Advances and Applications in Mathematical Sciences
Volume 18, Issue 9, July 2019, Pages 843-850
© 2019 Mili Publications

DECENTRALIZED E-VOTING IN CRUCIAL NETWORK USING BLOCKCHAIN TECHNOLOGY

MANOJ ATHREYA A, ASHWIN A KUMAR, NAGARAJATH S M, GURURAJ H L, RAVI KUMAR V, SACHIN D N and RAKESH K

Computer Science & Engineering
Vidyavardhaka College of Engineering
Mysuru, India
E-mail: manojathreya.cs@vvce.ac.in
ashwinkumar.cs@vvce.ac.in
nagarajath.cs@vvce.ac.in
gururaj1711@vvce.ac.in

Abstract

E-Voting (Electronic Voting) is a mechanism of voting through electronic means to aid the chores of casting and counting of votes. It can be defined as a voting machine connected to internet, to this e-voting mechanism we introduce blockchain technology. In this method each voter will be a peer in the network of peers, it has a decentralized architecture where it runs on a voting pattern which is fair, open and verifiable system where ballot-box is a transparent medium. Blockchain is a growing list of records called blocks, that are linked using cryptography. It is a decentralized, distributed and an immutable ledger to store digital transactions. Its databases are managed using peer-to-peer network where all the nodes in a network are equal and is the major concern in the types of network architecture. The decentralization of blockchain means that it won't depend on a central point of control. With a lack of single authority, which makes the system equitable and more secure to validate transactions and to record data which makes it incorruptible. It uses consensus protocol for efficient transmission and communication of data between nodes. There are many online voting systems available which are of client-server architecture and will have single point of failure, but using blockchain technology we can eliminate it and provide more efficient mechanism for existing one. In this paper, we have proposed an efficient and secured way of e-voting using blockchain technology, the e-voting is done in a decentralized network and there exist many approaches, but the approach using blockchain technology provides a new dimension to the application.

2010 Mathematics Subject Classification: Primary 05A15; Secondary 11B68, 34A05.

Keywords: Blockchain, *E*-Voting, Decentralized, Distributed peer-to-peer network, Smart contracts.

Received December 17, 2018; Accepted January 23, 2019

1. Introduction

E-voting is a system where people vote through internet using ethereum account. The voter should have an ethereum account which acts as a identity card for voting, then the voter selects the candidate and votes for that person [1]. The person can vote from remote location it does not need to come to the voting booth for voting. This can be implemented worldwide and the technology used is more secure and safe. Blockchain is a set of linked-lists where the data stored in it is immutable, which means once the data is stored it cannot be changed. It is decentralized, distributed and public digital ledger. Decentralization means storing data in different nodes across peer-to-peer network, thus eliminating the risks when the data is stored centrally [2]. A blockchain, also called as a distributed, immutable ledger is essentially an append-only data structure maintained by set of nodes which won't trust each-other fully. Nodes in a blockchain network agree on a set of blocks which are ordered, having multiple transactions. Hence, blockchain is viewed as a log of ordered transactions [3]. Centralized applications have been in presence for a very long period of time and certainly has many drawbacks and issues of its own like single point of failure, hackable, less transparent and cannot bail internet censorship. For decades, we have been putting our eggs in a basket and that too in someone else's basket which simply means that to create trust between ourselves, we rely on third parties and Blockchain solves the problem the middleman [4]. Blockchain serves a most potent solution to resolve this issue. It is one of the unruliest techs out there. Its distributed, decentralized and immutable properties make it the absolute way to store and track data across numerous domains and use case [5].

Blockchain enabled smart contracts employ proof-of-stake validation for transactions, which promises significant performance advantages compared to proof-of-work solutions [6]. Smart contracts have become a reality with the boom of blockchain technology, which operates without trusted third parties for settling transactions and disagreements among pseudonymous participates [7]. Peer-to-Peer (P2P) protocols provides distribution of high data capacity to users, which are scalable [8]. Peer-to-peer blockchain networks has no central point of failure, as they lack centralize points of vulnerability that hackers can exploit. Blockchain technology can be used to create a constant, transparent, public ledger for organizing sales records, which tracks digital usage and payments distribution to content creators. [9]. Ethereum is an essential and an ultimate foundation layer, where a blockchain with in-built Turing-complete programming language. It allows anybody to write smart contracts for building decentralized applications with their own rules of state functions, transactions, and ownership [10].

By having all these functionalities and enhanced features when compared to the existing system which lies in a centralized network, our decentralized network provides better standards to the system. The proposed theory shows how this is made possible and makes the system easier.

2. Related Work

2.1. Ethereum Blockchain

A blockchain is a cryptographically safe transactional singleton machine with shared state and The Ethereum blockchain is fundamentally a transaction-based state machine. In computer science, a state machine refers to a series of inputs and based on those inputs, will transition to a new state.

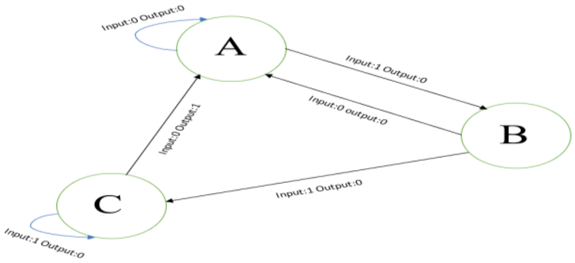


Figure 2.1

The first state is called as genesis state which is similar to a blank state on the network. When transactions are executed, this genesis state transitions into some final state. At any point in time, this final state represents the current state of Ethereum.

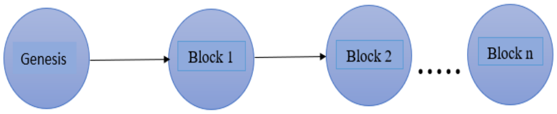


Figure 2.2

As per definition, we have a transactional singleton machine with shared-state but whenever multiple paths are generated, it is called fork.

Basic fundamental of Ethereum:

- Accounts: A account always has a transition state associated with it and a 20-byte address. A Ethereum address system is a 160 bit that is used to find existence of any account.

- State: Ethereum is built on a transaction state machine on which technology handles all transactio based state machine concepts.

- Gas and Fees: Each and every computation result in transaction on the Ethereum network which incurs a fee and that fee is paid in terms of some form called gas.

- Transactions: A transaction is a cryptographically signed piece of instruction that is generated by an externally owned account, serialized, and then submitted to the blockchain.

- Blocks: All transactions are added to a block and a series of such blocks that are chained together to infinite length are called blockchain.

- Mining and Proof of Work: Proof of work describes a system that needs a not-insignificant but feasible amount of effort in order to deter malicious uses of computing power.

3. Mathematical Analysis

ECDSA stands for Elliptic Curve Digital Signature Algorithm. It is an algorithm that uses an elliptic curve to “sign” data where third parties can verify the signature.

The cryptographic hash function SHA-256

SHA-256 is a cryptographic keyless hash function; that is, an MDC (Manipulation Detection Code).

The algorithm uses the following functions:

$\mathrm{Ch}(A, B, C) = (A \wedge B) \oplus (A \wedge C)$,

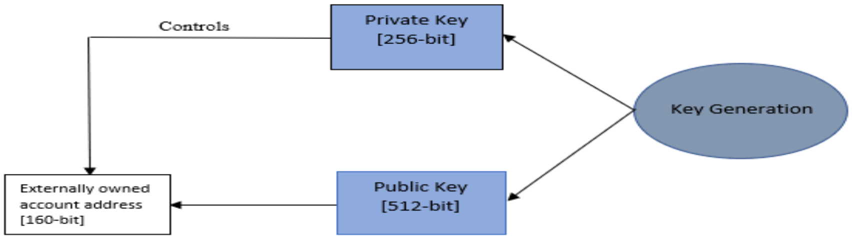
$\mathrm{Maj}(A, B, C) = (A \wedge B) \oplus (A \wedge C) \oplus (B \wedge C)$,

$\Sigma0(X) = \mathrm{RotR}(A, 2) \oplus \mathrm{RotR}(A, 13) \oplus \mathrm{RotR}(A, 22)$,

$\Sigma1(X) = \mathrm{RotR}(A, 6) \oplus \mathrm{RotR}(A, 11) \oplus \mathrm{RotR}(A, 25)$,

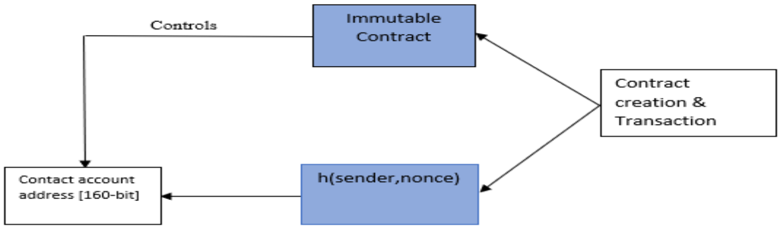
$\sigma0(X) = \mathrm{RotR}(A, 7) \oplus \mathrm{RotR}(A,18) \oplus \mathrm{ShR}(A, 3)$,

$\sigma1(X) = \mathrm{RotR}(A, 17) \oplus \mathrm{RotR}(A, 19) \oplus \mathrm{ShR}(A, 10)$,



Address and key generation for externally owned contracts

Figure 3.1


Controls
Immutable Contract
Contract creation & Transaction
Contact account address [160-bit]
h(sender,nonce)

Contract account creation

Figure 3.2

4. Case Study Analysis

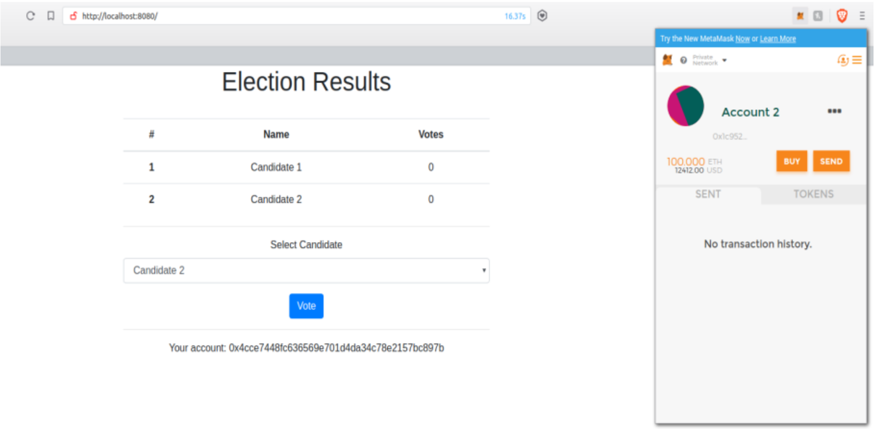
The most remarkable thing about this Blockchain technology is that it increases the capacity of the whole network and keeps its ledgers in a never-ending state of forwarding momentum making it immutable. This technology is extremely secure as every individual who gets in the blockchain network is given with unique identification address. This guarantees that the account holder himself is handling the transactions. The encryption of block in chain makes it hard-boiled for any hacker to strike the existing setup of the chain. Transaction speed is increased to very high level as existing banking organisation takes plenty of time to process and initiate transaction.

Ethereum is preferred as a better platform for development and blockchain network. Extending the network which provides wide extent of use cases, which is powered by smart contracts. All transactions are done in real time and for some exchange of Ethers (currency of Ethereum network), all blocks area scripted by miners, who execute these scripting and validation transaction, which is expensive with respect to energy and time.

Use of real Ethereum network is quite expensive for experimenting, developing and testing purpose (requires spending of Ethers). Also, it occupies huge memory in network. Thus, private Test networks are used and made available to the developers and one of them is Ganache, which is a personal blockchain used to build and deploy dApps. In order to extend your test network, peers should download a legit wallet from the official website and change the connection with main network to preferred test network.

4.1. Methodology

Metamask is one of the browser extension which enables to interact with dapps and are available on all popular browsers. Connect MetaMask using seed phrase created by Ganache.



http://localhost:8080/

Election Results

#	Name	Votes
1	Candidate 1	0
2	Candidate 2	0

Select Candidate

Candidate 2

Vote

Your account: 0x4cce7448fc636569e701d4da34c78e2157bc897b

Try the New MetaMask Now or Learn More

Private Network

Account 2

0x1c952...

100.000 ETH
12412.00 USD

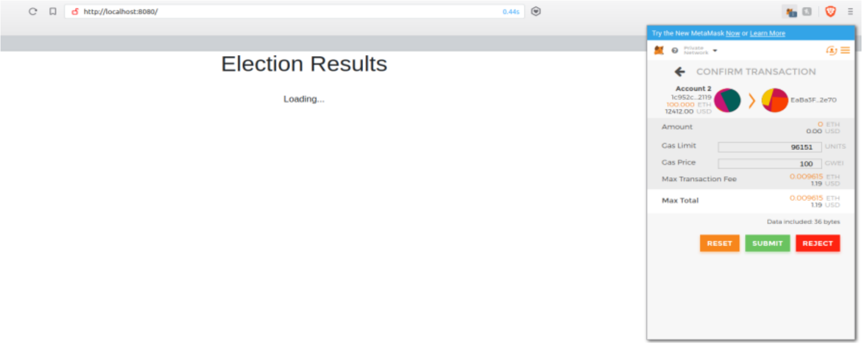
BUY SEND

SENT TOKENS

No transaction history.

Figure 4.1

The user chooses the candidate which they wish and clicks on the Vote button, where a Metamask prompt will automatically open seeking to agree the transaction.


http://localhost:8080/

Election Results

Loading...

Try the New MetaMask Now or Learn More

Private Network

CONFIRM TRANSACTION

Account 2
1c952c...2119
100.000 ETH
12412.00 USD

EaBa3F...2e70

Amount 0 ETH 0.00 USD

Gas Limit 96151 UNITS

Gas Price 100 GWEI

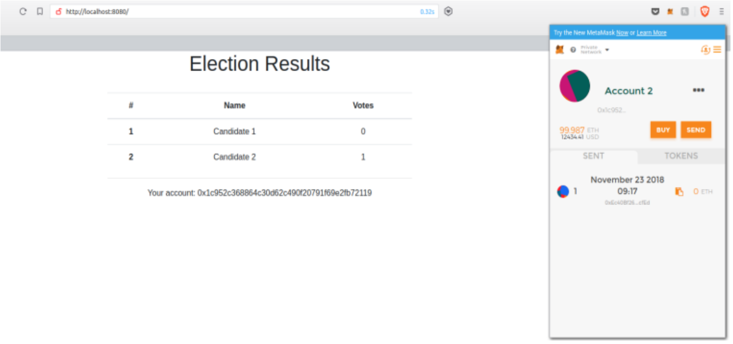
Max Transaction Fee 0.009615 ETH 1.19 USD

Max Total 0.009615 ETH 1.19 USD

Data included: 36 bytes

Figure 4.2

Click Submit to accept the transaction. This would add a new transaction in the blockchain returning the transaction hash and displays election result which also disables to vote again.


http://localhost:8080/

Election Results

#	Name	Votes
1	Candidate 1	0
2	Candidate 2	1

Your account: 0x1c952c368864c30d62c490f20791f69e2fb72119

Try the New MetaMask Now or Learn More

Private Network

Account 2
0x1c952...

99.987 ETH
12434.41 USD

November 23 2018 09:17
1
0xEc40Bf26...cfEd
0 ETH

Figure 4.3

5. Conclusion

This paper, proposes different technology stack for reliable *e*-voting system. Where the voting format is made simpler and easier. It provides a new dimension to the existing technology as blockchain implemented e-voting system is a new of its kind. Our architecture uses blockchain technology which assures more security to the data, it focuses mainly on functionality of blockchain enforced smart contracts. They incorporate methods for managing automated smart contracts which are more efficient and secure matching with hierarchical conditional structures and transfer of contract between various smart contracts. Blockchain enforced smart contracts enables services which are automated, efficient, secure and allow resource distribution. The mathematical analysis and case-study analysis proposed in this paper show the robustness, security, scalability factor and its unique features to provide better-user environment.

References

[1] Vitalik Buterin, A next generation smart contract & decentralized application platform, Ethereum White Paper 2013.

[2] Yu Nandar Aung and Thitinan Tantidham, Review of Ethereum: Smart Home Case Study, 2017, 2nd International Conference on Information Technology (INCIT)

[3] Ali Kaan Koç, Emre Yavuz, Umut Can Çabuk, Gökhan DalkÕlÕç, Towards Secure E-Voting Using Ethereum Blockchain, 2018 IEEE.

[4] Thang N. Dinh and My T. Thai, AI and Blockchain: A Disruptive Integration, IEEE COMPUTER SOCIETY 2017.

[5] Zhongxing Ming, Shu Yang, Qi Li, Dan Wang, Mingwei Xu, Ke Xu and Laizhong Cui, Black cloud: A Blockchain-based Service-centric Network Stack, block cloud technical whitepaper 2016.

[6] Christopher Ehmke, Florian Wessling and Christoph M. Friedrich, Proof-of-Property-*A* Lightweight and Scalable Blockchain Protocol, 2018 ACM/IEEE 1st International Workshop on Emerging Trends in Software Engineering for Blockchain.

[7] Andrei Sambra, Amy Guy and Sarven Capadisli, Building Decentralized Applications for the Social Web, WWW 2016 Companion, April 11-15, 2016, Montréal, Québec, Canada. ACM 978-1-4503-4144-8/16/04. http://dx.doi.org/10.1145/2872518.2891060

[8] Tien Tuan Anh Dinh, Rui Liu and Meihui Zhang, Untangling Blockchain: A Data Processing View of Blockchain Systems, 2017 IEEE.

[9] Massimo Bartoletti, Stefano Lande, Livio Pompianu and Andrean Bracciali, A general framework for blockchain analytics, 2017 ACM.

[10] Matthias Wichtlhuber, Peter Heise, Björn Scheurich and David Hausheer, Reciprocity with Virtual Nodes: Supporting Mobile Peers in Peer-to-Peer Content Distribution, 9th CNSM 2013.

[11] Satoshi Nakamoto (24 May 2009), Bitcoin: A Peer-to-Peer Electronic Cash System

[12] Patrick Dai, Neil Mahi, Jordan Earls and Alex Norta, Smart-Contract Value-Transfer Protocols on a Distributed Mobile Application Platform, 2017 IEEE

[13] Craig Wright and Antoaneta Serguieva, Sustainable Blockchain-Enabled Services: Smart Contracts, 2017 IEEE International Conference on Big Data (BIGDATA).