Title: B-Voting System
Name: Amol More
Roll No: N20111021
Subject: Degree Project 1

Problem Statement

- In the current system, voting is done by using EVM (Electronic Voting Machine).
- This system can be replaced by the online voting (E-voting) system which will limit the voting frauds.
- Expanding e-voting into Blockchain technology could be the solution to alleviate the present concerns in e-voting.
- With this view in mind, we are going to develop Online Voting system using Blockchain.
- This E-voting system has the potential to make the voting process easier and more accessible for electors.

Overview

Voting whether conducted through the traditional ballot or via electronic means forms the basis on which democracy depends. With the rise in technological impact on the youth of the country and the various anomalies faced by the current electoral process, using technology to modify the existing process is necessity of the time. However, for any new technique to take the place of current voting system, the said system needs to satisfy certain minimum criteria. Electronic Voting has taken Centre place in research with the intention of minimizing the cost associated in setting up the voting process, while ensuring the electoral integrity is maintained by fulfilling privacy, security and compliance requirements.

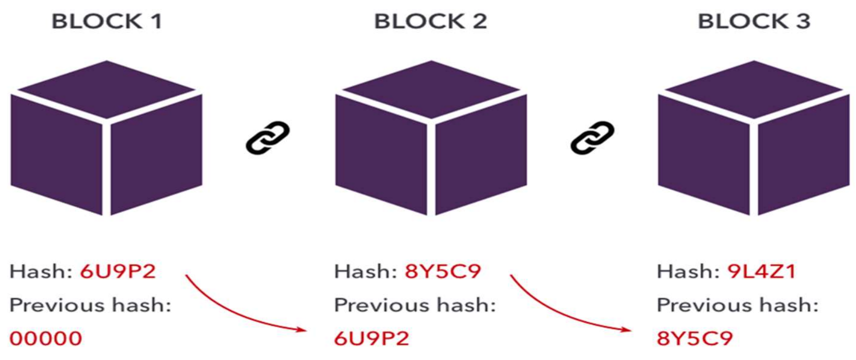
The current method, whether electronic or not has proved to be unsatisfactory with respect to transparency. It can be very difficult for the voters to be assured that the vote he/she has casted during the election reflects in the election result. Electronic voting using Direct Recording Electronic do not generate receipt on successful casting of votes. No record of election except vote count is made public by the government, which means that the voters are not assured of any external interference in case of government conducting the process of vote recounting. Replacing the traditional method with electronic method using Blockchain technique has the ability to prevent potential frauds that may take place during election.

What is Blockchain??

- A blockchain is a digital ledger of transactions that is duplicated and distributed across the entire network of computer systems on the blockchain. It is a system of recording information in a way that makes it difficult or impossible to change, hack, or cheat the system.
- The Blockchain Structure is also known as an append-only data structure, such that new blocks of data can be written to it, but cannot be altered or deleted. Private blockchain limits the read and write access, only specific participants can verify their transactions internally. That makes the transaction on a private network cheaper, since they only need to be verified by a few nodes that are trusted and with guaranteed high processing power.
- Nodes are very well-connected and faults can quickly be fixed by manual intervention, allowing the use of consensus algorithms which offer finality after much shorter block times.
- Blockchain consists of a very important concept called blocks.

Blocks

- Every chain consists of multiple blocks and each block has three basic elements
- Data (i.e., transactions), the hash of the previous block and the block hash value. Hash value is a unique value, identifying one block. It depends on the block's content (data and previous block hash), so each block has its unique hash value, and it's identifying this block only.
- Therefore, each block can reference or point to the block before, which means the four block is taking a reference to the third one is taking a reference to the second, and so on and thus a chain of block is formed which we call as blockchain.



- The key element that makes blockchain immutable is cryptographic hashes, which is why blockchain is immutable.

Cryptography + Blockchain Hashing Process = Immutability

Transaction

- The data stored in blockchain in the form of transactions. A blockchain transaction is a transfer of crypto money. A transaction is a new record of exchange of some value or data between two public addresses of the blockchain
- One can think of a transaction as being a record that describes one account attempting to send money to another account. A transaction is created any time two accounts exchange some amount of money

nonce	How many times the a transaction
to	Address of account this money is going to
value	Amount of ether (crypto) to send to the target address
gasPrice	Amount of ether the sender us willing to pay per unit gas to get this transaction processed.
startGas/gasLimit	Units of gas that transaction can consume
v	Cryptography pieces of data that can be used to generate the senders account address. Generated from the sender's private key.
r	
s	

Key features of Blockchain:

- High Availability
- Verifiability
- Transparency
- Immutability
- Distributed Ledgers
- Decentralised

Tools and Technologies used in project:

- Solidity
- Metamask
- Ganache
- Truffle

Ethereum

- For developing E-voting using Blockchain we used Ethereum - a popular platform for creating distributed Blockchain applications that support smart contracts. Ether (ETH) is the native cryptocurrency of the platform.
- Ethereum is a decentralized, open-source blockchain with smart contract functionality. Ether is the native cryptocurrency of the platform.

Smart Contracts:

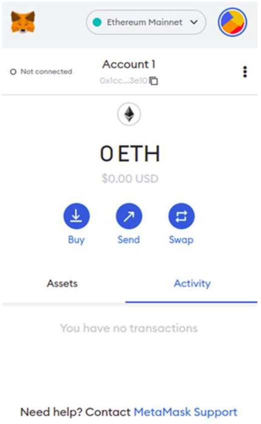
- Smart contracts are self-executing contracts which contain the terms and conditions of agreement between peers.
- They are simply programs stored on a blockchain that run when predetermined conditions are met.
- They typically are used to automate the execution of an agreement so that all participants can be immediately certain of the outcome, without any intermediary's involvement or time loss.
- Smart contracts eradicate the need for a third-party intermediary of facilitator, essentially giving you full control of the agreement.

Solidity

- Solidity is a contract-oriented, high-level programming language for implementing smart contracts. Solidity is highly influenced by C++, Python and JavaScript and has been designed to target the Ethereum Virtual Machine (EVM).
- It is statically typed, supports inheritance, libraries and complex user-defined types among other features.

Metamask

- For performing any transaction on the blockchain we require an account which will have unique account address. This can be created by using the Metamask chrome extension.
- Metamask is a crypto wallet & gateway to blockchain apps. It generates passwords (in the form of mnemonic) and keys on your device, so only you have access to your accounts and data. It helps users in interacting with the blockchain network.



○ Not connected

Account 1

0x1cc...3e10

0 ETH

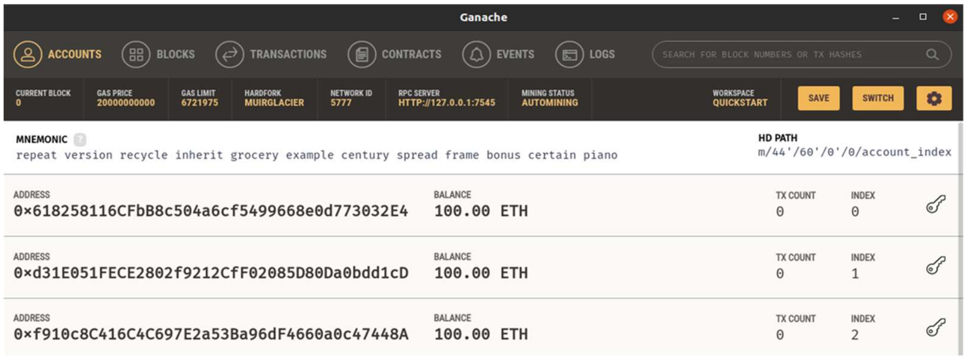
$0.00 USD

You have no transactions

Need help? Contact MetaMask Support

Ganache

- Since working with the main Ethereum network costs actual money for transactions, we are using a local RPC "Ganache".
- Ganache is a local test network for rapid Ethereum and distributed application development.
- It can be used across the entire development cycle; enabling us to develop, deploy, and test our dApps in a safe and deterministic environment.
- It provides us 10 accounts each having 100 Ethers (ETH) for testing purpose.



CURRENT BLOCK 0
GAS PRICE 20000000000
GAS LIMIT 6721975
HARDFORK MUIRGLACIER
NETWORK ID 5777
RPC SERVER HTTP://127.0.0.1:7545
MINING STATUS AUTOMINING
WORKSPACE QUICKSTART

MNEMONIC
repeat version recycle inherit grocery example century spread frame bonus certain piano

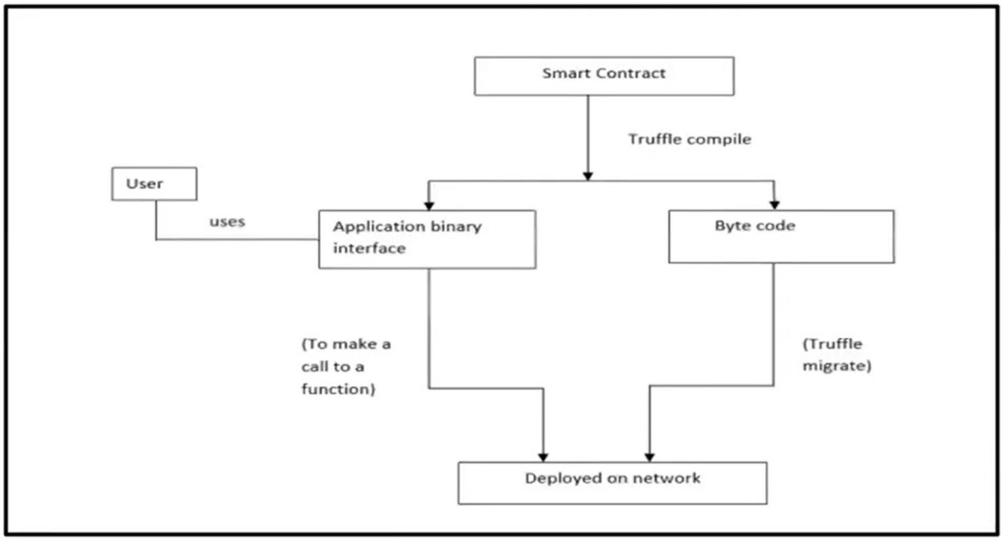
HD PATH
m/44'/60'/0'/0/account_index

ADDRESS	BALANCE	TX COUNT	INDEX
0×618258116CFbB8c504a6cf5499668e0d773032E4	100.00 ETH	0	0
0×d31E051FECE2802f9212CfF02085D80Da0bdd1cD	100.00 ETH	0	1
0×f910c8C416C4C697E2a53Ba96dF4660a0c47448A	100.00 ETH	0	2

Truffle

- To interact with our compiled smart contract in a hassle-free manner we use Truffle suite.
- Truffle is the most popular development framework for Ethereum which makes lots of work easier.
- This generates an artifact which plays an important role in the successful deployment of our application.
- It takes care of managing our contract artifacts so we don't have to include support for custom deployments, library linking etc.

Blockchain Dataflow



Scope:

Enhanced Security:

The scope of the system is very vast as it can be implemented in any organization where elections play a major role in electing their representatives. The system can be adapted as per the need and the number of participants using the system. The techniques and concepts used in providing a base to the system uses strong encryption techniques to provide privacy to the votes and tamper free results.

Possible Upgrades:

- We can add Feature of Automatic Voter Verification instead of Manual Verification which is done by Admin.
- We can add fingerprint authentication mechanism to avoid the requirement to remember Metamask Account Address.

References:

https://core.ac.uk/download/pdf/155779036.pdf

https://www.economist.com/sites/default/files/plymouth.pdf

https://www.mdpi.com/1424-8220/21/17/5874/pdf