IJIRCCE

e-ISSN: 2320-9801 | p-ISSN: 2320-9798

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

Volume 10, Issue 4, April 2022

INTERNATIONAL STANDARD SERIAL NUMBER INDIA

Impact Factor: 8.165

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 4, April 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1004096|

Blockchain Based Online Voting

Sahil Phalle, Shweta Kadam, Mithilesh Dudhal, Vighnesh Kamath, Prof. Sagar Rajebhosale

UG Students, Dept. of C.S., Keystone School of Engineering, Pune, Maharashtra, India

Assistant Professor, Dept. of C.S., Keystone School of Engineering, Pune, Maharashtra, India

ABSTRACT: Election is a way to choose the representatives through a fairness, integrity, and democratic rules. During the election, the voting system, allows authenticated voters to declare their vote for contender. In aspect, the voting mechanism can exactly control many elements that are political science, social science, and economics.
Thus, the approach of the voting mechanism prerequisite responds and should be treated before the election is taken. The voting mechanism initiate evolving from paper voting, then electronic voting and the current will be Internet voting. briefly, E-voting is simply an electronic system, while Internet voting is nothing but remote electronic voting.
E-voting is the ubiquitous globally and it is a means that often represents freedom of the election. Therefore, most of the countries sustain to research and develop the E-voting process. Eventually, the current voting system is however far from what it should deliver. It provides a decentralized structure that distributes online information synchronously among the peer-to-peer network without a centralized database. Because of machinery improvement, Blockchain has represented a specific technology that to the test like "ideal online privacy" and Web 3.0 decentralized apps. Hence, the study proposes Blockchain based Online Voting System to enhance the integrity, optimize the voting practice, produces persistent voting results, and bolster the clarity of the voting system. Lastly, the research addressed the flaws of the current Internet-voting system and auspiciously applied Blockchain technology to resolve those weaknesses.

KEYWORDS: Blockchain; E-voting; Ethereum; I-voting; Web 3.0.

I. INTRODUCTION

Election has a very major role in democracy because it is the deciding factor of the future of a country but the major concern is that society doesn't trust the election system. improper electrical system is the issue seen by even the world's biggest democracies like United States, India and Japan. Additionally, the voting mechanism have cultured and the infringement of security has evolved. The extensive issues that commitment to be send in the present voting mechanism are vote implements, EVM hacking, polling booth seize and election manipulation.

The complication was inspected in the voting systems in this project and attempting to propose the online-voting model that can solve these problems. Using an adequate hashing algorithm approach, block formation and isolate, data collection and result declaration by resourceful blockchain method is mandatory to fix the issue a high-end to end system that ensures security and privacy. This project proposes an online-voting system that uses the Blockchain Ethereum to create a wallet with the credentials of the user. The elector will gain a tamper-proof and authenticated personal ID. The user will be getting the opportunity to vote in the using token which would be transmitted anonymously from voter's wallet to candidate's wallet.

Blockchain also uses to conserve voters' inconspicuousness while still public can inspect publicly inspection.

1.1 EXISTING SYSTEM

A) Paper Ballots

The history of the voting system is exceptionally lengthy, start from paper ballots, then E-voting and finally to I-voting. Paper ballots which represent the first voting system that introduced by South Australia and Victoria since 1856, also known as Australian ballot, or secret ballot. The idea of paper ballots was allowing voters to determine their vote by the marking tools (i.e., pen, pencil) and counting process will be using hand-counted or an optical scanner. Even after many years, paper ballots still one of the voting systems considered most "trust." Paper ballot with the optical scan" represent the highest availability during 2012 U.S. presidential elections. Moreover, the researchers constantly compare the EVM with the paper ballots.

Voting Process

- Voter travel to the designated polling station.
- Poll official verifying voter's identity.
- Poll official issues a ballot paper to the voter.
- Voter carry to the area that for marking the paper.

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 4, April 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1004096|

• Voter fold paper.
• The voter determines the vote by marking the paper.
• The voter unfolds the paper.
• The voter places the paper into a box.

B) E-voting

According to the last research, there are 31 countries accomplished with E-voting structure and 20 countries formed out to use EVMs. Electronic voting structure has been all over the place and most used in Asian countries. In globally, India was the largest democracy. transparency, integrity, and Privacy of E-voting structure have been a huge concern that a few of the countries transformed into terminated by it (i.e., Netherland, France). DRE /EVM is the well-used E-voting structure in loads of the democracy. EVM was first introduced by United State since 1974 EVM could be defined into three types which are touchscreens, dials and buttons. After all, they possess one thing in common that reserved the vote into CPU memory. The idea is to merge the counting process and voting which literally says stores the vote when it was choose by the voter. Moreover, to distribute audibility and verifiability, VVPAT would be an add-on to some of the EVMs.

Voting Process

• Voter travel to the designated polling station.
• Poll official verifying voter's identity.
• Voter go to the place for pick vote.
• The voter pick vote selects any one of the knobs that represent the contender on the EVM.

II. LITERATURE SURVEY

In [1] authors useda high security password is checked in the main database beforevoting is allowed. The voter will be able to confirm if the vote is transferred to thecorrect candidate or party. A person from his or her allocated constituency may alsovote. The tallying of the votes can be done manually, thus saving the data. In [2] Authors usedthe main goal of this venture is to build a safe electronic votingmachine using Finger printing technique that distinguishes evidence, so that we canuse the Aadhar card database for specific marks. The online-voting confirmationprocess should be possible during the race voting season using finger vein detection,which enables the electronic poll reset to allow voters to cast their votes. In [3] This paper suggests a system that makes use of appropriate hashingmethods to ensure data security. This paper intro-duces the concept of block creation and block sealing. The implementation of a block sealing principle helps tomake the blockchain flexible to meet polling process requirements. In [4] A Real Indian EVM Security Review is taken from anonymous source. The paper states that EVM is vulnerable to extreme attacks that may alter theoutcome and breach the ballot's confidentiality. Use custom hardware, two attackshave been demonstrated. In [5] Estonia was the first country in the world to use Internet voting nationally, and todaymore than 30% of its ballots are cast online. In this paper, we analyze the security ofthe Estonian I-voting system based on a combination of in-person electionobservation, code review, and adversarial testing. Adopting a threat model thatconsiders the advanced threats faced by a national election system—includingdishonest insiders and state-sponsored attacks—we find that the I-voting system hasserious architectural limitations and procedural gaps that potentially jeopardize theintegrity of elections. In experimental attacks on a reproduction of thesystem, we demonstrate how such attackers could target the election servers orvoters' clients to alter election results or undermine the legitimacy of the system. Ourfindings illustrate the practical obstacles to Internet voting in themodern world, and they carry lessons for Estonia, for other countries consideringadopting such systems, and for the security research community. In [6] Online voting is a trend that is gaining momentum in modern society. It has great potential to decrease organizational costs and increase voter turnout. It eliminates the need to print ballot papers or open polling stations—voters can vote from wherever there is an Internet connection. Despite these benefits, online voting solutions are viewed with a great deal of caution because they introduce new threats. A single vulnerability can lead to large-scale manipulations of votes. Electronic voting systems must be legitimate, accurate, safe, and convenient when used for elections. Nonetheless, adoption may be limited by potential problems associated with electronic voting systems. Blockchain technology came into the ground to overcome these issues and offers decentralized nodes for electronic voting and is used to produce electronic voting systems mainly because of their end-to-end verification advantages. This technology is a beautiful replacement for traditional electronic voting solutions with distributed, non-repudiation, and security protection characteristics. The following article gives an overview of electronic voting systems based on blockchain technology. The main goal of this analysis

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 4, April 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1004096|

was to examine the current status of blockchain-based voting research and online voting systems and any related difficulties to predict future developments. This study provides a conceptual description of the intended blockchain-based electronic voting application and an introduction to the fundamental structure and characteristics of the blockchain in connection to electronic voting. As a consequence of this study, it was discovered that blockchain systems may help solve some of the issues that now plague election systems. On the other hand, the most often mentioned issues in blockchain applications are privacy protection and transaction speed. For a sustainable blockchain-based electronic voting system, the security of remote participation must be viable, and for scalability, transaction speed must be addressed. Due to these concerns, it was determined that the existing frameworks need to be improved to be utilized in voting systems.

III. PROPOSED METHODOLOGY

A. *I-voting:*

Since 2000, U.S. has been the first ever country used I-voting. Eventually, about 14 countries used I-voting application and out of 10 countries happy to carry on use in future. The most symbolic countries like Canada, Estonia, Switzerland and France. However, Estonia represents the leading country that uses I-voting system entirely.

I-voting can conduct in many ways like web platform, email, fax, and so on which refer to any remote based electronic transmission, that is, the origin of the naming “remote E-voting." Normally, Internet voting is the electronic voting transformation. nonetheless, in some cases, there are dangerous vulnerabilities alike virus infects voter PC and DDoS, spoofing, data tampering, and so on been distressed than electronic voting. For what internet voting does is merely resolved cost, complexity and accessibility problems. According to Dr. Teague, “The purpose of an election is not merely to select a winner, but to convince the loser, and their supporters, that they lost. Trust in the voting process is, therefore, an essential element to any voting system.” . Still there are some vulnerabilities of the network are well-known, and In some of the democracies continue the work of internet voting application. Nonetheless, the clarity of the voting means produces no change to electronic voting application, so there is no validation of information integrity.

We are proposing a system which has greater accessibility as it is a web application and possess greater security as authentication, authorization and verification.

Voting Process

•Admin will establish a voting instance by launching/deploying the structure in a blockchain network (EVM), then initiate an election instance and begin the election with the details of the election filled in (including applicants for people to vote).

•Then the possibly voters associate to the like blockchain network register to become a voter. Once the users successfully register, their various details are displayed/sent in the admins panel (i.e., verification page).

•Then admin will review if the registered information (Phone number, name and blockchain account address) is authentic and matches with his report. If it is, then the admin accepts the certified user by making them acceptable to take place and direct their individual vote in the election.

•The registered user i.e., voter followed by the approval from the admin direct their vote to the contender of interest (from the voting page).

•Later some time, based on the extent of the election the admin finishes the election. As that take place the voting is closed and the results are displayed announcing the winner at the top of the results

B. *Blockchain:*

Blockchain is a distributed, decentralized, public ledger. Blockchain is of three different types, i.e., public, private, and consortium blockchain. Ethereum and Bitcoin are examples of a public blockchain. This is demonstrated by the complicated mathematical functions. This analysis uses public blockchain i.e. Ethereum. It is basically a chain of blocks where a block is the primary component of the blockchain. A block is the header and the body, the block body involves the transactions that are being written to the network. The block header contains the block information which includes previous hash, nonce value and difficulty, block timestamp and transactions. [7] Each block also stores information about the person participating in the transaction. The block quantity is volatile, and is predicted 1 to 8 MB in capacity. The block first part notably says the block which should be insert.

1) Working of Blockchain

Blockchain is a structure that is created around peer-to-peer structure that can bemutually flagrantly by all of the consumers to generate record of undertaking that is immutable. In order to produce a block, an undertaking needs to

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 4, April 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1004096|

occur, after that the authority of undertaking needs to beverage. The undertaking will then be saved in a hash value and block must be given to the block for sealing. Thus, a block is created and sealed.

2) Why Blockchain technology?

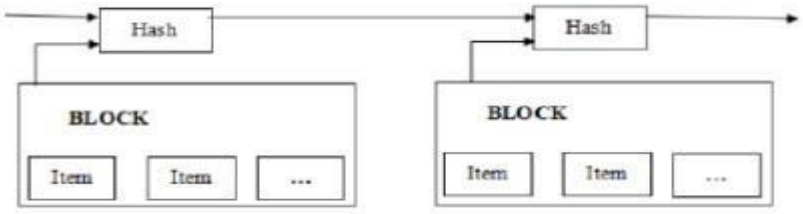

Figure 1: Blockchain

The mission of blockchain technologyis to redefine the "trust" of the system which eliminatesmiddlemen like governments and corporations, that is, the nextgenerations architecture – decentralization. With blockchaintechnology, the "trust" will be on the system or so-called smartcode instead of middlemen who in charge both data privacy andsecurity. Therefore, blockchain technology capabilities are what the I-voting system inevitably requires transparency, immutability, and so on.

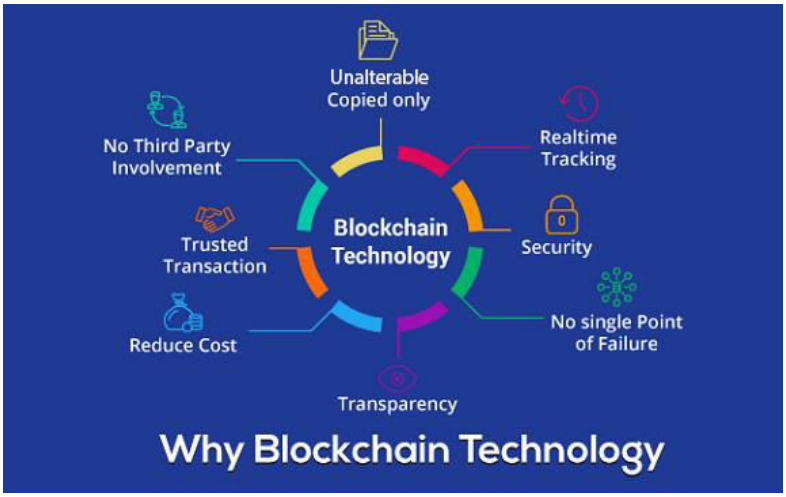

Figure 2: Why Blockchain Technology

C. *Ethereum:*

financial applications and Complex legal such as Smart contract can be created and deployed using Ethereum as an open platform to all. Ethereum can be fancied as a programmable Bitcoin in which the hidden layers of blockchain can be pre-owned by developers to create mutual ledgers, markets, digital associations and other endless potentiality involving immutable information and arrangement, all beyond the need for a mediator. Released in2015, Ethereum is the brainchild of prodigious VitalikButerinwho saw the possible applications of Bitcoins by Blockchain technologies as the next move in advance, the progress of the Blockchain civilization. Ethereum is now the cryptocurrency with the second-highest coin market cap and is projected to overtake Bitcoin as both a valued investment and as the most common cryptocurrency in the globe.

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 4, April 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1004096|

Figure 3: Ethereum

D. *Hashing:*

Hashing is the technique of balancing the variable input and arbitrary a size to a fixed output size. There are distinct services which perform different levels of hashing. We have implemented security by using SHA-256. SHA-256 is one of theSHA-1 also knows as SHA-2 heritor hash service and is one of the paramount hash functionsaccessible.SHA-256 is not enough more difficult to code than SHA-1 and not vulnerable yet. [3] The 256-bit key cause ADESA satisfying companion feature which is a symmetrical key encryption cipher, defined the same key is used for encryption and decryption. Unlike its other forebear, the algorithm's adaptability is that it grasps any input range and makes an arbitrary output range, at the same time all although algorithms generate set output length.

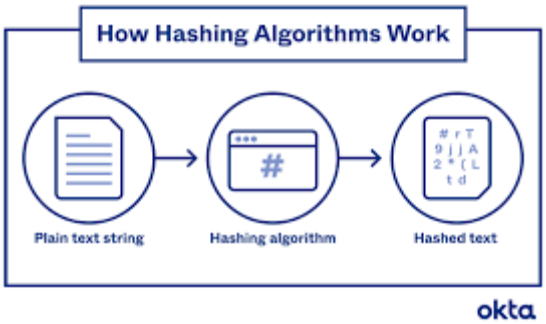

Figure 4: Hashing Working

IV. RESULTS & DISCUSSION

Moving forward with the former process of the project blockchain based online voting system below are the step-by-step figures to run the web application. We need to run Ethereum blockchain on local network using ganache-cli which is the latest version of test-rpc as shown in figure 5. Now admin will add the candidates for election as shown in figure 6. Once the admin has added candidates successfully, he can start the election by filling up required details as shown in figure 8. Once the election has been started by admin the voters can register themselves on the web application as shown figure 9. After successful registration by voter's admin will verify & approve them for voting as shown in figure 10. After verification by admin the voter can now vote for his or her chosen candidate as shown in figure 11. Once the election is ended by admin the voters can see the results as shown in figure 12. MetaMask is software cryptocurrency wallet used to interact with Ethereum blockchain as shown in figure 13. Each Transaction details can be shown on the MetaMask as shown in figure 14

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 4, April 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1004096|

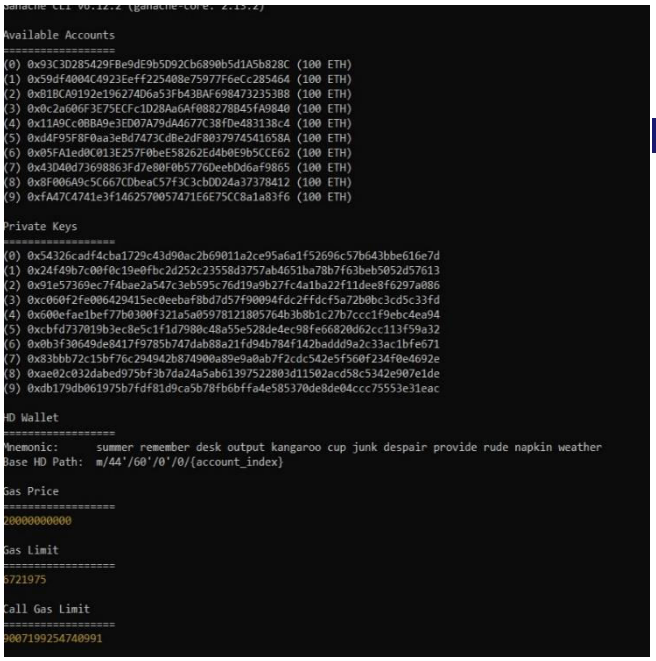

Figure 5: Ethereum Blockchain on local network

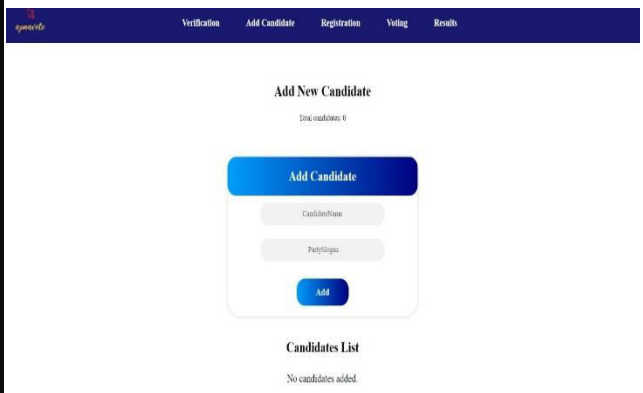

Figure 6: Add Candidate

FIGURE 7: CANDIDATE LIST

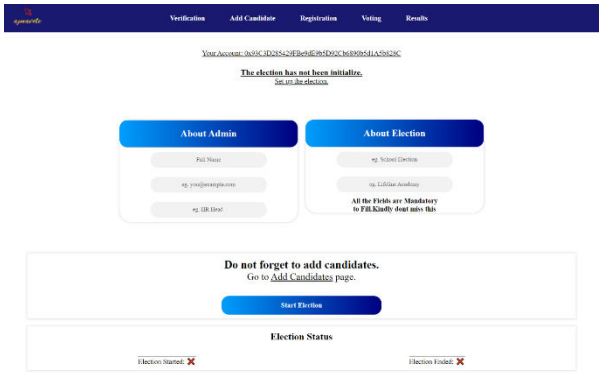

FIGURE 8: ADMIN PANEL

International Journal of Innovative Research in Computer and Communication Engineering

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 4, April 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1004096|

Figure 9: Registration Page

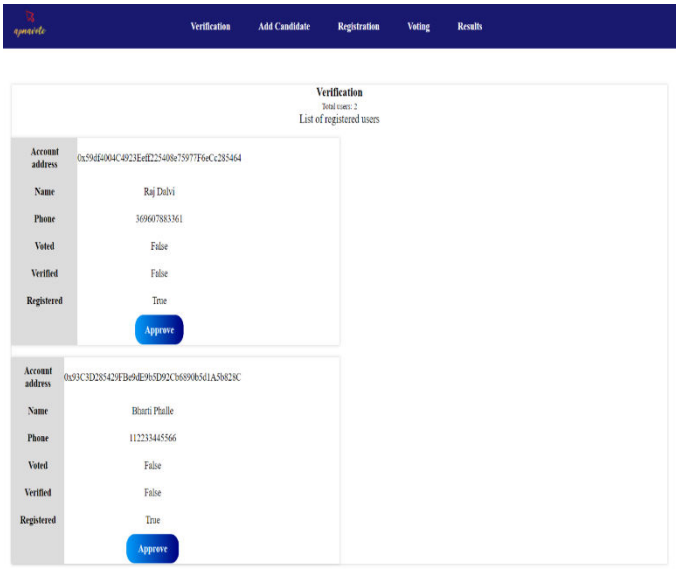

Figure 10: Verification Page

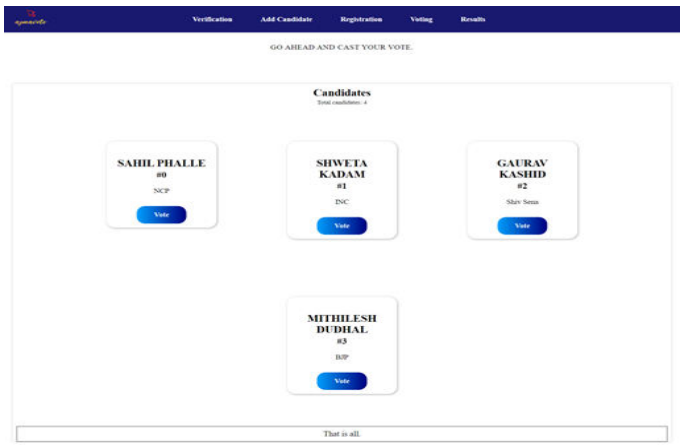

Figure 11:Voting Page

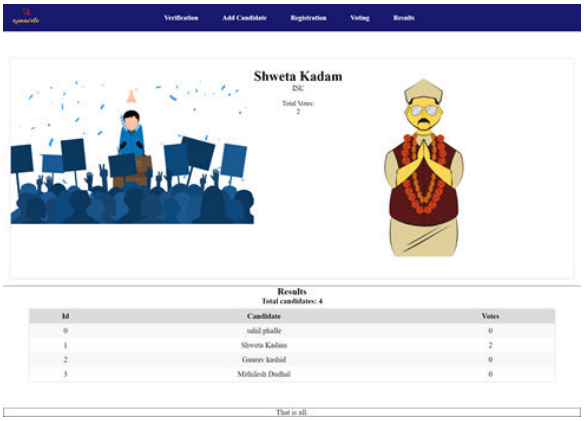

Figure 12: Result Page

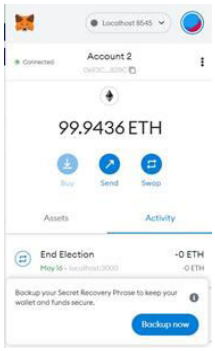

Figure 13: MetaMask Transaction

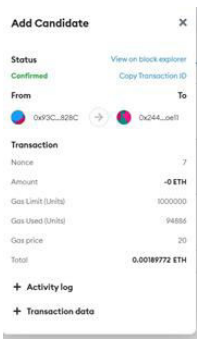

Figure 14: Transaction Details

| e-ISSN: 2320-9801, p-ISSN: 2320-9798| www.ijircce.com | |Impact Factor: 8.165 |

|| Volume 10, Issue 4, April 2022 ||

| DOI: 10.15680/IJIRCCE.2022.1004096|

V. CONCLUSION AND FUTURE WORK

To sufficiently develop an online voting system for the modern industry is not atrivial task, as the whole research is towards on the technical part. We have proposedto apply the blockchain technology to the online voting system. Unluckily in real-world,there is no such thing so-called best blockchain algorithm for all the complex problems. According to the blockchain research, the proposed solution is precisely the best fit andrecommended for the online voting system. All the blockchain algorithms whether areoptimized or trade-offs between the security and performance one, the primary aim istypically to establish the system extremely near to absolute safety. We have learnedfrom blockchain research that there may typically include potential weaknesses nomatter how to enforce the security of a system. The potential security threats may occurin the various scenario since the blockchain technology has different system architecture from the centralized one.

REFERENCES

[1] Online Voting System for India Based on AADHAR ID -Himanshu Agarwal, G. N. Pandeyin the year 2013
[2] S.Biometric voting system using aadhar card in India - SChakraborty, S Mukherjee in theyear 2016.
[3] AlGabriTrustworthy Electronic Voting Using Adjusted Blockchain Technology - Basit ShahzadRaju, Jon Crowcroft in the year 2019
[4] D. Security Analysis of India's Voting Machine - Hari K. Prasad, Arun Kankipati, SaiKrishnaSakhamuri in the year 2010.
[5] Security Analysis of the Estonian Internet Voting System - Drew Springall, TravisFinkenauer, Zakir Durumeric, Jason Kitcat, HarriHursti, Margaret MacAlpine, and J. Alex Halderman in the year 2014.
[6] Security Blockchain for Electronic Voting System – Review & Open Research Challenges- UzmaJafar ,MohdJuzaiddin Ab Aziz & Zarina Shukur in the year 2021.
[7] Electronic Voting Machine: Here's all you wanted to know about India's EVMs.
Retrieved 22 8, 2018, fromhttps://www.indiatoday.in/india/story/all-you-need-toknow-about-electronic-votingmachine-969155-2017-04-03. 2017
[8] What is Ethereum? — Ethereum Homestead 0.1documentation. Retrieved 22 8, 2018,From http://www.ethdocs.org/en/latest/introduction/what-isethereum.html.,2016.
[9] Wang, B.; Sun, J.; He, Y.; Pang, D.; Lu, N. Large-scale election based on blockchain.ProcediaComput. Sci. 2018, 129, 234–237. From
https://www.sciencedirect.com/science/article/pii/S1877050918302874?via%3DihubMuthukumar S,
[10] Shahzad, B.; Crowcroft, J. Trustworthy Electronic Voting Using Adjusted Blockchain Technology. IEEE Access 2019, 7, 24477–24488 from https://ieeexplore.ieee.org/document/8651451

INNO SPACE
SJIF Scientific Journal Impact Factor

Impact Factor: 8.165

doi cross ref

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INDIA

निस्केयर NISCAIR

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN COMPUTER & COMMUNICATION ENGINEERING

9940 572 462 6381 907 438 ijircce@gmail.com

www.ijircce.com

Scan to save the contact details