International Journal of Innovative Technologies
WWW.IJITECH.ORG
ISSN 2321-8665
Volume.07, Issue.01,
January-June, 2019,
Pages:29-32

E-Voting with Blockchain on Secure Platform Independent

S. RAJITHA[1], A. SARITHA[2]
[1]PG Scholar, Dept of CSE, SV Engineering College for Women, Tirupati, AP, India.
[2]Assistant Professor, Dept of CSE, SV Engineering College for Women, Tirupati, AP, India.

Abstract: Technology has positive impacts on many aspects of our social life. Designing 24 hour globally connected architecture enables ease of access to a variety of resources and services. Furthermore, technology like the Internet has been a fertile ground for innovation and creativity. One such disruptive innovation is blockchain – a keystone of crypto currencies. The blockchain technology is presented as a game changer for many of the existing and emerging technologies/services. With its immutability property and decentralized architecture, it is taking centre stage in many services as an equalization factor to the current parity between consumers and large corporations/governments. One potential application of the blockchainis in e-voting schemes. In this paper, we propose a potential new e-voting protocol that utilizes the blockchain as a transparent ballot box. The protocol has been designed to adhere to fundamental e-voting properties as well as offer a degree of decentralization and allow for the voter to change/update their vote.

Keywords: Block-Chain, Voting, Decentralization.

I. INTRODUCTION

Blockchain technology that shines sort of a star once the doorway and widespread acceptance of Bit-coin, the terribly 1st crypto currency in peoples' lifestyle, has become a trending topic in today's package world. At the start, blockchain was solely used for financial transactions and trade, however studies have began to recommend that it will be employed in more areas over time, as a result of there's a high degree of transparency during this system. For instance, in Bit-coin, since the wallets area unit in an exceedingly distributed structure, the whole quantity of coins and instant group action volume within the world will be followed momentarily and clearly. There's no would like for a central authority to approve or complete the operations on this P2P-based system. 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. 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. However, voters can change their vote before a preset deadline. Here, we 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 smart phone. BEV employs an encrypted key and tamperproof 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. The Blockchain's audit trail ensures that no vote has been changed or removed and that no fraudulent and illegitimate votes have been added. Put simply, blockchains enable the creation of tamper-proof audit trails for voting. In this article, we highlight some BEV implementations and the approach's potential benefits and challenges.

II. LITERATURE REVIEW

Cryptographic techniques are employed to ensure the security of voting systems in order to increase its wide adoption. However, in such electronic voting systems, the public bulletin board that is hosted by the third party for publishing and auditing the voting results should be trusted by all participants. Recently a number of blockchain-based solutions have been proposed to address this issue. However, these systems are impractical to use due to the limitations on the voter and candidate numbers supported, and their security framework, which highly depends on the underlying blockchain protocol and suffers from potential attacks (e.g., force-abstention attacks). To deal with two aforementioned issues, we propose a practical platform-independent secure and verifiable voting system that can be deployed on any blockchain that supports an execution of a smart contract. Verifiability is inherently provided by the underlying blockchain platform, whereas cryptographic techniques like Paillier encryption, proof-of-knowledge, and linkable ring signature are employed to provide a framework for system security and user-privacy that are independent from the security and privacy features of the blockchain platform.

We analyze the correctness and coercion-resistance of our proposed voting system. We employ hyper ledger Fabric to deploy our voting system and analyze the performance of our deployed scheme numerically. Blockchain is offering new opportunities to develop new types of digital services. While research on thetopic is still emerging, it has mostly focused on the technical and legal issues instead of taking advantage ofthis novel concept and creating advanced digital services. In this paper, 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. Voting is a fundamental part of democratic systems; it gives individuals in a community the faculty to voice their opinion. In recent years, voter turnout has diminished while concerns regarding integrity, security, and accessibility of current voting systems have escalated. E-voting was introduced to address those concerns; however, it is not cost-effective and still requires full supervision by a central authority. The blockchain is an emerging, decentralized, and distributed technology that promises to enhance different aspects of many industries. Expanding e-voting into blockchain technology could be the solution to alleviate the present concerns in e-voting.

In this paper, we propose a blockchain-based voting system, named Bronco Vote that preserves voter privacy and increases accessibility, while keeping the voting system transparent, secure, and cost-effective. Bronco Vote implements a university-scaled voting framework that utilizes Ethereum's blockchain and smart contracts to achieve voter administration and auditable voting records. In addition, Bronco Vote utilizes a few cryptographic techniques, including homomorphic encryption, to promote voter privacy. Our implementation was deployed on Ethereum's Testnet to demonstrate usability, scalability, and efficiency. Election is a very important event in a modern democracy but large sections of society around the world do not trusttheir election system which is major concern for the democracy. Even the world's largest democracies like India, United States, and Japan still suffer from a flawed electoral system. Vote rigging, hacking of the EVM (Electronic voting machine), election manipulation, and polling booth capturing are the major issues in the current voting system. In this paper, we are investigating the problems in the election voting systems and trying to propose the E-voting model which can resolve these issues. Also this article aiming to evaluate the application of blockchain as service to implement distributed electronic voting systems. The section of paper will highlight some of the popular blockchain frameworks that offer blockchain as a service and associated electronic E-voting system which is based on blockchain that addresses all limitations respectively, it also preserve participant's anonymity while still being open to public inspection.

III. PROBLEM STATEMENT

Election Polling is a complex system as well as costly system. Here we are presenting a novel Secure, Privacy Preserving and cost effective election polling concept which uses Web Technology with GPRS Connectivity, Cloud Data Storage and Homomorpic encryption. This system has two types of users one is Election Officer & another is Booth Manager, Booth Manager system developed with voters functionality where voters are going to poll. Election officer will act as an admin user and he has to do the setting and configuration setting for election polling. Booth Managers are the area manages those who are responsible to add the voters details into the system and has retrieval system by which they can able to view the voted candidate details and sum of the votes. Voters has to go the Booth where the Booth manager verify the voter and allow him to poll on the Booth's Laptop where the our voting system is running. This proposed system has a method to execute operations on encrypted data without decrypting them which will provide us with the same results after calculations as if we have worked directly on the raw data.

A. Blockchain Based Electronic Voting System

1. Requesting 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 number provided to registered voters by the local authorities. The system will check all information entered and, if matched with a valid voter, the user will be authorized to cast a vote. Our e-Voting system will not allow participants to generate their own identities and register to vote. Systems that allow identities to be arbitrarily generated are usually vulnerable to the Sybil attack where attackers claim a large number of fake identities and stuff the ballot box with illegitimate votes.

2. Casting a vote

Voters will have to choose to either vote for one of the candidates or cast a protest vote. Casting the vote will be done through a friendly user interface. For each voter a token is generated known as Ethereum, with initial Boolean value one, once a vote is casted it becomes 0. A voter can cast a vote if and only if Ethereum value is 1.In this way revoting problem is resolved.

3. Encrypting votes

After the user casts his vote, the system will generate an input that contains the voter identification number followed by the complete name of the voter as well as the hash of the previous vote. This way each input will be unique and ensure that the encrypted output will be unique as well. The encrypted information will be recorded in the block header of each vote cast. The information related to each vote will be encrypted using SHA one-way hash function that has no known reverse to it. The only theoretically possible way to reverse the hash would be to guess the seed data and the encryption method and then hash it to see if the results match. This way of hashing votes makes it nearly impossible to reverse engineer, therefore there would be no way voters' information could be retrieved.

4. Adding the vote to the Blockchain

After a block is created, and depending on the candidate selected, the information is recorded in the corresponding blockchain. Each block gets linked to the previously cast vote.

IV. RESULTS AND DISCUSSION

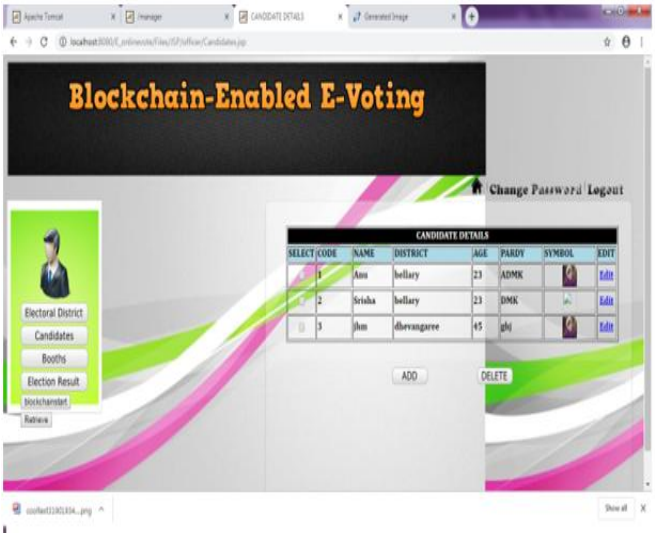

Fig1. Candidate Details.

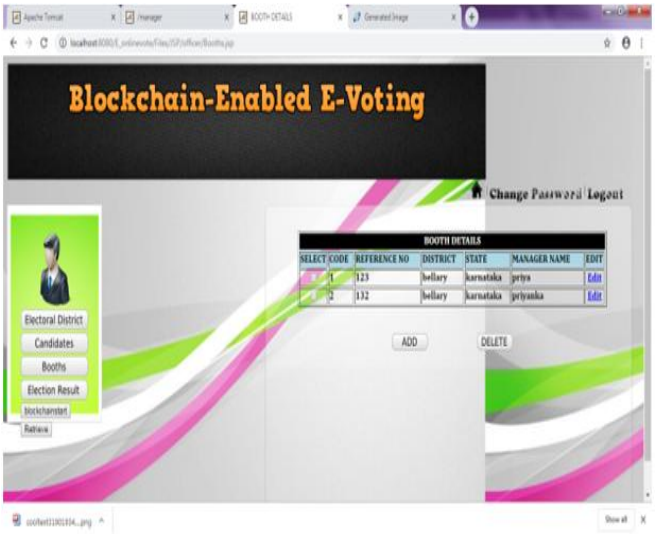

Fig2. Booth Details.

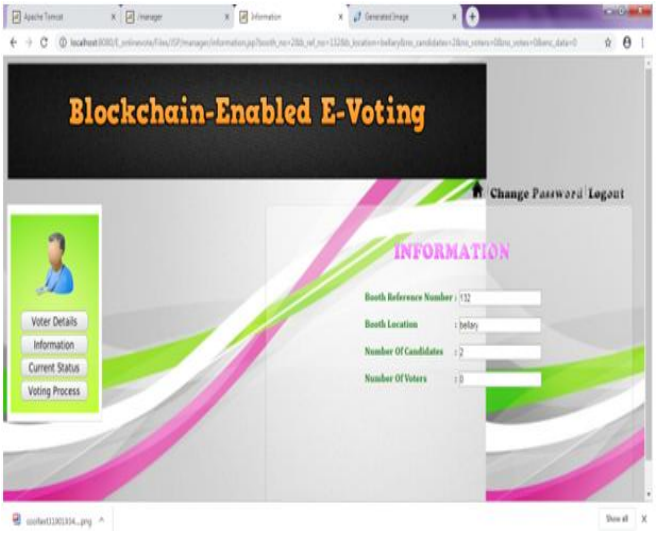

Fig3. Booth Information.

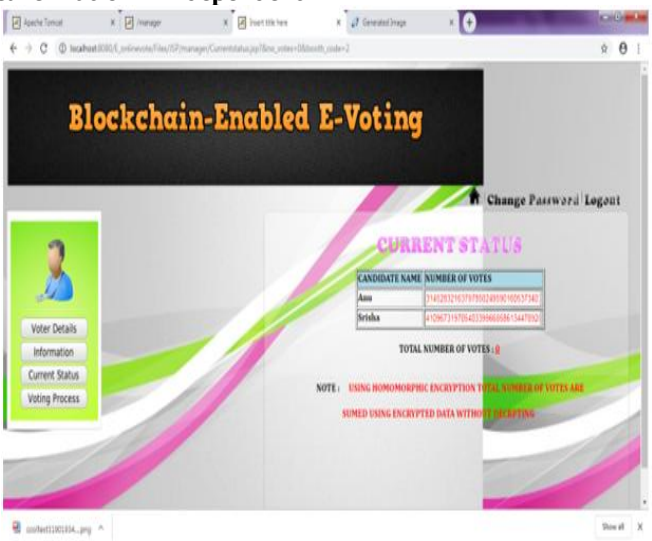

Fig4. Voting Process.

V. CONCLUSION

E-voting, as discussed in the paper, is a potential solution to the lack of interest in voting amongst the young tech savvy population. For e-voting to become more open, transparent, and independently auditable, a potential solution would be base it on Blockchain technology. This paper explores the potential of the Blockchain technology and its usefulness in the e-voting scheme. The paper proposes an e-voting scheme, which is then implemented. The implementation and related performance measurements are given in the paper along with the challenges presented by the Blockchain platform to develop a complex application like e-voting. The paper highlights some shortcomings and presents two potential paths forward to improve the underlying platform (Blockchain technology) to support e-voting and other similar applications. Blockchain technology has a lot of promise; however, in its current state it might not reach its full potential.

VI. REFERENCES

[1] Ahmed Ben Ayed(2017);A Conceptual Secure Blockchain –Based Electronic Voting System; International Journal of Network Security & Its Applications (IJNSA) Vol.9, No.3.

[2] PavelTarasov and Hitesh Tewari(2017);The Future of E-Voting; IADIS International Journal on Computer Science and Information Systems Vol. 12, No. 2, pp. 148-165 I.

[3] Zibin Zheng1, Shaoan Xie1, Hongning Dai2, Xiangping Chen4, and HuaiminWang3(2017);An Overview of Blockchain Technology : Architecture, Consensus, and Future Trends; IEEE 6th International Congress on Big Data.

[4] Jesse Yli-Huumo1, Deokyoon Ko2, Sujin Choi4*, Sooyong Park2, Kari Smolander3(2016); Where Is Current Research on Blockchain Technology?—A Systematic Review; PLOS-ONE.

[5] Mahdi H. Miraz1, Maaruf Ali2(2018); Applications of Blockchain Technology beyond Crypto currency; Annals of Emerging Technologies in Computing (AETiC) Vol. 2, No. 1, 2018.

[6] Michael Crosby, Google,Nachiappan, Yahoo, Pradhan Pattanayak, Yahoo, Sanjeev Verma, Samsung Research America, Vignesh Kalyanaraman, Fairchild Semiconductor (2015); Blockchain Technology Beyond Bitcoin.

[7] Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram, and Konstantinos Markantonakis (2018); E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy; arXiv:1805.10258v2 [cs.CR].

[8] Kibin Lee, Joshua I. James, Tekachew Gobena Ejeta, HyoungJoong Kim(2016); Electronic Voting Service Using Block-Chain;Journal of Digital Forensics, Security and Law.

[9] Aayushi Gupta1*, Jyotirmay Patel2, Mansi Gupta1, HarshitGupta1(2017); Issues and Effectiveness of Blockchain Technology on Digital Voting; International Journal of Engineering and Manufacturing Science. ISSN 2249-3115 Vol. 7, No. 1 (2017).