Journal of Information Technology Management

Print ISSN: 2008-5893

Online ISSN: 2423-5059

A Decentralized Polling System Using Ethereum Technology

Samarth Shakya*

*Corresponding Author, MSc in Information Security, Department of Information Technology, Institute of Engineering Technology Devi Ahilya University, Indore 452017, India. E-mail: samarthshakya@gmail.com

Vivek Kapoor

Assistant Professor, Department of Information Technology, Institute of Engineering Technology Devi Ahilya University, Indore 452017, India. E-mail: vkapoor@ietdavv.edu.in

Abstract

Polling system is not trusted everywhere around the world it is very important in this modern world to replace the traditional polling system with the new technology. Some countries like United States, Japan, and India suffer from corrupted polling system. Major issues are faced by current polling systems like system hacking, vote rigging, vote manipulation, distributed denial of service attack, and online polling booth capturing. This paper will lead to the problems faced by the traditional polling system and how the new technology will provide the solution to that problem. Also, our purpose is to check the feasibility of the system by recording the transaction fees and evaluate the right way to spend the amount of gas in the transaction. This will highlight blockchain frameworks including blockchain as a service and polling system which is on blockchain that addresses all constraint introducing ethereum which is a blockchain-based distributed computing platform. Ethereum is open source, and publicly available with a system featuring smart contracts. It provides the cryptocurrency wallets that let you make cheap, instant payments with gas in the form of ethers. The ethereum community is the most active and largest blockchain community in the world. There is no centralized organization that controls ethereum.

Keywords: Blockchain; Ethereum; Decentralization; Gas; Distributed System; Metamask

DOI: https://10.22059/jitm.2022.85645 Manuscript Type: Research Paper University of Tehran, Faculty of Management

Received: January 12, 2021 Accepted: March 25, 2020

Introduction

Blockchain is relatively new technology, as we see the earlier work in Blockchain some of research is extended from side to side in the last ten years. The area of investigation are security and privacy check on blockchain and usage of blockchain in various ways with digital ledger techniques, their challenges and application. Many countries are seeking the opportunity and have taken some initiative to improve their existing voting system by making it a decentralized voting system with peer-to-peer network. The first country in the world to use blockchain technology is Sierra Leone to verify votes in an election in March, 2018. Blockchain is the best technology for polling systems because it provides the failure to modify or remove information from blocks makes the polling system immutable. Blockchain technology consists of a large number of interconnected nodes is supported by a distributed network. Nodes have their own copy of distributed ledger which have the record of all the transactions processed by the network. There will be no single authority that controls the network. This network allows users to vote anonymously. It is making e-voting acceptable as our modern democracies are built up on voting system. The Increase of voter lack of enthusiasm in recent years, especially among the younger generation which is more into computers and technology the e-voting is a potential solution to attract voters specially the young one. A robust polling scheme requires distribution of authority which is provided in blockchain. A great decentralized application utilizing blockchain technology allows you perform the same actions without a third party. Since a blockchain is a permanent record of transactions(votes) that are distributed on every node making votes immutable. Introducing a secured and customizable voting application made for everyday use built on the Ethereum blockchain, a 100% decentralized platform customizable and simple, so that you can remove your focus from security and focus on what matters.

Rationale

Polling system focuses on voting techniques which can be applied concomitantly to business purposes. The main objective of this is to bring together the seemingly disparate fields, such as Decentralized applications, Ethereum, Smart contracts, Blockchain and Knowledge discovery.

The problem with existing e-voting system is:

1. Centralized Architecture
2. Hacking of the centralized voting systems.
3. Election Manipulation.
4. Vote casting: Votes should be anonymous to everyone including the administrators.
5. Security problems: The DDoS attacks are well known attack in voting systems.
6. No transparency and trust: People usually do not trust when everything is online.

All these are the reasons which seeks and motivates to develop a decentralized system.

There are some of the objectives to which we have focus while developing a decentralized ethereum polling system. To make any transaction in ethereum based system we have to pay some transaction fee that is also known as gas. This gas is variable with the transaction and the words used by user in the transaction.

This research focuses on the feasibility of the polling system as we are going to use a large number of transactions. It also defines the proportion in which the transaction being processed. The agenda behind developing a polling system is to give people a right to vote on particular scenarios rather than electing a particular candidate to do so. People can also give the topics to get the votes from the people anonymously.

Background

The solution to the voting problem is to use ethereum technology. It serves the property of distribution, immutability, irreversibility, provides data-security and more importantly it is decentralized. The background working of ethereum blockchain technology can be classified in five main features:

a) Smart Contract: Developer creates a decentralized application while using the Ethereum technology with creation of a self-enforcing piece that managed by peer to peer network of computer according to the need. This smart contract can contain the business logic or agreement between the two or more people directly written in the lines of code. Smart contracts are created with a help of open source solidity programming platform like *remix.ethereum* and tested and deployed with the help of truffle framework.
b) Publishing: After the creation, that smart contract is published on ethereum blockchain and to publish it some amount of ether is deducted from the connected blockchain account. The publishing of smart contract can be done with truffle framework by a command *truffle migrate*.
c) User: To use the decentralized application user has to pay some amount of ether. To do so user/client must have an active ethereum account with a private key. The user account must contain some amount of gas to process the transaction. Transaction for each allowed feature can be processed only once. This feature gives the quality of uniqueness to the system. To pay ether user should have metamask extension in systems browser.
d) Miners: They verify or validate the transactions and add it to a new block these blocks together forms a ledger which is distributed among all the nodes. Based on a cryptographic hash algorithm they compete to solve a difficult mathematical problem and the solution is called the Proof-Of-Work. They are also rewarded with ether for each successful block.
e) Nodes: A infrastructure of blockchain is formed by nodes. They check a newly formed

block and add it to the blockchain. Any proposed "new block" to the ledger must reference the previous version of the ledger, which creates a chain possess immutability.

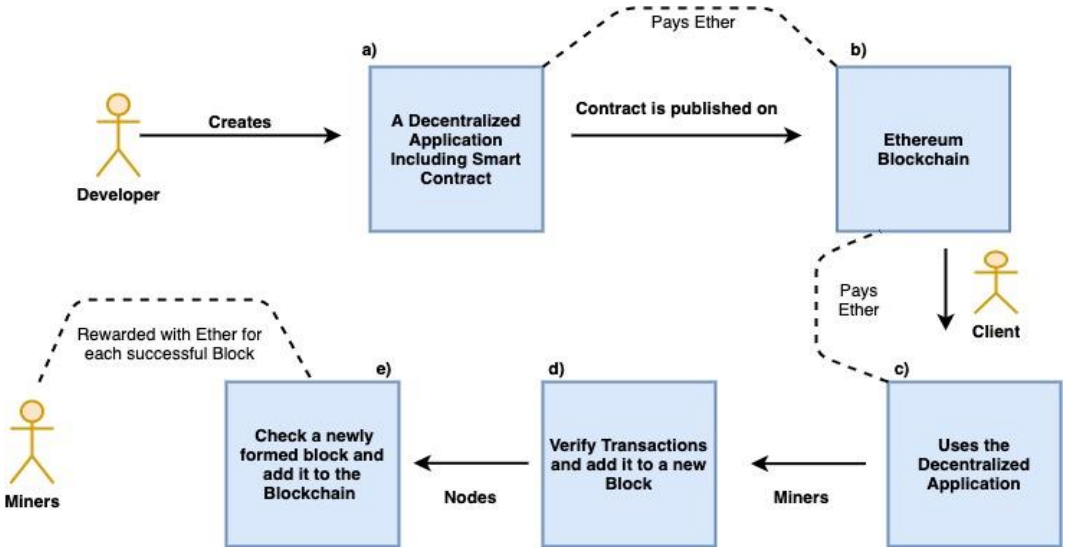

Figure 1. Background flow of ethereum blockchain.

Proposed System

In this section we introduce our proposed polling system that aims at solving the existing barriers.

System Components

The proposed platform consists of the various following components:

1) Smart Contract: There is only one type of smart contract present in our system that is polling contract. This contract serves purpose to authenticate the voters and start the voting process. Polling contract increment the count of votes immediately when voted. It ensure the feature that only one vote is given with the private key. Appendices A list the code of our polling contract.
2) Ganache: It acts as a public blockchain dependency. Ganache is a personal blockchain deployed locally. We are going to use the ganache for the deployment of our polling contract and running tests. Appendices B list the free accounts provided by ganache to test out smart contract on local blockchain bases.
3) Truffle Framework: Truffle is a tool used to develop ethereum blockchain while using the solidity programming language. Truffle also provides various functionalities like automated testing, client side development, network and smart contract management. Appendices C shows the test result using truffle framework.
4) Metamask: If we want to use a user interface of any application our browser should support the connection to blockchain network. Metamask is the browser extension or

plugin used to connect to the required blockchain network. We can also manage our personal accounts in Metamask. We can install it in Chrome, Firefox and Opera. Appendices D shows the Metamask account in chrome browser.

Experiment

If we begin using polling application we will get to know that the amount of gas we are paying while using metamask is not constant. There is an option in metamask to choose the amount of gas we have to pay like slow, average and fast time transaction cost. To know how it is varying we had recorded the number of letters used to provide the topic to vote and the amount of gas which is in ETH required for them to complete the transaction as shown in Table 1.

Table 1. Experiment Data Record

No. Of Letters	Slow Cost (ETH)	Slow Time	Average Cost (ETH)	Average Time	Fast Cost (ETH)	Fast Time	Hex DATA
1	0.00343776	17min 12sec	0.000418977	3min 42sec	0.00547893	24 sec	100
5	0.003440064	3min 12sec	0.004085076	3min 12 sec	0.005482602	24 sec	100
10	0.003442944	11min 2sec	0.00376572	3min42sec	0.005594784	24 sec	100
15	0.003445824	13min 6 sec	0.003984234	3min 54 sec	0.005599464	24 sec	100
20	0.003448704	9min 42sec	0.00377202	4min 0 sec	0.005604144	30 sec	100
25	0.003343722	19min30sec	0.004098756	3min 54sec	0.005608824	30 sec	100
30	0.003346512	17min 24sec	0.004102176	3min 54sec	0.005613504	30 sec	100
35	0.00505506	22min 2 sec	0.006571578	3min 30sec	0.008762104	30 sec	132
40	0.005394944	21min 48 sec	0.00674368	3min 42sec	0.008935376	36 sec	132
45	0.00506046	20 min 18sec	0.00674728	3min 1sec	0.008771464	36 sec	132
50	0.005569476	20min 46sec	0.007257196	3 min 30 sec	0.009113688	36 sec	132

Results

With the recorded table we can conclude that the amount as gas is variable with number of letters used as well as the time required to complete the transaction. These can be easily understandable by the following recorded graphs.

Analysing the number of letters with amount of gas required.

Considering the Fast Cost (ETH) from the Table 1 we can see that the amount of ETH required is slightly increasing as we increase the number of letters in our transaction. That means if we want to create a block with a long phrase we need to pay the higher amount of gas for the transaction.

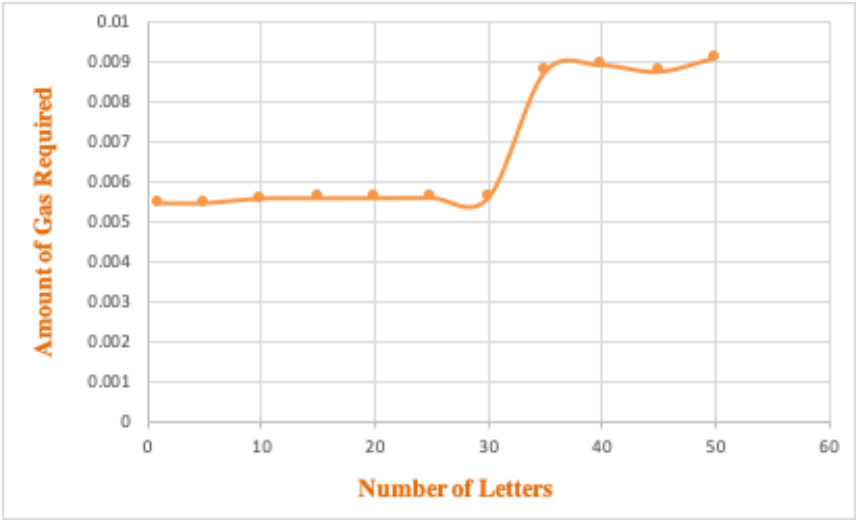

Figure 2. Number of letters vs amount of gas required.

Analysing the number of letters with time required to complete the transaction

Considering the Fast Time (seconds) from Table 1 we can conclude that the time required to complete the transaction is directly proportional to the number of letters in the phrase. More the number of letters in the phrase more time it will take to complete the transaction.

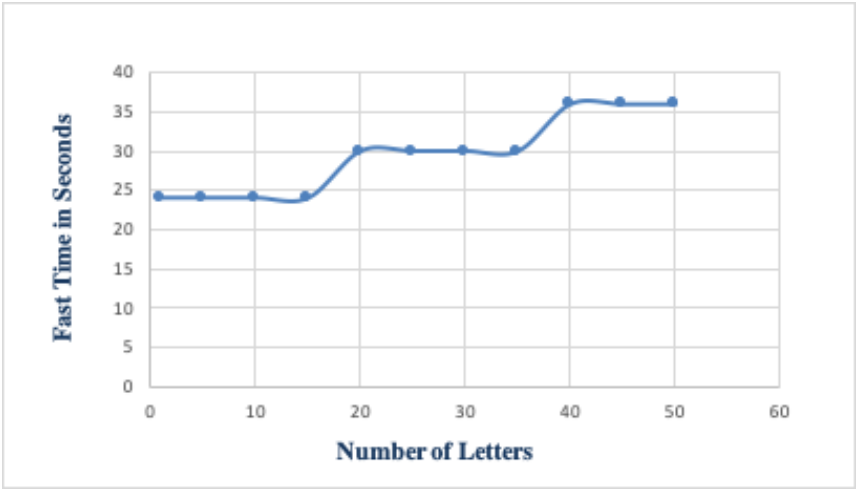

Figure 3. Number of letters vs time required.

Analysing the Efficient way to choose the transaction type.

We can see that Fast transaction type is better than any other type as there is only a slight change in the ETH but the time difference is very high in all other transaction as shown in Table 1. All the transaction type are showing the similar property as compare to the amount of gas which is a direct proportion.

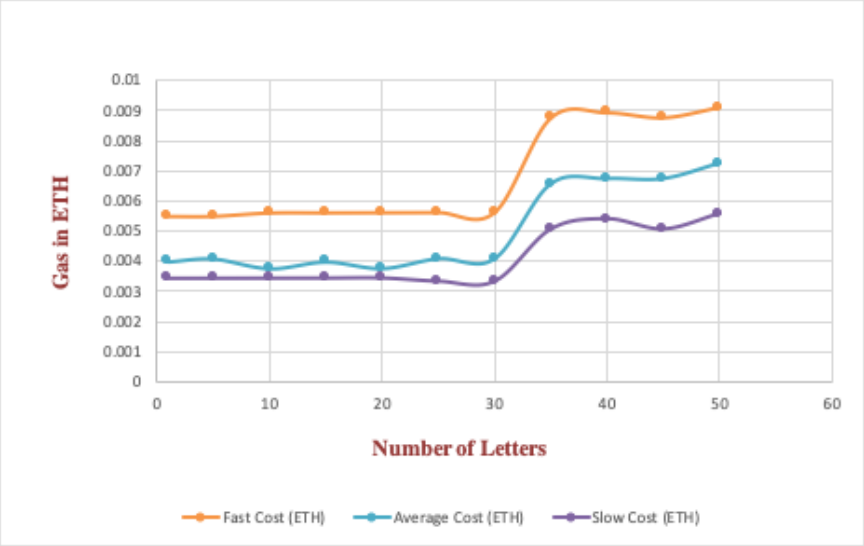

Figure 4. Number of letters vs Fast-Average-Slow Cost (ETH)

Conclusion

The paper analyzes the polling system on real world scenarios and implemented it using the ethereum technology. It also gives the experiment regarding the variability of amount of gas which we pay during transaction using metamask by finding the efficient way to do so. It also gives a brief idea about tools used for the developing an ethereum blockchain based application. By reading this paper carefully one can develop an ethereum blockchain application of their own by following the steps given. This polling system integrates the election voting to a new form where one can vote on real world scenario or one can clears their confusion regarding to any topic with the opinions of people.

Conflict of interest

The authors declare no potential conflict of interest regarding the publication of this work. In addition, the ethical issues including plagiarism, informed consent, misconduct, data fabrication and, or falsification, double publication and, or submission, and redundancy have been completely witnessed by the authors.

Funding

The author(s) received no financial support for the research, authorship, and/or publication of this article

References

Ben Ayed, A. (2017). A Conceptual Secure Blockchain- Based Electronic Voting System. *International Journal of Network Security & Its Applications (IJNSA)*, 9 (3).

Bhosale, K.; Akbarabbas, K.; Deepak, J. & Sankhe, A. (2019). Blockchain based Secure Data Storage. *International Research Journal of Engineering and Technology (IRJET)*, 6 (3).

Bulut, R.; Kantarcı, A.; Keskin, S.; Bahtiyar, S. (2018). Blockchain-Based Electronic Voting System for Elections in Turkey. *Istanbul Technical University Istanbul, Turkey.*

Chan Zheng Wei, Clement; Chai Wen Chuah (2018): Blockchain-Based Electronic Voting Protocol. *International Journal On Informatics Visualization*, 2 (4).

H. Bergquist, Jonatan (2017): Blockchain Technology and Smart Contracts. *Uppsala Universitet Examensarbete 30 hp* .

Hatiskar, Vaibhav; G. Pai, Archana (2018): Blockchain and it's Integration with Supply Chain. *International Journal of Computer Applications (0975 – 8887)*, 179 (52).

Kaan Koç, Ali; Yavuz, Emre; Can Çabuk, Umut; Dalkılıç, Gökhan (2018): Towards Secure E-Voting Using Ethereum Blockchain. *researchgate.net/publication/323318041*.

McCorry, Patrick; F. Shahandashti Siamak; Hao Feng (2017): A Smart Contract for Boardroom Voting with Maximum Voter Privacy. *School of Computing Science, Newcastle University UK.*

Khan, Tayyab, Karan Singh, Mohamed Abdel-Basset, Hoang Viet Long, Satya P. Singh, and Manisha Manjul. "A novel and comprehensive trust estimation clustering based approach for large scale wireless sensor networks." IEEE Access 7 (2019): 58221-58240.

Pareek, Shubham; Upadhyay, Anuj; Doulani, Satya; Tyagi, Siddarth; Varma, Aditya(2018): E-Voting using Ethereum Blockchain. *International Journal for Research Trends and Innovation*, 3 (11).

Shrinivas, Manoj; S.Chandan; Farhan Shamail, Mohammed; K, Ramyashree (2019): A Decentralized Voting Application using Blockchain Technology. *International Research Journal of Engineering and Technology (IRJET)*, 6 (4).

Tso, Raylin; Liu, Zi-Yuan; Hsiao, Jen-Ho(2019): Distributed E-Voting and E-Bidding Systems Based on Smart Contract. *Multidisciplinary Digital Publishing Institute.*

V. Arun; Dutta, Aditya; Rajeev, Sourav; Mathew Varghese, Rohan (2019): E-Voting using a Decentralized Ethereum Application. *International Journal of Engineering and Advanced Technology (IJEAT) ISSN: 2249-8958*, 8 (4).

www.dappuniversity.com/articles/the-ultimate-ethereum-dapp-tutorial (Building an Ethereum Decentralized Application)

Bibliographic information of this paper for citing:

Shakya, Samarth, & Kapoor, Samarth (2022). A Decentralized Polling System Using Ethereum Technology. *Journal of Information Technology Management*, Special Issue, 1-8.