VoteEth : An e-Voting System Using Blockchain

Divyanshi Dixit, Student, EPCET Bangalore India, divi.dixit45@gmail.com

Dr. Nanda Ashwin, professor, EPCET Bangalore India, nandaashwin7@gmail.com

G Lakshmi, Student, EPCET Bangalore India, lakshmi.aug31@gmail.com

Aman Mishra, Student, EPCET Bangalore India, aman07mishra@gmail.com

M U Bhavin, Student, EPCET Bangalore India, bhavinmachamada@gmail.com

Abstract **Technology has positive impacts on many aspects of our social life. Access to a variety of resources becomes easy because of globally connected architecture. 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 crucial improvement for many of the already existing and emerging technologies. It stands as a equalization factor due to its immutable property and decentralized architecture.one of the efficient application is e-voting scheme using blockchain. The objective of such a scheme would be to provide a decentralized architecture to run and support a voting scheme that is open, fair, and independently verifiable. 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 (within the permissible voting period). The study depicts the pros and cons of blockchain usage in a practical point of view.**

***Keywords* — Blockchain ,Crypt currencies, E-voting, Ethereum, Privacy, Smart contact**

I. INTRODUCTION

Modern democracy is built on ballet based or e-voting. In recent years voter apathy has been increasing, especially among the younger computer/tech savvy generation. Young voters are attracted by the concepts of e-voting. 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 history of transactions in the network will be present in the each node of the distributed ledger. The network is not under the control of single authority. A transaction is accepted if and only if majority of the nodes are agreed. This network allows users to remain anonymous. Using the concepts of blockchain, e-voting has become more acceptable and reliable.

Smart contracts are blocks of code that are stored on the blockchain. Smart contracts consists of functions or events that allow contracts to interact with each other and users. Since these smart contracts are stored on the blockchain, the code is not modifiable and is available for use by nodes connected to the blockchain. To protect the system against malicious users and compensate miners for computational power usage, the execution of every transaction includes a transaction fee, referred to as “gas” in Ethereum. Gas is the unit of measure for the amount of work that is accomplished for an operation and the gas price is measured in terms of ether in Ethereum. Smart contracts also extend the use of private blockchain; as opposed to public blockchain, private blockchains are only accessible by one organization. While this sacrifices part of the blockchains decentralization property, it enhances the privacy of the blockchain. Our system for handling university voting, VoteEth, implements a private blockchain. We believe a private blockchain is suitable based on the needs for the integrity and privacy of ballots.

Obvious advantages of e-voting using blockchain includes: i) greater transparency due to open and distributed ledgers, ii) inherent anonymity, iii) security and reliability (especially against Denial of Service Attacks) and iv) immutability (integrity of individual vote is maintained). Existing works explore how blockchain can be used to improve the e- voting schemes or provide some strong guarantees of the above listed requirements. The paper do not completely discuss about the limitations, drawbacks and implementation of blockchain in a large scale voting scheme. This paper discusses both the efficiency and drawbacks of using blockchain technology in e-voting.

DOI : 10.18231/2454-9150.2019.0580

II. Literature Survey

A. *Existing System*

Electronic Voting Machine (also known as EVM) is voting using electronic means to either aid or take care of the chores of casting and counting votes.

An EVM have two units: the control unit and the balloting unit. These units are connected together by a cable. The presiding officer or the polling officer is responsible to keep the control unit of the EVM.For an electors to cast their vote has to go to voting compartment in which balloting unit is kept. Using this the elector identity is verified. The EVM, instead of issuing a ballot paper, the polling officer will press the Ballot Button which enables the voter to cast their vote. A list of candidates names and/or symbols will be available on the machine with a blue button next to it. The voter can press the button next to the candidate's name they wish to vote for.

B. *Proposed System*

We intent to build an immutable Block-Chain based E-voting system which empowers voters to cast their vote digitally. Providing a voting system that is open, fair, and independently verifiable deployed on a secure decentralized architecture with maximum power in the hands of voters. Provide a system to cast votes on a distributed trustless system where data can't be modified once committed. Provide Users with most of the powers, instead of the booth manager. Cast a vote for your constituency irrespective of place and time.

C. Module Description

- **Booth:**The booth is a node in the peer-to-peer network of the blockchain. It takes part in the mining and the consensus process. This means that the entire blockchain will be locally stored at each of the booths.For each of the transactions received by the booth from the voters a smart contract is used to validate the transaction, ensuring that no voter casts more than one vote.The hash for each of the transactions received by the booth from the voters is calculated and the merkel tree is generated. The block is thus formed and put on the blockchain by a smart contract.Booth will have information about the booth like the booth reference number, booth location,total number of voters destined to vote in his booth etc. The Booth Manager can use this module to see view this information.He can also add or delete any voter from the list before the election has started.

- **Voter:**Voters are simple account holders who use the blockchain instance by downloading by installing a software client on their machine, downloading the instance's ledger and submitting transactions to the network. Unlike the booth, voters can freely connect to and disconnect from the network at anytime. Inside a software client the user can have several wallets, one for each election he's eligible to participate. Each wallet has a unique wallet address.

- **Electoral Commissioner:** Election commissioner has the authority to add, delete or edit election related data. Candidate details like name, age, party, district can checked, edited, added or deleted. Likewise even the booth details like the reference number, district and the booth manager in-charge can be seen or edited. The election officer has the authority to invoke the vote-counting module and announce the winner of election.

- **Vote Counting:** This module is invoked by the election commissioner after the election during the vote counting phase.It traverses the whole blockchain to count the number of votes won by each of the candidates and returns this data to the election commissioner.

- **Block chain:** It is the framework on which the whole system works. In our project we use the framework and the tools provided by Ethereum to set up our own blockchain.

III. ARCHITECTURE

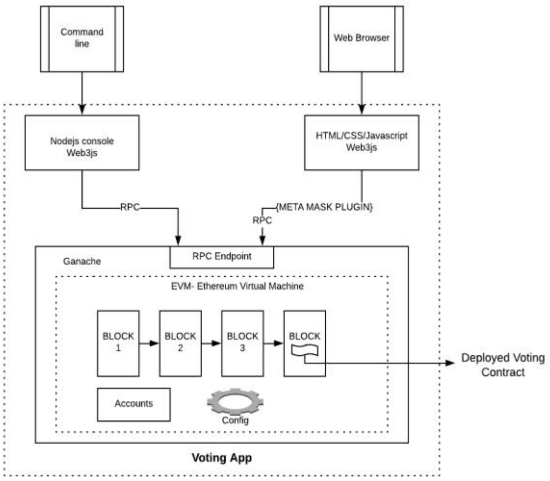


Figure 1 E-voting Architecture

A. *Blockchain Mining*

To reach consensus on the state of the blockchain in a trust-less network, a concept known as 'mining' is employed. The role of a miner node is to verify transactions, group transactions into blocks, and append them to the blockchain. To append a new block to the blockchain, the hash of the block must begin with a certain number of zeros. To achieve this, a number called a 'nonce' is included in each block ;each time miners hash the block without solving the computational problem, they increment the nonce and rehash the block. The difficulty of solving the hashing problem is described as 'Proof of Work,' signifying the

DOI : 10.18231/2454-9150.2019.0580

computational power and difficulty needed to append a new block to the blockchain.

B Eth.calls

Every valid transaction executed is stored on the blockchain. Due to this, blockchain can suffer from scalability issues. Valid transactions sent to smart contracts in the Ethereum blockchain are considered state changeable calls and consume gas. To reduce gas consumption and the number of transactions on the blockchain, the Ethereum blockchain allows the. Calls to be utilized in addition to transactions. Eth.calls allows nodes to send messages to other nodes or smart contracts to retrieve its current state without storing the message on the blockchain 5. Therefore, Eth.calls are similar to simulations of transactions. By executing Eth.calls to send notifications/messages or to retrieve current states, the size of the blockchain can be greatly reduced.

C MetaMask

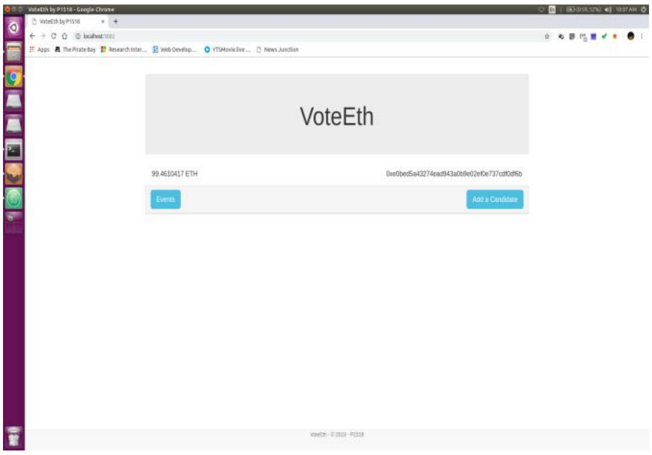
MetaMask was created to increase the accessibility of the Ethereum blockchain to the average user. A plug-in for Chrome, MetaMask acts as an Ethereum browser, allowing users to manage their Ethereum wallet and interact with decentralized applications and smart contracts without running a full node. Through MetaMask, users are able to manage multiple accounts and easily switch between different networks 5 . In order to allow users the flexibility of using the Ethereum blockchain without running a full node, MetaMask relies on trusted nodes to broadcast the transactions of MetaMask users in order to be mined. Since transactions are signed using the sender's private key, which is stored locally on the user's machine, MetaMask cannot impersonate the user and send transactions on the user's behalf. Acting as an intermediary between Chrome and the Ethereum blockchain, MetaMask allows users the convenience and security of the blockchain within a popular browser.

IV. FEATURE ENHANCEMENT AND APPLICATION

In future work, we will investigate the possibility of implementing Paillier cryptosystem as a library in Solidity. With the system we currently have, moving the cryptography to a library in Solidity could largely improve our individual ballot verifiability. Having the Paillier library in Solidity would help us generate a ICISSP 2018 - 4th International Conference on Information Systems Security and Privacy 106 new private and public key for each ballot. This will help us achieve individual voter audition different ballots without compromising the other ballots. To increase user accessibility, we will also look into integrating the Ethereum Light wallet into our system will allow users to unlock their accounts in our UI without needing to run a node or plugin. Finally, to help with voter verification, we will try to integrate an API/process that will allow us to check the validity of all e-mails used to register into our system.

V. RESULT

A. Figures and Tables



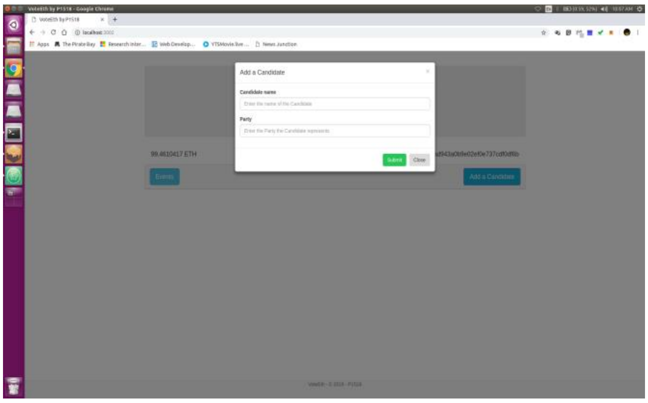
VoteEth

99.4610417 ETH

0xe0bed5a43274ead943a0b9e02ef0e737cdf0df6b

Figure 2 Initial Setup

The administrator is responsible for the initial deployment of both the Registrar and Creator contracts to activate the system and enable users to start registering, voting, and creating new voting contracts. When deploying the Registrar Contract, the administrator is also responsible for whitelisting a set of e-mail domains that are allowed to register to be part of the voting system.

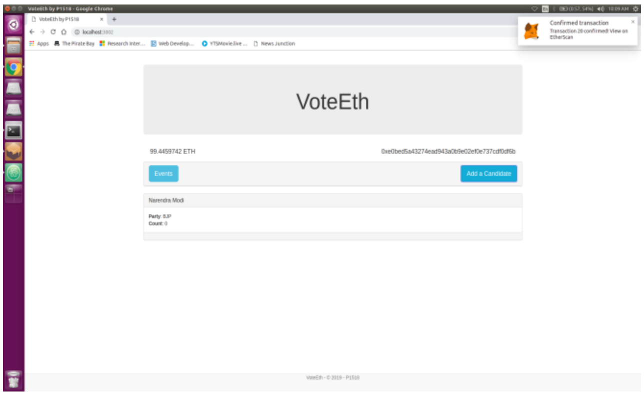


Add a Candidate

Candidate name: Enter the name of the Candidate

Party: Enter the Party the Candidate represents

Figure 3 Adding Candidate



Confirmed transaction
Transaction 20 confirmed! View on EtherScan

VoteEth

99.4459742 ETH

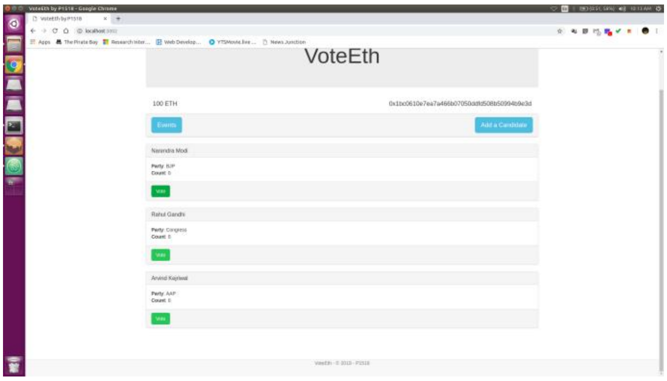
0xe0bed5a43274ead943a0b9e02ef0e737cdf0df6b

Narendra Modi

Party: BJP
Count: 0

Figure 4 List of Candidates

DOI : 10.18231/2454-9150.2019.0580



VoteEth

100 ETH

0x1bc0610e7ea7a466b07050ddfd508b50994b9e3d

Narendra Modi

Party: BJP
Count: 0

Rahul Gandhi

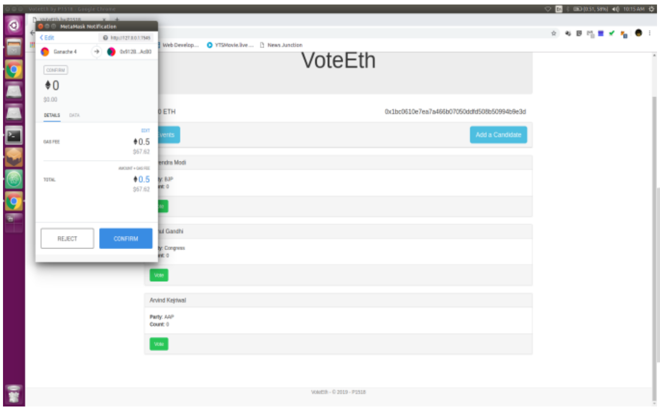
Party: Congress
Count: 0

Arvind Kejriwal

Party: AAP
Count: 0

VoteEth - © 2019 - P1518

Figure 5 Casting Vote Page



MetaMask Notification

Ganache 4 → 0x9128...Ac80

CONFIRM

0

$0.00

GAS FEE 0.5 $67.62

AMOUNT + GAS FEE

TOTAL 0.5 $67.62

VoteEth

0x1bc0610e7ea7a466b07050ddfd508b50994b9e3d

Arvind Kejriwal

Party: AAP
Count: 0

VoteEth - © 2019 - P1518

Figure 6 Confirmation Of Transcation

VI. 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. There needs to be concerted effort in the core blockchain technology research to improve is features and support for complex applications that can execute within the blockchain network.

References

[1] L. C. Schaupp and L. Carter, “E-voting: from apathy to adoption,” Journal of Enterprise Information Management, vol. 18, no. 5, pp. 586–601, 2005.

[2] W. D. Eggers, Government 2.0: Using technology to improve education, cut red tape, reduce gridlock, and enhance democracy. Rowman & Littlefield, 2007.

[3] T. M. Harrison, T. A. Pardo, and M. Cook, “Creating open government ecosystems: A research and development agenda,” Future Internet, vol. 4, no. 4, pp. 900–928, 2012.

[4] K.-H. Wang, S. K. Mondal, K. Chan, and X. Xie, “A review of contemporary e-voting: Requirements, technology, systems and usability,” Data Science and Pattern Recognition, vol. 1, no. 1, pp. 31–47, 2017.

[5] D. A. Gritzalis, “Principles and requirements for a secure e-voting system,” Computers & Security, vol. 21, no. 6, pp. 539–556, 2002.

[6] R. Anane, R. Freeland, and G. Theodoropoulos, “E-voting requirements and implementation,” in The 9th IEEE CEC/EEE 2007. IEEE, 2007, pp. 382–392.

[7] T. Moura and A. Gomes, “Blockchain voting and its effects on election transparency and voter confidence,” in Proceedings of the 18th Annual International Conference on Digital Government Research, ser. dg.o ’17. New York, NY, USA: ACM, 2017, pp. 574–575. [Online]. Available: http://doi.acm.org/10.1145/3085228.3085263

[8] A. B. Ayed, “A conceptual secure blockchain-based electronic voting system,” International Journal of Network Security & Its Applications, vol. 9, no. 3, 2017.

[9] P. McCorry, S. F. Shahandashti, and F. Hao, “A smart contract for boardroom voting with maximum voter privacy,” in International Conference on Financial Cryptography and Data Security. Springer, 2017, pp. 357–375.

[10] BitCongress. Control the world from your phone. [Online]. Available: http://www.bitcongress.org/BitCongress Whitepaper.pdf

[11] FollowMyVote.com, Tech. Rep., 2017. [Online]. Available: https: //followmyvote.com

[12] “Tivi - verificable voting: Accesssible, anytime, anwhere,” TIVI, Tech. Rep., 2017. [Online]. Available: https://tivi.io

DOI : 10.18231/2454-9150.2019.0580