Decentralized E Voting System Using Blockchain

by

Abhay Chaurasiya

Roll. No.: 2018IMT-005

Under the Supervision of

Dr.Anuraj Singh

ABV–INDIAN INSTITUTE OF INFORMATION TECHNOLOGY AND MANAGEMENT GWALIOR (M.P.), INDIA

Motivation

- Transparency, decentralization, irreversibility, nonrepudiation, Of blockchain Technology. .
- The architecture provides a secure voting process without redundancy of existing (not based on blockchain) systems. .
- In previous research because of the transparency property from blockchain, ballots are visible when they are cast to the blockchain network. This exposes the progress of the election during the voting phase, and may greatly influence the outcome of the election. .
- To solve this problem I use permission blockchain.
- Permissioned blockchains can be seen as an additional blockchain security system, as they maintain an access control layer to allow certain actions to be performed only by certain identifiable participants.

Key related research

- Current voting system suffer from various attack.
  - DDos attack.
  - Polling Both Capturing
  - Vote alteration and manipulation
  - Malware attacks
- Blockchain can help to implement a electronic voting system that is immutable transparent and cannot be hacked into in order to change the result.
- Control the access of blockchain, by simply employing a permissioned blockchain for the election.

Review of key related research

- I have proposed to plan the current web based democratic framework which is coordinated with the Blockchain innovation. The proposed framework enjoys the accompanying benefits when contrasted with the current framework:
- Here I used a permission blockchain which does not allow ballots to be visible during vote cast.
    - Clients' can cast a ballot from anyplace on the planet until they have a citizenship of the country.
    - The democratic is put away in the Blockchain which makes it sealed.
    - As there's no remaining in line for making choice it will save a great deal of time and lessen the responsibility

cont...

- Design a synchronized model of voting records based on distributed ledger technology(DLT) to avoid forgery of voters.
- Design a user credential model based on elliptic curve cryptography(ECC) to provide authentication and non-repudiation.
- The disruption idea is the use of two linked side chain, one way pegged side chain.

cont...

- The disruption idea is the use of two linked side chain, one way pegged side chain.
- The first side chain record the voting operation of voters.
- The second side chain counts the voters assigned to the various candidates.
- By integrating the above designs, we propose a Blockchain-Based e-voting scheme, which meets the essential requirements of E-Voting process.

Objectives

- To use the permission blockchain so that ballots are not visible during vote cast.
- To reduce the workload of setting up an election booth and conducting elections in physical form. .
- Non-Resident Indian can cast their votes as it is totally online.
- I am supposed to learn the concept of Blockchain and how it can be utilized to work on different sectors.

Methodology/System Design

- Ethereum: It is platform to developed distributed blockchain application that support smart contracts and I use this to develop E- Voting system.
- Smart Contract: It is self executing contract which run when predetermined conditions are met.
- Solidity: It is contract-oriented, high level language For implementing the smart contracts.
- Meta mask: It is crypto wallet and gateway to blockchain apps. It generates password and key on your device , So only you have access to your accounts and data. It help user to interacting with the blockchain network.

cont...

- Ganache: Ganache is local test network for rapid Ethereum and distributed application development and can be used across the entire development. Enabling us to test, deploy and develops dapps in a safe and deterministic environment. .
- Truffle: It is a development framework for Ethereum this provide us to compiled smart contracts. This generates an artifacts which play an important role in the successful deployment of application.

Implementation Details

- Validate the voter identity.
  - Submit identity information which gets verified by the organisation.
  - Organisation can refer to the database of the registered voters and verify the person is registered on their database and is eligible to vote.
  - All the information will be securely added on to the voter blockchain.
- After the identity is verified.
- A smart contract will be executed that will issue a valid so that he can vote and submit it to the ballot box.

cont...

- Blockchain based voting system ensure that a user does not vote multiple times.
- After voting the vote becomes a transaction and gets stored in the blockchain after encryption.
- Once the vote is casted, it cannot be modified because of the immutable characteristics of blockchain.
- The voter will be even provided with the option to print the receipt as a proof of casting the vote.
- Through blockchain, the voter will be able to verify that his vote has been casted and counted.

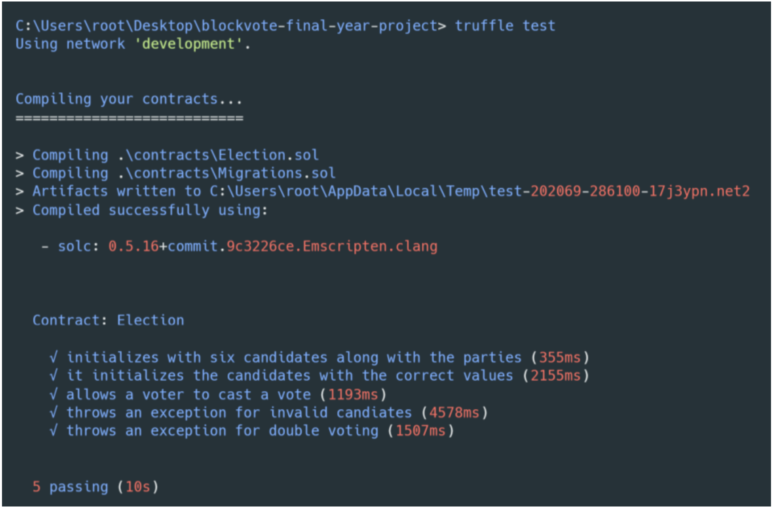
cont...

- The voter can even audit each ballot box and confirm if the election results are accurate by retaining the privacy of other voters.
- The election result can be declared immediately after the voting is over without any chances of human error.
- Blockchain technology will provide the required flexibility to a voter to login.
- This would encourage more and more people to vote and become a part of the democratic world.

Result and Testing

- Steps for Unit Testing are:-
  - Creation of a Test Plan
  - Creation of Test Cases and the Test Data
  - Creation of scripts to run the test cases wherever applicable
  - Execution of the test cases, once the code is ready
  - Fixing of the bugs if present and re-testing of the code
  - Repetition of the test cycle until the Unit is free from all types of bugs.

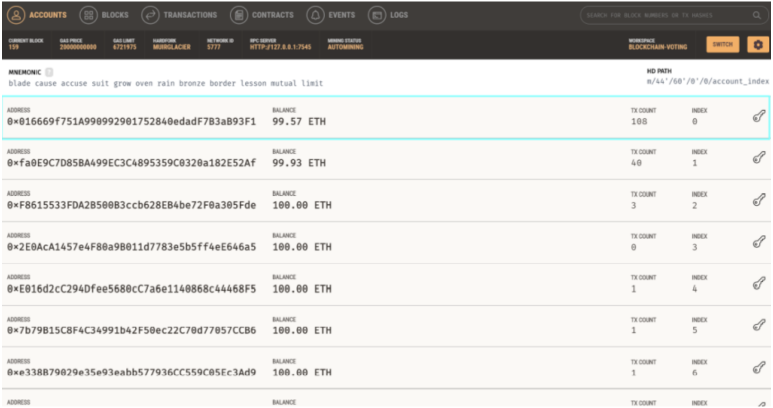
cont...



```
C:\Users\root\Desktop\blockvote-final-year-project> truffle test
Using network 'development'.


Compiling your contracts...
===========================

> Compiling .\contracts\Election.sol
> Compiling .\contracts\Migrations.sol
> Artifacts written to C:\Users\root\AppData\Local\Temp\test-202069-286100-17j3ypn.net2
> Compiled successfully using:

   - solc: 0.5.16+commit.9c3226ce.Emscripten.clang



  Contract: Election

    √ initializes with six candidates along with the parties (355ms)
    √ it initializes the candidates with the correct values (2155ms)
    √ allows a voter to cast a vote (1193ms)
    √ throws an exception for invalid candiates (4578ms)
    √ throws an exception for double voting (1507ms)


  5 passing (10s)
```

Figure: Test Report

cont...



CURRENT BLOCK	GAS PRICE	GAS LIMIT	HARDFORK	NETWORK ID	RPC SERVER	MINING STATUS	WORKSPACE
159	20000000000	6721975	MUIRGLACIER	5777	HTTP://127.0.0.1:7545	AUTOMINING	BLOCKCHAIN-VOTING

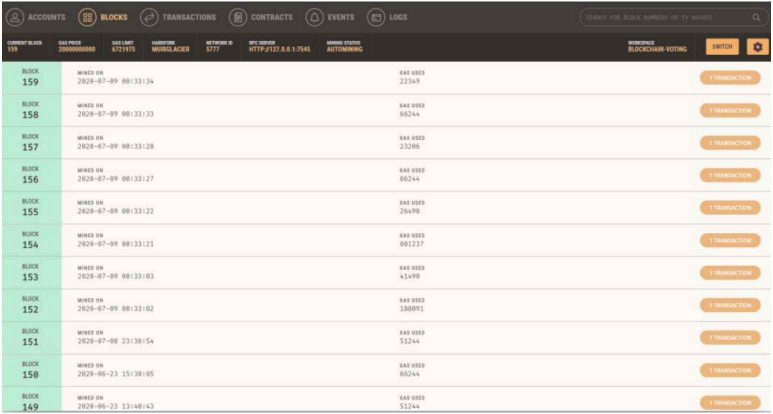
MNEMONIC
blade cause accuse suit grow oven rain bronze border lesson mutual limit

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

ADDRESS	BALANCE	TX COUNT	INDEX
0×016669f751A990992901752840edadF7B3aB93F1	99.57 ETH	108	0
0×fa0E9C7D85BA499EC3C4895359C0320a182E52Af	99.93 ETH	40	1
0×F8615533FDA2B500B3ccb628EB4be72F0a305Fde	100.00 ETH	3	2
0×2E0AcA1457e4F80a9B011d7783e5b5ff4eE646a5	100.00 ETH	0	3
0×E016d2cC294Dfee5680cC7a6e1140868c44468F5	100.00 ETH	1	4
0×7b79B15C8F4C34991b42F50ec22C70d77057CCB6	100.00 ETH	1	5
0×e338B79029e35e93eabb577936CC559C05Ec3Ad9	100.00 ETH	1	6

Figure: Smart Contract Owner Account

cont...

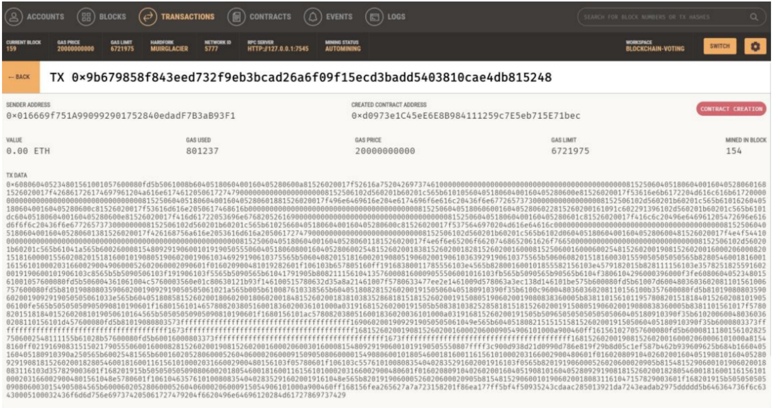


CURRENT BLOCK	GAS PRICE	GAS LIMIT	HARDFORK	NETWORK ID	RPC SERVER	MINING STATUS	WORKSPACE
159	20000000000	6721975	MUIRGLACIER	5777	HTTP://127.0.0.1:7545	AUTOMINING	BLOCKCHAIN-VOTING

BLOCK	MINED ON	GAS USED	
159	2020-07-09 00:33:34	22349	1 TRANSACTION
158	2020-07-09 00:33:33	66244	1 TRANSACTION
157	2020-07-09 00:33:28	23206	1 TRANSACTION
156	2020-07-09 00:33:27	66244	1 TRANSACTION
155	2020-07-09 00:33:22	26490	1 TRANSACTION
154	2020-07-09 00:33:21	801237	1 TRANSACTION
153	2020-07-09 00:33:03	41490	1 TRANSACTION
152	2020-07-09 00:33:02	188091	1 TRANSACTION
151	2020-07-08 23:36:54	51244	1 TRANSACTION
150	2020-06-23 15:30:05	66244	1 TRANSACTION
149	2020-06-23 13:40:43	51244	1 TRANSACTION

Figure: Block Mined after transaction

cont...



CURRENT BLOCK 159 | GAS PRICE 20000000000 | GAS LIMIT 6721975 | HARDFORK MUIRGLACIER | NETWORK ID 5777 | RPC SERVER HTTP://127.0.0.1:7545 | MINING STATUS AUTOMINING | WORKSPACE BLOCKCHAIN-VOTING

TX 0×9b679858f843eed732f9eb3bcad26a6f09f15ecd3badd5403810cae4db815248

SENDER ADDRESS
0×016669f751A990992901752840edadF7B3aB93F1

CREATED CONTRACT ADDRESS
0×d0973e1C45eE6E8B984111259c7E5eb715E71bec

VALUE
0.00 ETH

GAS USED
801237

GAS PRICE
20000000000

GAS LIMIT
6721975

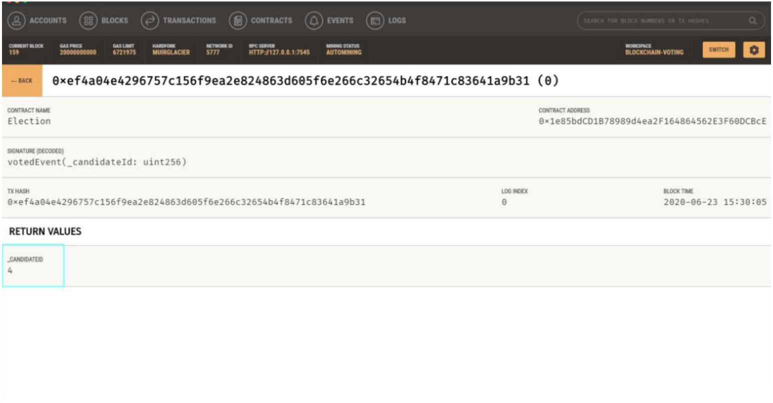
MINED IN BLOCK
154

TX DATA

```
0×608060405234801561001057600080fd5b5061008b6040518060400160405280600a81526020017f52616a7520426973746100000000000000000000000000000000000000000000000000000000008152506040518060400160405280601 68
1526020017f426861726174697961204a616e61746120506172747900000000000000000000000000008152506102d560201b60201c565b6101056040518060400160405280600e81526020017f53616e6b6172204d616c616b61720000
000000000000000000000000000000008152506040518060400160405280601881526020017f496e6469616e204e6174696f6e616c20436f6e677265737300000000000000008152506102d560201b60201c565b61016260405
18060400160405280600c81526020017f53616d616e2050617468616b000000000000000000000000000000000000000000815250604051806060016040528060228152602001610 91c602291396102d560201b60201c565b6101
dc6040518060400160405280600e81526020017f416d61722053696e67682052616900000000000000000000000000000000000081525060405180604001604052806 01c81526020017f416c6c20496e646961205472696e616
d6f6f6c20436f6e677265737300000000008152506102d560201b60201c565b6102566040518060400160405280600c81526020017f5375646970204d616e64616c0000000000000000000000000000000000000000000000008152506040
5180604001604052806013815260200 17f426168756a616e2053616d616a205061727479000000000000000000000000000008152506102d560201b60201c565b6102d06040518060400160405280600481526020017f4e4f54410
0000000000000000000000000000000000000000000000000000000000008152506040518060400160405280601181526020017f4e6f6e65206f66207468652061626f7665000000000000000000000000000000008152506102d56020
1b60201c565b61041a565b600260008154809291906001019190505550604051806080016040528060025481526020018381526020018281526020016000815250600160006002548152602001908152602001600020600082 0
1518160000155602082015181600101908051906020019061034692919061037556 5b5060408201518160020190805190602001906103639291906103755 65b506060820151816003015590505050505 65b8280546001816001
161561010002031660029004906000526020600020906 01f016020900481019282601f106103b657805160ff19168380011785556103e4565b82800160010185555821561 03e4579182015b82811115610 3e35782518255591602
0019190600101906103c8565b5b5090506103f191906103f5565b5090565b61041791905b808211156104135760008160009055506001016103fb565b5090565b90565b6104f3806104296000396000f3fe608060405234801 5
61001057600080fd5b5060043610610 04c5760003560e01c80630121b93f146100515780632d35a8a21461007f5780633477ee2e1461009d578063a3ec138d146101be575b600080fd5b61007d6004803603602081101561006
757600080fd5b8101908080359060200190929190505050610 21a565b005b610087610338565b6040518082815260200191505060405180910390f35b6100c96004803603602081101561 00b357600080fd5b81019080803590
6020019092919050505061033e565b604051808581526020018060200180602001848152602001838103835286818151815260200191508051906020019080838360005b838110156101195780820151818401526020810190 5
06100fe565b5050505090509081019060 1f16801561014657808203805160018360200361010 00a031916815260200191505b50838103825285818151815260200191508051906020019080838360005b8381101561017f5780
820151818401526020810190506101645 65b50505050905090810190601f1680156101ac5780820380516001836020036101000a031916815260200191505b50965050505050505060405180910390f35b610200600480360 36
020811015610 1d457600080fd5b81019080803573ffffffffffffffffffffffffffffffffffffffff16906020019092919050505061049e565b6040518082151515158152602001915050604051809103 90f35b6000803373ff
ffffffffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffffffffffff16815260200190815260200160002060009054906101000a900460ff161561027057600080fd5b6000811180156102825
7506002548111155b61028b57600080fd5b6001600080337 3ffffffffffffffffffffffffffffffffffffffff1673ffffffffffffffffffffffffffffffffffffffff16815260200190815260200160002060006101000a8154
8160ff021916908315150217905550600160008281526020019081526020016000206003016000815480929190600101919050555080 7ffff3c900d938d21d0990d786e819f29b8d05c1ef587b462b939609625b684b1660405
16040518091039 0a250565b600254815 65b6001602052806000526040600020600091509050806000015490806001018054600181600116156101000203166002900480601f0160208091040260200160405190810160405280
92919081815260200182805460018160011615610100020316600290048015610 3f05780601f106103c5576101008083540402835291602001916103f0565b820191906000526020600020905b815481529060010190602001 8
08311610 3d357829003601f168201915b505050505090806002018054600181600116156101000203166002900480601f0160208091040260200160405190810160405280929190818152602001828054600181600116156101
000203166002900480156104 8e5780601f1061046357610100808354040283529160200191610 48e565b820191906000526020600020905b8154815290600101906020018083116104715782900 3601f168201915b505050505
09080600301549050845 65b600060205280600052604060002060009150549061 01000a900460ff168156fea265627a7a723158201f86ea177ff5bf4f50935243cdaac285013921da7243eadab2975ddddd5b646364736f6c63
430005100032436f6d6d756e697374205061727479204f6620496e64696120284d61727869737429
```

Figure: Contract Creation Transaction

cont...



CURRENT BLOCK 159
GAS PRICE 20000000000
GAS LIMIT 6721975
HARDFORK MUIRGLACIER
NETWORK ID 5777
RPC SERVER HTTP://127.0.0.1:7545
MINING STATUS AUTOMINING
WORKSPACE BLOCKCHAIN-VOTING

0×ef4a04e4296757c156f9ea2e824863d605f6e266c32654b4f8471c83641a9b31 (0)

CONTRACT NAME
Election

CONTRACT ADDRESS
0×1e85bdCD1B78989d4ea2F164864562E3F60DCBcE

SIGNATURE (DECODED)
votedEvent(_candidateId: uint256)

TX HASH
0×ef4a04e4296757c156f9ea2e824863d605f6e266c32654b4f8471c83641a9b31

LOG INDEX
0

BLOCK TIME
2020-06-23 15:30:05

RETURN VALUES

_CANDIDATEID
4

Figure: Voted Event Transaction

Cont..

- An E-Voting system based on Permission Blockchain that do not exposes the progress of election during voting phase.
- System that minimize the cost of voting system.
- Make Voting Convenient for the voter.
- The voting as well as the counting process more transparent.

Expected research outcome

- An E-Voting system based on Permission Blockchain that do not exposes the progress of election during voting phase.
- System that minimize the cost of voting system.
- Make Voting Convenient for the voter.
- The voting as well as the counting process more transparent.

References I

- Wolchok, Scott, et al. "Security analysis of India's electronic voting machines.", *Proceedings of the 17th ACM conference on Computer and communications security.*,2018 .

- Ohlin, Jens David. "Did Russian cyber interference in the 2016 election violate international law." , *Tex. L. Rev. 95* .,2016.

- Brightwell, I., Cucurull, J., Galindo, D., Guasch, S.: An overview of the ivote 2015 voting system , ,2015.

- Barnes, Andrew, Christopher Brake, and Thomas Perry. "Digital Voting with the use of Blockchain Technology." , *Team Plymouth PioneersPlymouth University* .,2016.

- Caiazzo, Francesca, and Ming Chow. "A BlockChain Implemented Voting System." ,2016.

References II

Ayed, Ahmed Ben. "A conceptual secure blockchain-based electronic voting system." , *International Journal of Network Security Its Applications 9.3* ,2017.

Yu, Bin, et al."Platform-independent secure blockchain-based voting system." , *International Conference on Information Security. Springer, Cham.*,2018.