEID-Chip-App-v3_5-20140327.pdf.
[4]. Cybernetica."Internet Voting Solution."https://cyber.ee/uploads/2013/03/cyber_ivoting_NEW2_A4 _web.pdf.

[5]. Ministry of Local Government and Modernisation. "Internet Voting Pilot to be Discontinued." https://www.regjeringen.no/en/aktuelt/Internet-voting-pilot-to-be-discontinued/id764300/ .
[6]. J. A. Halderman, and V. Teague, "The New South Wales iVote System: Security Failures and Verifications Flaws in a Live Online Election." International Conference on E-Voting and Identity. (2015), pp. 35-53.
[7]. S. Wolchok, E. Wustrow, D. Isabel, J. A. Halderman, "Attacking the Washington, DC Internet Voting System." International Conference on Financial Cryptography and Data Security (2012), pp. 114-128.