International Journal of Innovative Research in Computer Science & Technology (IJIRCST)
ISSN: 2347-5552, Volume-9, Issue-2, March 2021
https://doi.org/10.21276/ijircst.2021.9.2.14
Article ID IRP1139, Pages 98-103
www.ijircst.org

Decentralized Incognito Limpid E-Voting System

Dr. Yojna Arora[1], Mr. Vivek Birla[2], Mr. Rajat Gupta[3] and Mr. Samarth Tiku[4]

[1,2,3,4] Department of Computer Science, College of Computer Science and Engineering, Amity University, Haryana, India

Correspondence should be addressed to Dr. Yojna Arora; yojana183@gmail.com

ABSTRACT- Voting is a constitutional part of governmental systems which gives the people of the nation the liberty to express their opinions. The contemporary system constitutes Electronic Voting Machines (EVM) that is a pile-up of data natively and centralized, making it implausible. Since the data is amassed locally over the EVM(s) prior to the election's cessation, it could be hacked. Furthermore, there have been events of "polling booth hijacking" in some regions during the elections. Ethereum blockchain technology addresses concerns regarding integrity, security, and accessibility of current voting systems. Expanding e-voting into Ethereum based blockchain technology is one potential application of the emerging blockchain technology. This paper presents a decentralized, incognito, and limpid e-voting system named "DILE". It will escalate accessibility as the users could cast their votes without paying a visit to the polling booths. DILE makes practical and effective use of Ethereum's blockchain technology and smart contracts for its implementation.

KEYWORDS- DILE, Smart Contracts, Ethereum, Blockchain, E-Voting.

I. INTRODUCTION

E-voting systems are being adopted across the key public sectors as a replacement to the traditional ballot system through Ethereum blockchain technology. The idea in a Decentralized Incognito Limpid E-voting System (DILE) is simple. To use a cryptocurrency analogy, DILE issues each voter a "meta mask wallet" containing a user credential. All individuals get a single "token" granting the voters an opportunity to cast a vote. Ethereum blockchain technology clinches that no vote has been altered or removed, and no illegal votes have been added. Some countries have done an extensive research to use e-voting systems. Still, no reliable and efficient e-voting system can be incorporated on a larger scale and faces momentous security concerns towards the voting system's integrity. With the advances of blockchain technology, we have chosen to use Ethereum blockchain in e-voting due to its tendency to match the demands of ground breaking technologies that are immutable, decentralized, fast transactions, secured and reliable. Here comes the role of the Ethereum blockchain.

A. Ethereum: a Programmable Blockchain

Ethereum based blockchain is a community-driven technology that is a decentralized, open-source blockchain featuring smart contract functionality and powering thousands of decentralized applications. Ether, the cryptocurrency with a [1] market capitalization of $160,212,869,021 of the Ethereum Blockchain, which is the second-largest cryptocurrency, is the most actively used blockchain. Smart contracts are programs stored inside a specific address inside the Ethereum blockchain. Moreover, smart contract acts like contracts in the real world but are entirely digital, deployed to Ethereum network and run as programmed.

B. Merkle Tree

Merkle tree is also referred to as "binary hash trees." It is a data structure in which pair of nodes is hashed constantly until only one hash value remains, making data more secure and efficient. As illustrated in the Figure 1 , a Merkle Tree is created in a bottom-up approach that each transaction T, I, K, and U is hashed and is stored in each leaf node, inducing Hash T, I, K, and U. Continuously, these leaf nodes are summarized in parent node by hashing Hash T and Hash I, generating Hash TI, and separately hashing Hash K and Hash U, generating Hash KU. Hash TI and Hash KU are hashed again to produce the Merkle Root(Root Hash).

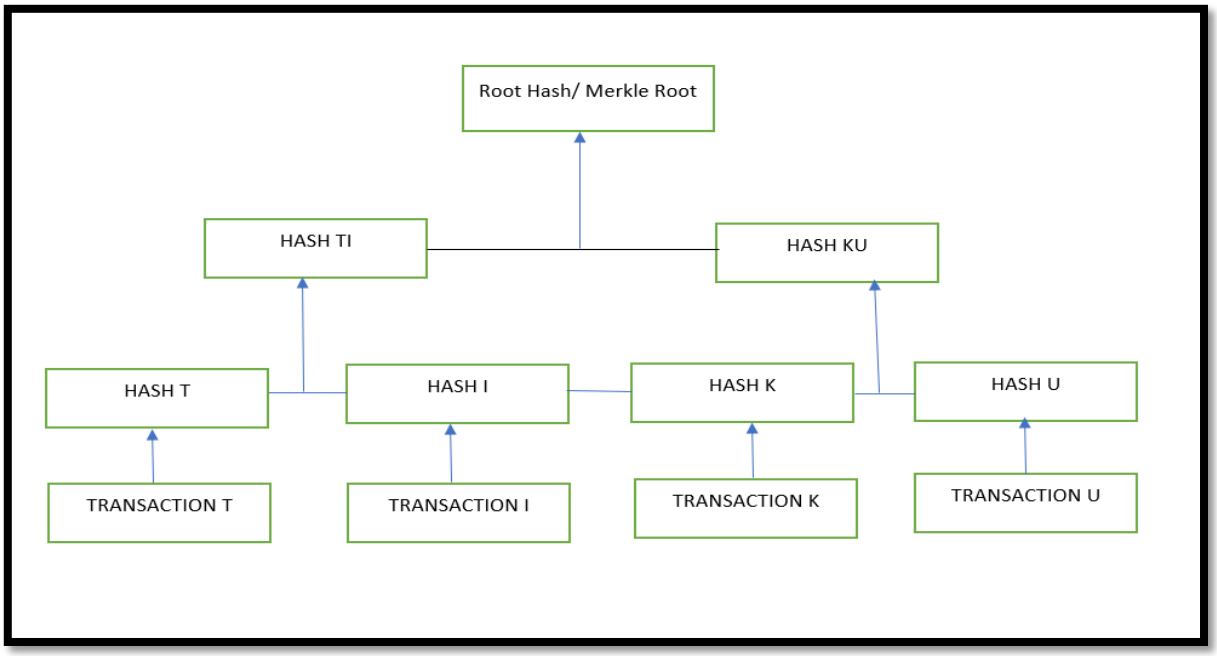

Fig.1: Merkle Tree

II. MOTIVATION AND RELATED WORK

Our primary motivation is to provide a Decentralized, incognito, and Limpid E-voting System(DILE) and show that a reliable e-voting system is attainable using the Ethereum blockchain. Extensive research has been done on implementing blockchain into e-voting schemes. Reference [2], highlights the pros and cons of using the blockchain technology from a practical point of view in developing , deploying and usage contexts , also addresses few properties like: Fairness , Eligibility, Privacy, Verifiability and Coercion-resistant. Reference [3] , highlights that Panja and Roy deployed the blockchain technology to the already existing DRE-ip evoting scheme, which guards verified and confirmed ballots from being modified before the tallying period of time and dispenses an alternative to secure public bulletin board . Reference [4] , highlights about Bronco Votes , an e-voting system which proposes to use a variety of holomorphic encryption modus operandi to facilitate voter's safety , requiring larger integer number than supported in Solidity , henceforth making its cryptography through a server inducing vulnerability in the e-voting system.

III. PROPOSED WORK

To make the whole process fair and user-oriented, we have deployed Ethereum smart contracts and stored all the necessary information on it , proposing A Decentralized Incognito Limpid E-voting System (DILE). Current e-Voting scheme incorporates EVM which are at risk to cyber attacks. DILE aims at providing a digital infrastructure where users can cost votes around the globe and casted votes cant be tampered with , provided that the Ethereum Blockchain provides immutability.

A. Preliminaries

a. Solidity

Solidity is statically-typed curly-braces based object-oriented high level programming language for implementing smart contracts on numerous blockchain platforms, notably Ethereum Blockchain

b. Ganache

Ganache is an emulator in accordance with Ethereum blockchain emulating a full Ethereum node natively on a system generating 10 dummy accounts with balance of 100 ether in respective accounts .[5] Moreover , features auto-mining only while recieving an incoming transaction.

c. MetaMask

MetaMask is a wallet that provides a secured connection to Ethereum Blockchain to connects to variety of [6]
This new world decentralized applications (Dapp) keeping users data and valuables safe and sound acting as a shield from hackers and data collectors. MetaMask seamlessly moves between sends money at a fraction of cost.

d. Truffle

Truffle is a framework to compile, test and deploy your smart contracts. [7]Truffle is a testing framework with built-in smart contract compilation , has a development environment along with configurable asset pipeline.

e. Nodejs and NPM

Node.js or Node is an open-source, cross-platform, server side JavaScript platform . NPM is a package manager for setting tools and libraries.

B. Architecture

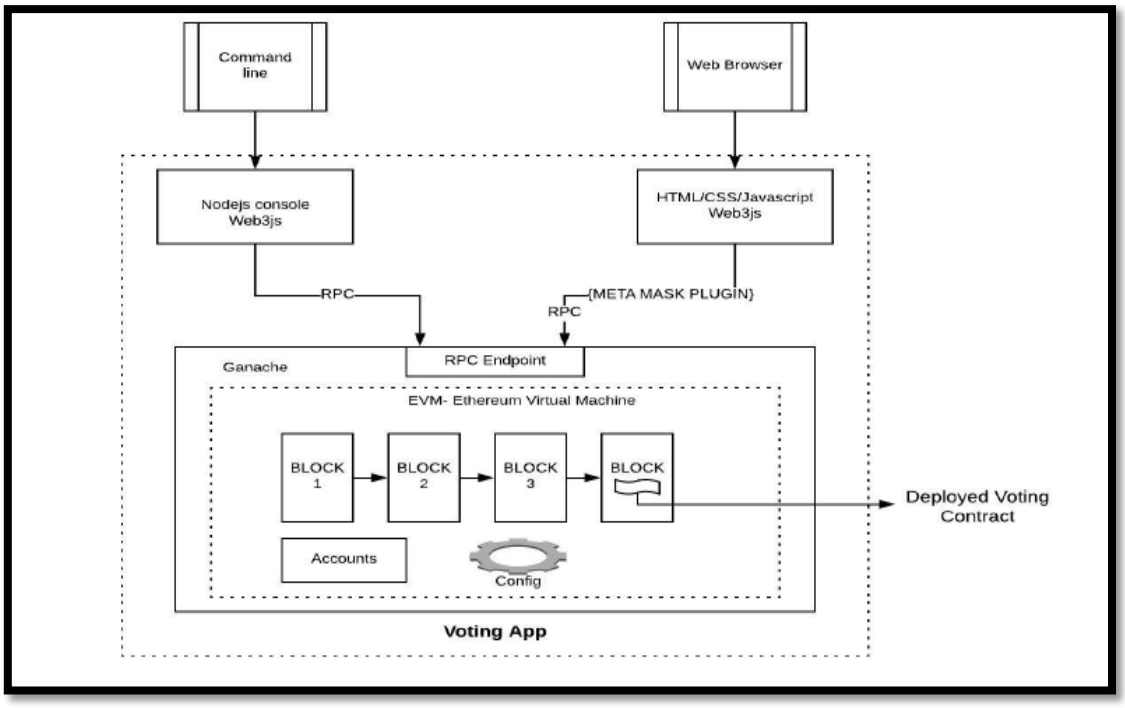

Fig. 2: System Architecture

The system architecture of the proposed system is as illustrated in Figure 2. The decentralized e-voting application would be accessible using the command-line interface or through the web browser. MetaMask Wallet is installed as a plugin in the Google Chrome browser. Users can interact with the e-voting application using a command-line interface in which users will be addressed with Nodejs console provided the commands are typed in it. The user can also interact with the user interface via CSS, Javascript, React, and HTML to deliver the commands.Web3.js is an assemblage of libraries authorizing the user to access a native or distant Ethereum node via WebSocket, HTTP, or IPC connection.Web3.js delivers the commands using RPC(s) and are detected at the RPC Endpoint of Ganache which the Ethereum Virtual Machine forwards. The smart contracts will be deployed over the Ethereum blockchain on Kovan Test Network. The config file directs the copious configuration criterion of the Ethereum Blockchain.

VI. IMPLEMENTATION

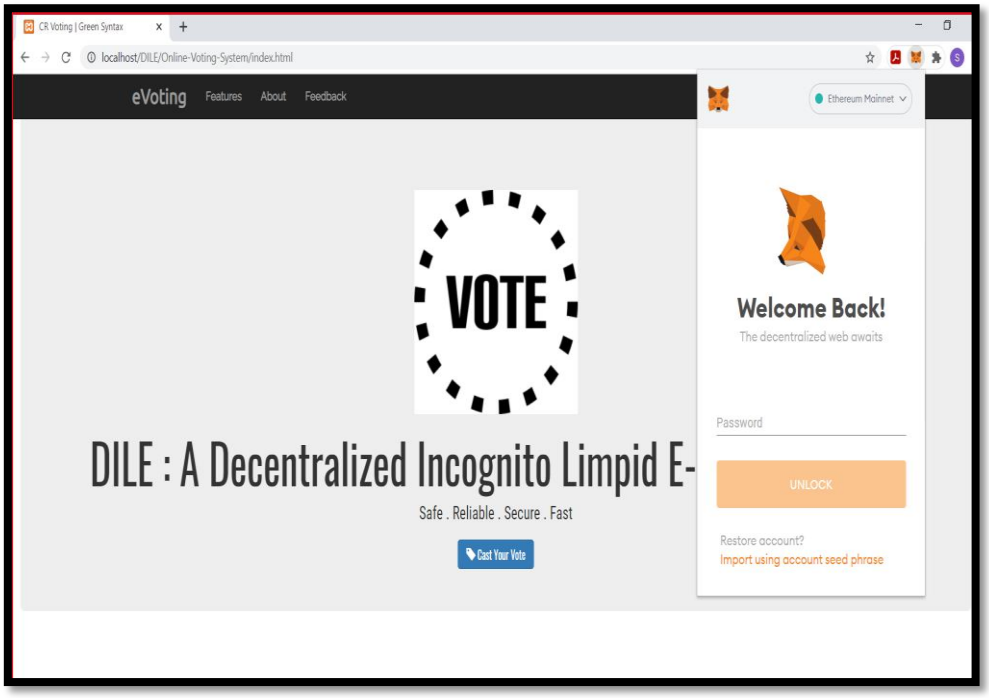

Fig. 3: Loading Page of DILE

As illustrated in Figure 3, the user is redirected to the home page of DILE: A Decentralized Incognito Limpid E-voting System. The user needs to create an Ethereum address and log in via Metamask on the Kovan test network of Ethereum Blockchain, a prerequisite for e-voting.

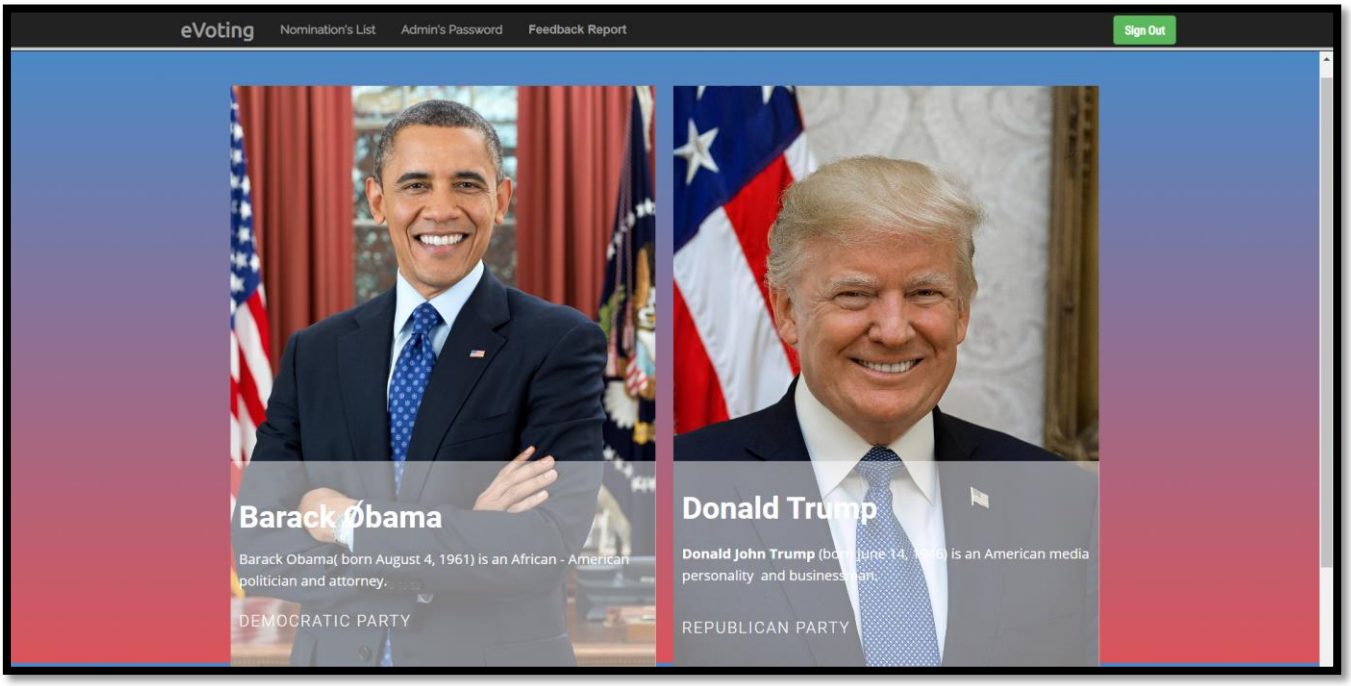

Fig. 4: Nominated Candidates

As illustrated in Figure 4, two nominated candidates are presebted on the website. Users can read the prosopography of both the nominated candidates and vote accordingly to their own choices.

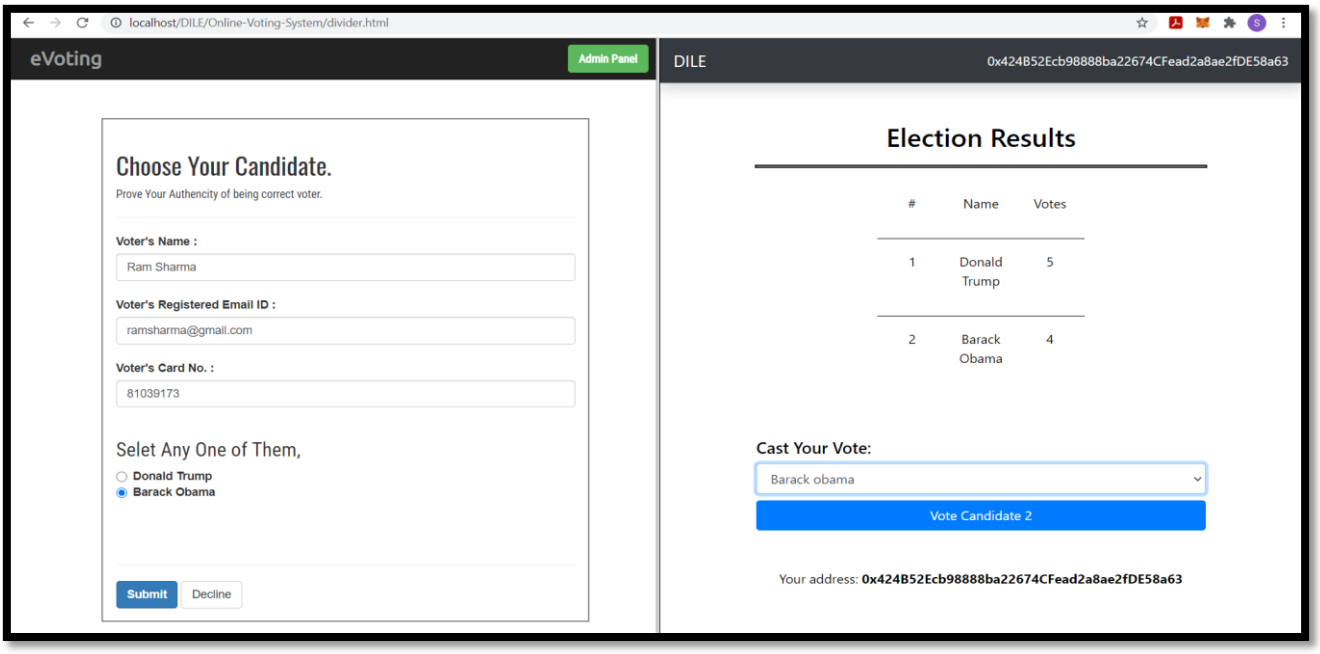

Fig. 5: Casting of Votes Using Ethereum Blockchain

As illustrated in Figure 5, Users need to be connected to their respective accounts via their Ethereum address through the MetaMask Wallet, provided the user has also registered their Name, Aadhaar id, and e-mail address on the website in order for the users to be eligible for voting. After casting their votes, users can also see live results updated. Once a Vote has been cast, it cannot be cast again by the same person.

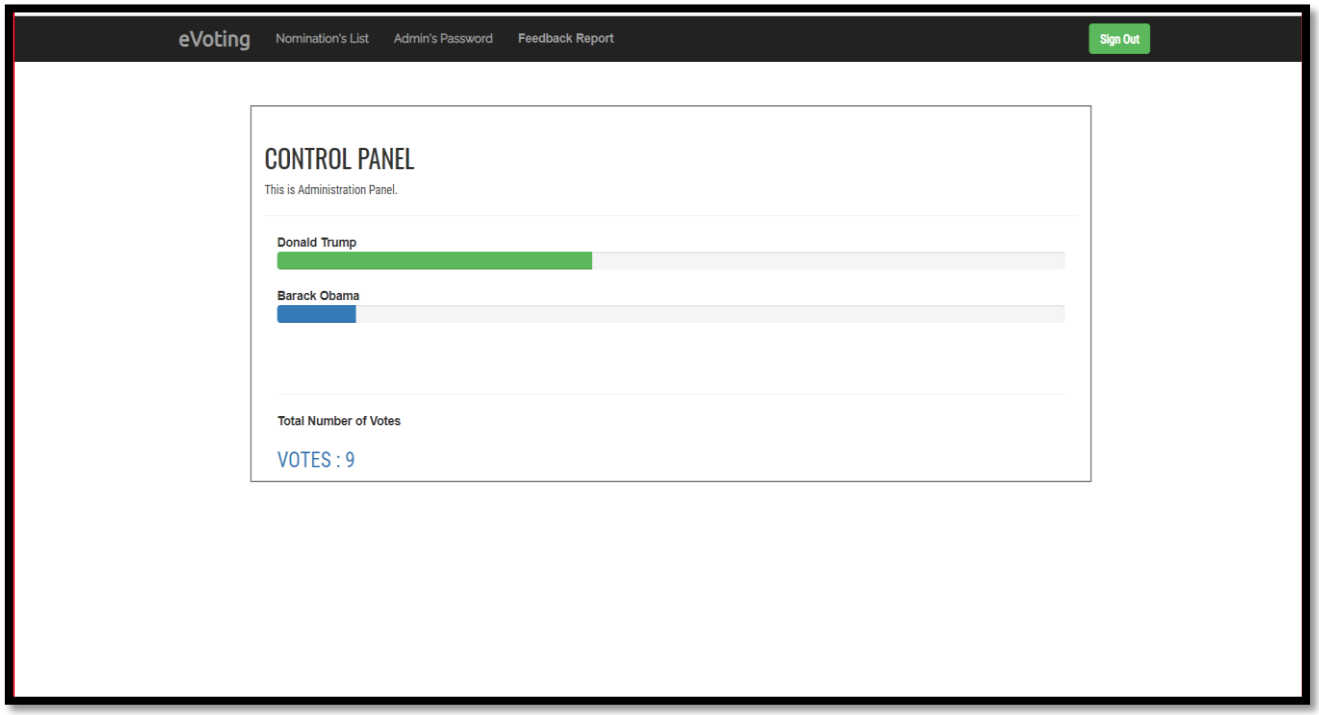

Fig. 6: Admin Control showing graphical representation for Casted Votes

As illustrated in Figure 6, Admin control shows the users graphical representation of votes cast. A total number of votes cast will also be displayed in the admin control.

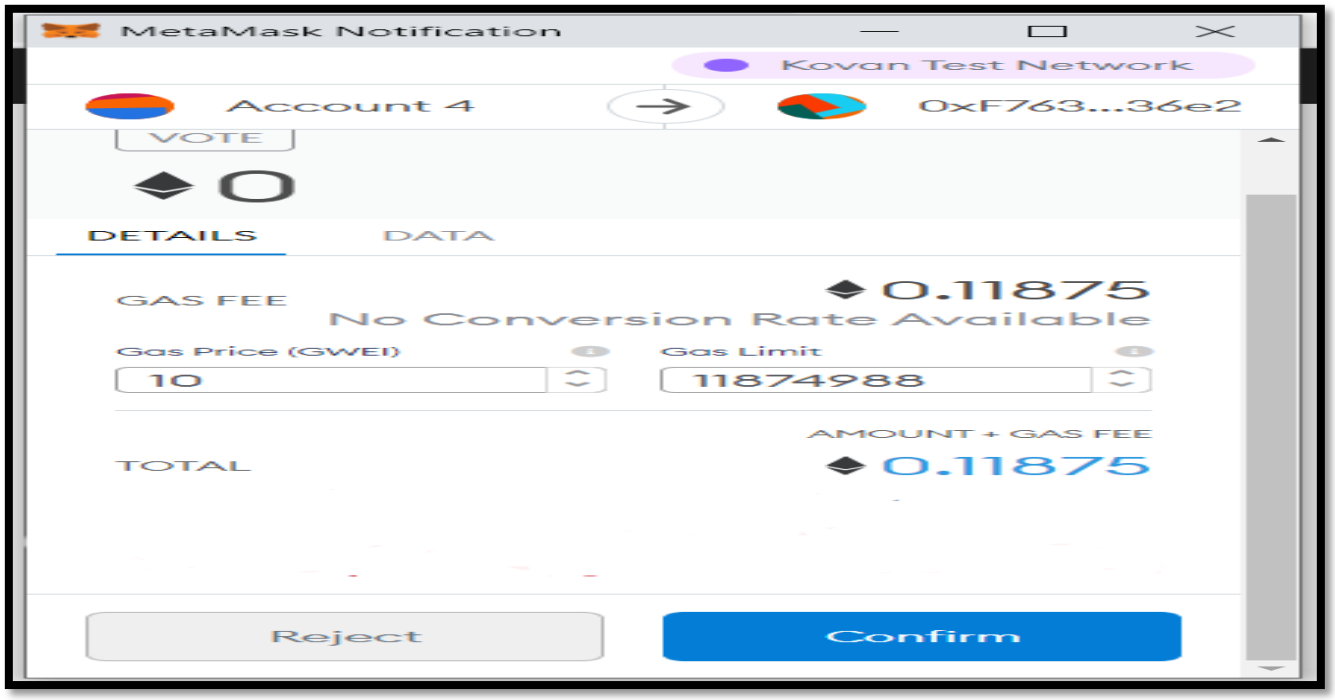

Fig. 7: Performing Transaction using Meta Mask for the confirmation of votes

As illustrated in Figure 7, in order for a vote to be cast, users need to pay ether and gas fees so that a transaction can be confirmed on the Kovan test network of the Ethereum blockchain.

VII. CONCLUSION

A Decentralized Incognito Limpid E-voting System (DILE)is proposed and realized in this work. This project saves a lot of time in counting the vote and declaring the results. We store the data on Ethereum blockchain so as to make the whole election process transparent , anonymous and secured. Account Address are anonymous but can

perform transactions on Ethereum blockchain , allowing voting process to be completed. We can conclude that our evoting system which is deployed on kovan test network can be easily deployed and setup to use an evoting system for a small scale globally or other similar settings.

REFERENCES

[1] Ethereum Market Capitalization Available at: https://coinmarketcap.com/currencies/ethereum/ last accessed, 26 February 2021

[2] Freya Sheer Hardwick, Apostolos Gioulis, Raja Naeem Akram, and Konstantinos Markantonakis, "E-Voting with Blockchain: An E-Voting Protocol with Decentralisation and Voter Privacy", ISG-SCC, 2018

[3] S. Panja and B. K. Roy, "A secure end-to-end verifiable e-voting system using zero knowledge based blockchain." IACR Cryptology e-Print Archive, vol. 2018, p. 466, 2018.

[4] Gaby G. Dagher , Praneeth Babu Marella , Matea Milinkovic and Jordan Mohler, "Bronco Vote: Secure Voting System using Ethereum's Blockchain", In Proceedings of the 4th International Conference on Information Systems Security and Privacy (ICISSP 2018), pages 96-107, 201.

[5] Ahmed Ben Ayed, "A Conceptual Secure Blockchain- based Electronic Voting System", International Journal of Network Security & Its Applications (IJNSA) Vol.9, No.3, May 2017.

[6] Friðrik Þ. Hjálmarsson, Gunnlaugur K. Hreiðarsson, "Blockchain-Based E-Voting System", School of Computer Science Reykjavik University, Iceland, January 2018.

[7] Kashif Mehboob Khan , Junaid Arshad and Muhammad Mubashir Khan "Investigating performance constraints for blockchain based secure e-voting system", Future Generations of computer System Vol .105 , April 2020.

ABOUT THE AUTHORS

Dr. Yojna Arora ,PhD (Computer Science & Engineering) , M.Tech (Computer Science & Engineering) , B.Tech (Information Technology). Assistant Professor Computer Science & Engineering Faculty of Science Engineering And Technology Amity University Haryana, Amity Education valley, , Pachgaon,Manesar, Gurgaon, Haryana 122413

Vivek Birla, Assistant Professor -II Overall Coordinator - B.Tech + MBA Program Chairman - ASET / AIIT - Alumni Cell Ph.D (p), MBA, B.Tech – ECE Amity University - Gurgaon email : vbirla@ggn.amity.edu, www.amity.edu/gurgaon *ASET - Amity School of Engineering and Technology & AIIT - Amity Institute of Information and Technology.

Rajat Gupta, Bachelor of Technology in Computer Science And Engineering Amity Education Valley Gurugram, Manesar, Panchgaon, Haryana 122413

Samarth Tiku, Bachelor of Technology in Computer Science And Engineering Amity Education Valley Gurugram,Manesar, Panchgaon, Haryana 122413