Decentralized Public and Private Ledger Technology and Its Applications

Akshat Minesh Doshi

School of Engineering and Applied Science, Ahmedabad University
StartNExcel
Guide: Himanshu Chudasama, Rushiraj Yadav

BTP-2, 7 May 2018

Outline

1. Introduction
2. Blockchain
3. How Bitcoin Transaction Works
4. Blockchain Technology
5. Blockchain Technology Type
6. Cryptocurrency
7. How Blockchain Transaction Works
8. Top Cryptocurrencies
9. ERC-20 Based Token on Ethereum Blockchain
10. SEAS-AU ERC-20 Based Token on Ropsten Test Network
11. Mining
12. Blockchain for Business
13. Decentralized Voting Application on Ethereum Blockchain

Introduction

- Blockchain is the technology behind all of this crypto currencies. Blockchain helps to build **trusted, powerful and transparent** with the potential to disrupt intermediaries, third party expensive process.
- Blockchian is one kind of linked list. Blockchian is a cryptographed, secure, decentralized database. Shared, trusted, public ledger of transactions, that everyone can inspect but which **no single user controls** or can change. Once you put something into it, it will stay there forever.
- **Applications of Blockchain**: Cryptocurrency, Smart Contracts, Government body, Digital Identity, Registry, IoT, compliance, Financial Service, Health care, Insurance

Blockchain

- A **block** refers to a **set of transactions that are bundled together** and added to the chain at the same time. In the Bitcoin blockchain, the miner nodes bundle unconfirmed and valid transactions into a block. Each block contains a given number of transactions.
- A blockchain can be both **permissionless or public** (like Bitcoin or Ethereum) and **permissioned or private** (like the different Hyperledger blockchain frameworks).
- In the Bitcoin network, **miners** must solve a cryptographic challenge to propose the next block. This process is known as **'proof of work'**, and requires significant computing power.
- These **smart contracts** are a piece of code running on top of a blockchain network, where digital assets are controlled by that piece of code implementing arbitrary rules.

Blockchain

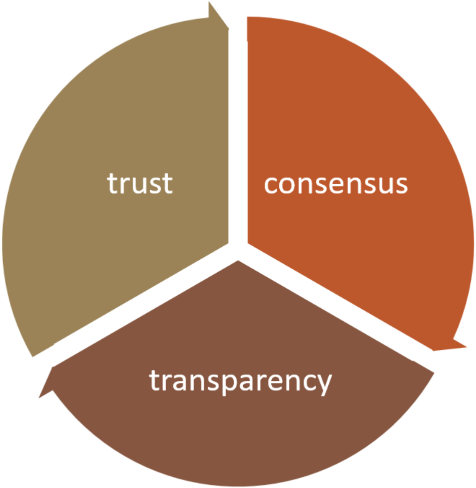
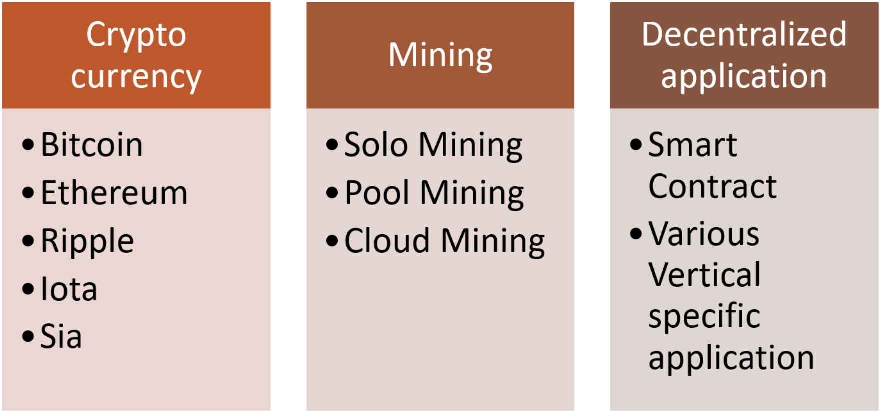


Figure: Blockchain Pillar

Blockchian Technology Types



Crypto currency

- Bitcoin
- Ethereum
- Ripple
- Iota
- Sia

Mining

- Solo Mining
- Pool Mining
- Cloud Mining

Decentralized application

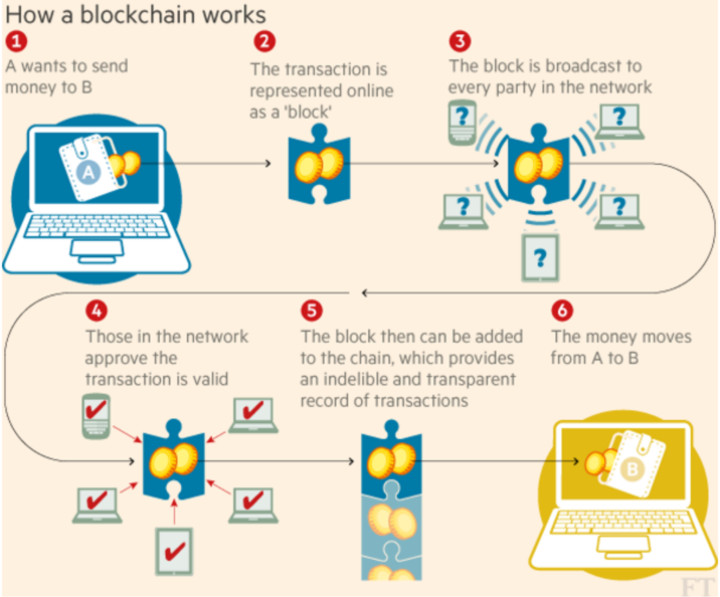
- Smart Contract
- Various Vertical specific application

Figure: One can divide the use cases of the blockchain technology in major 3 categories.

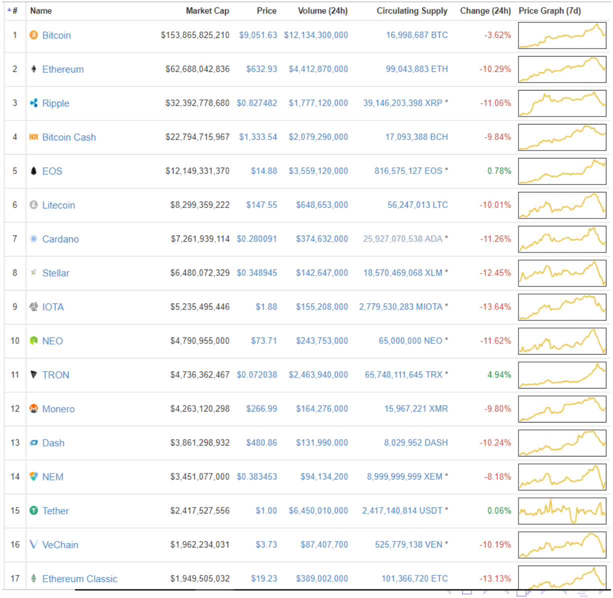
Cryptocurrency

- Current System of Money Transfer
  - Send Money from A in USA to B in India
  - Bank verifies A, checks balance, verifies B and gives it to B.
  - Bank takes fees
- Problems
  - Central Authority
  - Slow
  - Costly
- Solution of this is crypto currencies. Benefits of this crypto coins or tokens are:
  - Removal of Central Authority
  - Rewarding Users of the Network
  - Enhanced Data Transparency
  - Better Fault Tolerance
  - Faster
  - Cheaper

How Blockchain Transaction Works

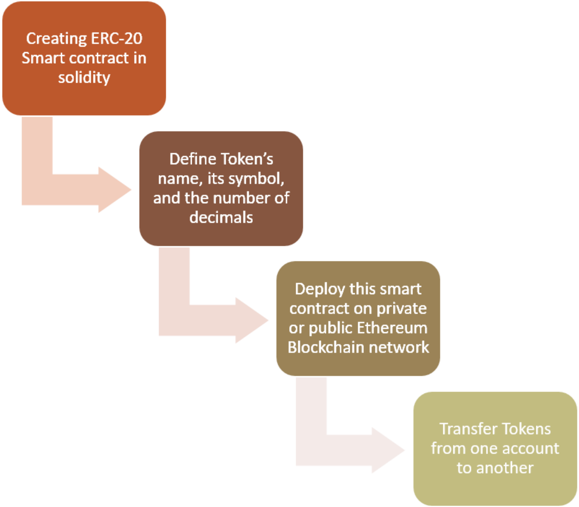

How a blockchain works
1
A wants to send money to B
A
2
The transaction is represented online as a 'block'
3
The block is broadcast to every party in the network
?
4
Those in the network approve the transaction is valid
5
The block then can be added to the chain, which provides an indelible and transparent record of transactions
6
The money moves from A to B
B
FT

Top cryptocurrencies



#	Name	Market Cap	Price	Volume (24h)	Circulating Supply	Change (24h)	Price Graph (7d)
1	Bitcoin	$153,865,825,210	$9,051.63	$12,134,300,000	16,998,687 BTC	-3.62%	
2	Ethereum	$62,688,042,836	$632.93	$4,412,870,000	99,043,883 ETH	-10.29%	
3	Ripple	$32,392,778,680	$0.827482	$1,777,120,000	39,146,203,398 XRP *	-11.06%	
4	Bitcoin Cash	$22,794,715,967	$1,333.54	$2,079,290,000	17,093,388 BCH	-9.84%	
5	EOS	$12,149,331,370	$14.88	$3,559,120,000	816,575,127 EOS *	0.78%	
6	Litecoin	$8,299,359,222	$147.55	$648,653,000	56,247,013 LTC	-10.01%	
7	Cardano	$7,261,939,114	$0.280091	$374,632,000	25,927,070,538 ADA *	-11.26%	
8	Stellar	$6,480,072,329	$0.348945	$142,647,000	18,570,469,068 XLM *	-12.45%	
9	IOTA	$5,235,495,446	$1.88	$155,208,000	2,779,530,283 MIOTA *	-13.64%	
10	NEO	$4,790,955,000	$73.71	$243,753,000	65,000,000 NEO *	-11.62%	
11	TRON	$4,736,362,467	$0.072038	$2,463,940,000	65,748,111,645 TRX *	4.94%	
12	Monero	$4,263,120,298	$266.99	$164,276,000	15,967,221 XMR	-9.80%	
13	Dash	$3,861,298,932	$480.86	$131,990,000	8,029,952 DASH	-10.24%	
14	NEM	$3,451,077,000	$0.383453	$94,134,200	8,999,999,999 XEM *	-8.18%	
15	Tether	$2,417,527,556	$1.00	$6,450,010,000	2,417,140,814 USDT *	0.06%	
16	VeChain	$1,962,234,031	$3.73	$87,407,700	525,779,138 VEN *	-10.19%	
17	Ethereum Classic	$1,949,505,032	$19.23	$389,002,000	101,366,720 ETC	-13.13%	

Ethereum Token/ERC-20 Smart Contract Creation



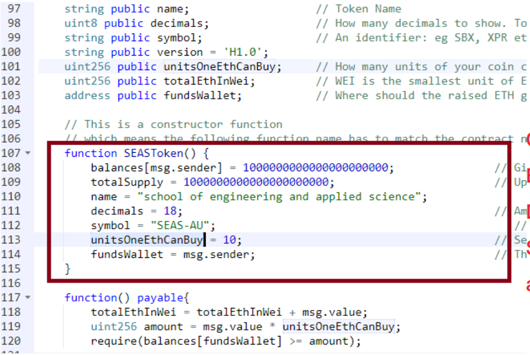
Creating ERC-20 Smart contract in solidity

Define Token's name, its symbol, and the number of decimals

Deploy this smart contract on private or public Ethereum Blockchain network

Transfer Tokens from one account to another

ERC-20 Based Tokens

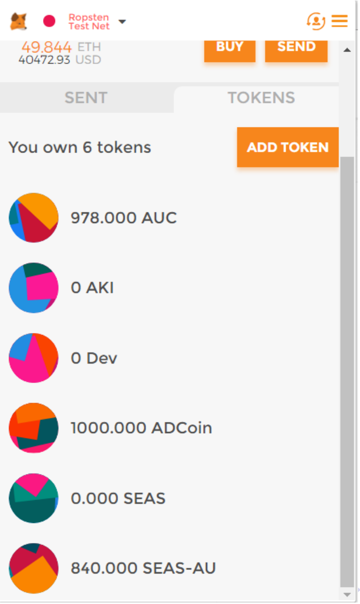


```
    string public name;                   // Token Name
    uint8 public decimals;                // How many decimals to show. To
    string public symbol;                 // An identifier: eg SBX, XPR et
    string public version = 'H1.0';
    uint256 public unitsOneEthCanBuy;     // How many units of your coin c
    uint256 public totalEthInWei;         // WEI is the smallest unit of E
    address public fundsWallet;           // Where should the raised ETH g

    // This is a constructor function
    // which means the following function name has to match the contract n
    function SEASToken() {
        balances[msg.sender] = 1000000000000000000000;                // Gi
        totalSupply = 1000000000000000000000;                         // Up
        name = "school of engineering and applied science";
        decimals = 18;                                                // Am
        symbol = "SEAS-AU";                                            //
        unitsOneEthCanBuy = 10;                                       // Se
        fundsWallet = msg.sender;                                     // Th
    }

    function() payable{
        totalEthInWei = totalEthInWei + msg.value;
        uint256 amount = msg.value * unitsOneEthCanBuy;
        require(balances[fundsWallet] >= amount);
```

Creating SEAS-AU ERC-20 Based Token. Define Token Name, Symbol, Total Supply and Price of the Token.

Figure: ERC-20 Based Token Creation (Token Name - ”School of Engineering and Applied Science”, Token Symbol - ”SEAS-AU”, Token Price - 1 Ether = 10 SEAS-AU Tokens)

Main Account Tokens



49.844 ETH
40472.93 USD

You own 6 tokens

978.000 AUC

0 AKI

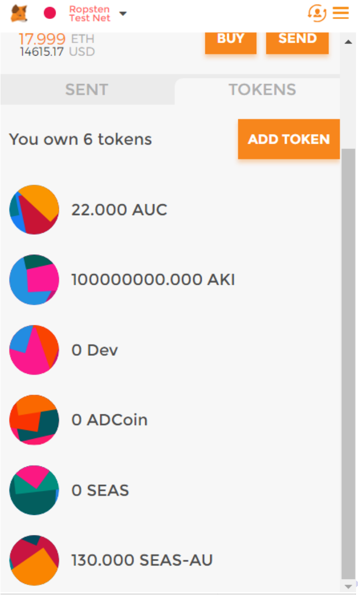
0 Dev

1000.000 ADCoin

0.000 SEAS

840.000 SEAS-AU

Another Account-1 For Transferring the Coin



17.999 ETH
14615.17 USD

You own 6 tokens

22.000 AUC

100000000.000 AKI

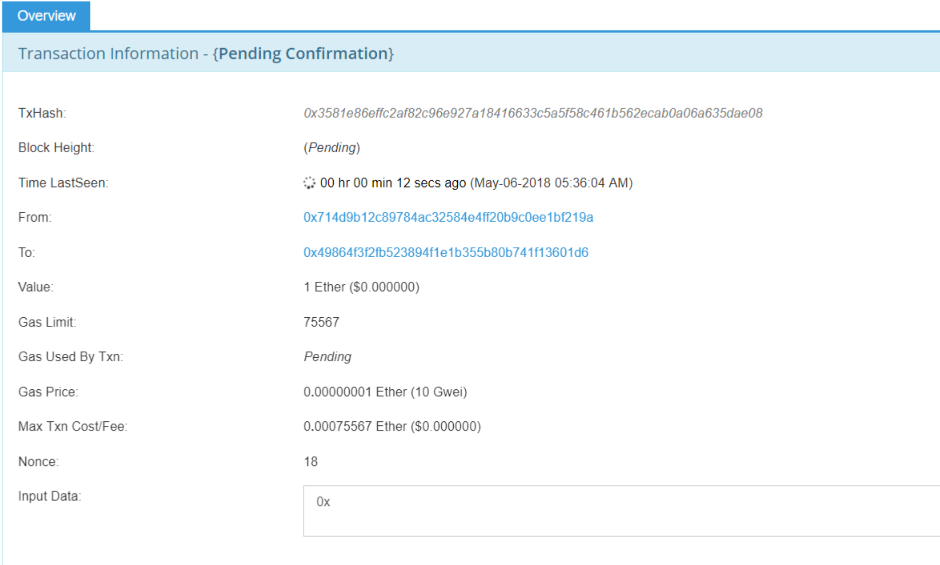
0 Dev

0 ADCoin

0 SEAS

130.000 SEAS-AU

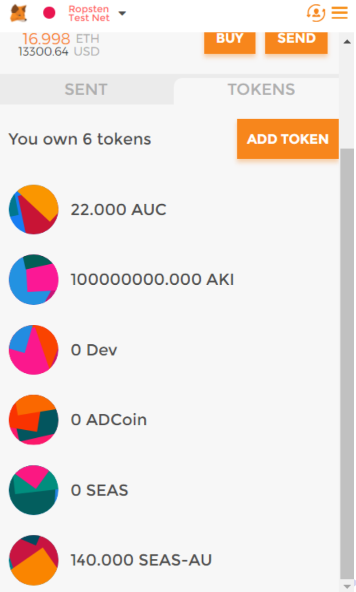
Transferring Token Transaction Pending



Transaction Information - {**Pending Confirmation**}

TxHash:	*0x3581e86effc2af82c96e927a18416633c5a5f58c461b562ecab0a06a635dae08*
Block Height:	(*Pending*)
Time LastSeen:	00 hr 00 min 12 secs ago (May-06-2018 05:36:04 AM)
From:	0x714d9b12c89784ac32584e4ff20b9c0ee1bf219a
To:	0x49864f3f2fb523894f1e1b355b80b741f13601d6
Value:	1 Ether ($0.000000)
Gas Limit:	75567
Gas Used By Txn:	*Pending*
Gas Price:	0.00000001 Ether (10 Gwei)
Max Txn Cost/Fee:	0.00075567 Ether ($0.000000)
Nonce:	18
Input Data:	0x

10 Token is Transferred From Main Account To Account-1



16.998 ETH
13300.64 USD

You own 6 tokens

22.000 AUC

100000000.000 AKI

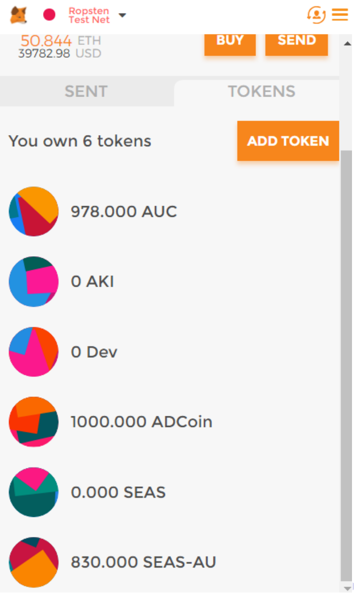
0 Dev

0 ADCoin

0 SEAS

140.000 SEAS-AU

10 Token is Deducted from Main Account



50.844 ETH
39782.98 USD

You own 6 tokens

978.000 AUC

0 AKI

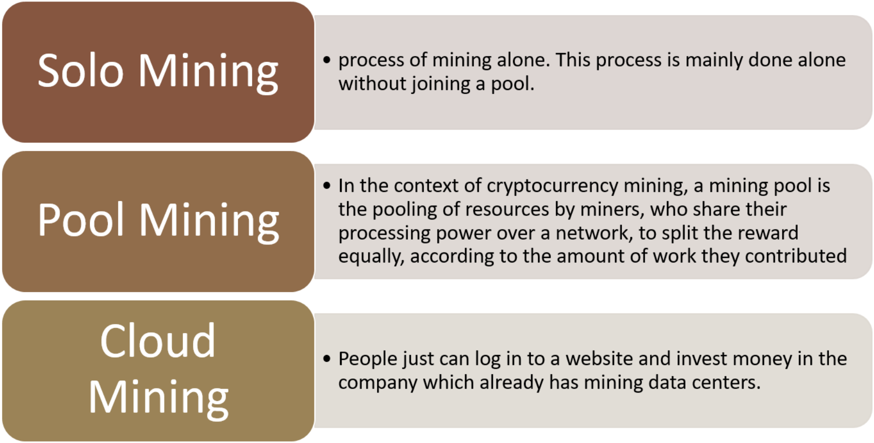
0 Dev

1000.000 ADCoin

0.000 SEAS

830.000 SEAS-AU

Mining



Solo Mining

- process of mining alone. This process is mainly done alone without joining a pool.

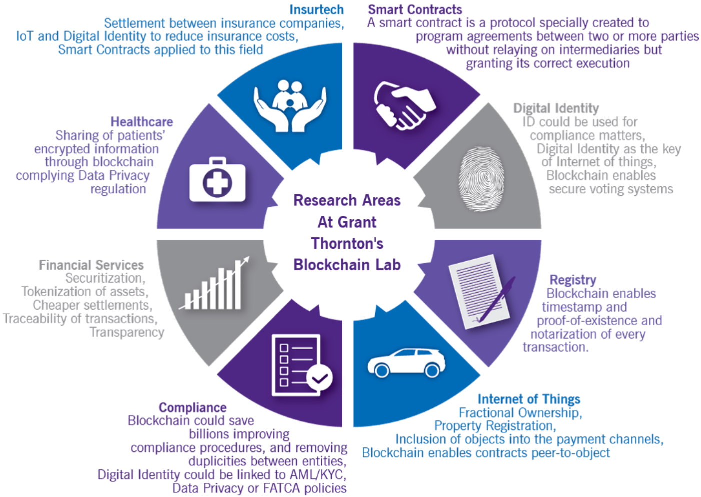
Pool Mining

- In the context of cryptocurrency mining, a mining pool is the pooling of resources by miners, who share their processing power over a network, to split the reward equally, according to the amount of work they contributed

Cloud Mining

- People just can log in to a website and invest money in the company which already has mining data centers.

Blockchain For Business



Research Areas At Grant Thornton's Blockchain Lab

Insurtech
Settlement between insurance companies,
IoT and Digital Identity to reduce insurance costs,
Smart Contracts applied to this field

Smart Contracts
A smart contract is a protocol specially created to
program agreements between two or more parties
without relaying on intermediaries but
granting its correct execution

Digital Identity
ID could be used for
compliance matters,
Digital Identity as the key
of Internet of things,
Blockchain enables
secure voting systems

Registry
Blockchain enables
timestamp and
proof-of-existence and
notarization of every
transaction.

Internet of Things
Fractional Ownership,
Property Registration,
Inclusion of objects into the payment channels,
Blockchain enables contracts peer-to-object

Compliance
Blockchain could save
billions improving
compliance procedures, and removing
duplicities between entities,
Digital Identity could be linked to AML/KYC,
Data Privacy or FATCA policies

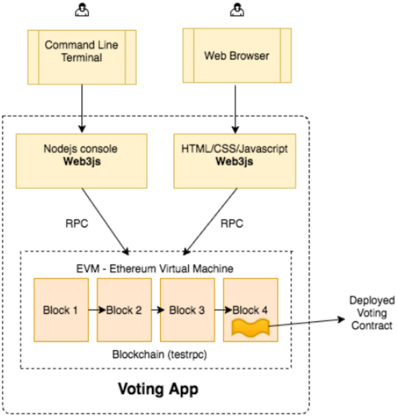
Financial Services
Securitization,
Tokenization of assets,
Cheaper settlements,
Traceability of transactions,
Transparency

Healthcare
Sharing of patients'
encrypted information
through blockchain
complying Data Privacy
regulation

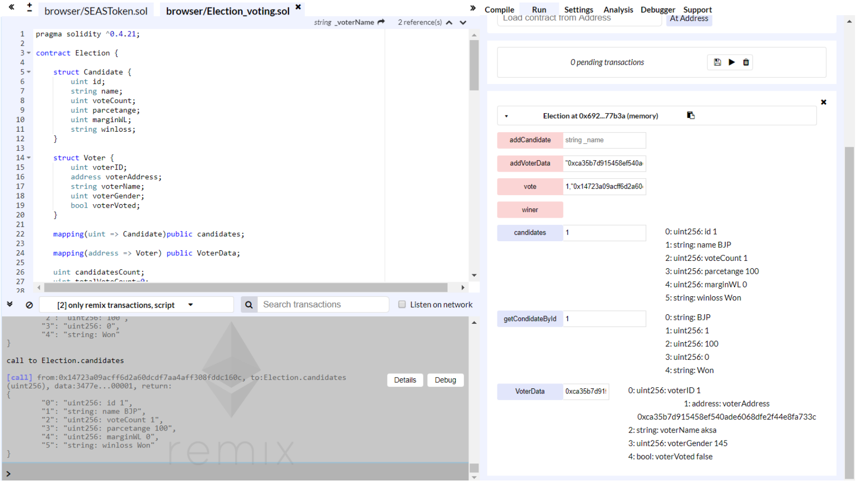
Voting Application

- I have made decentralized voting application. User or voter can vote for their favorite candidate from this application.
- Main functionality of this Dapp is that no one can hack this application and no one can give vote more then one time.
- Since a blockchain is a permanent record of transactions (votes) that are distributed, every vote can irrefutably be traced back to exactly when and where it happened without revealing the voters identity.
- In addition, past votes cannot be changed, while the present cant be hacked, because every transaction is verified by every single node in the network.
- And any outside or inside attacker must have control of 51 percent of the nodes to alter the record.

Voting Application Interaction With Ethereum Blockchain



Election Application



```
pragma solidity ^0.4.21;

contract Election {

    struct Candidate {
        uint id;
        string name;
        uint voteCount;
        uint parcetange;
        uint marginWL;
        string winloss;
    }

    struct Voter {
        uint voterID;
        address voterAddress;
        string voterName;
        uint voterGender;
        bool voterVoted;
    }

    mapping(uint => Candidate)public candidates;

    mapping(address => Voter) public VoterData;

    uint candidatesCount;
    uint totalVoteCount=0;
```

[2] only remix transactions, script

Search transactions

□ Listen on network

```
        "2": "uint256: 100",
        "3": "uint256: 0",
        "4": "string: Won"
}

call to Election.candidates

[call] from:0x14723a09acff6d2a60dcdf7aa4aff308fddc160c, to:Election.candidates
(uint256), data:3477e...00001, return:
{
        "0": "uint256: id 1",
        "1": "string: name BJP",
        "2": "uint256: voteCount 1",
        "3": "uint256: parcetange 100",
        "4": "uint256: marginWL 0",
        "5": "string: winloss Won"
}

>
```

Election at 0x692...77b3a (memory)

addCandidate: string _name

addVoterData: "0xca35b7d915458ef540a

vote: 1,"0x14723a09acff6d2a60

winer

candidates: 1

0: uint256: id 1
1: string: name BJP
2: uint256: voteCount 1
3: uint256: parcetange 100
4: uint256: marginWL 0
5: string: winloss Won

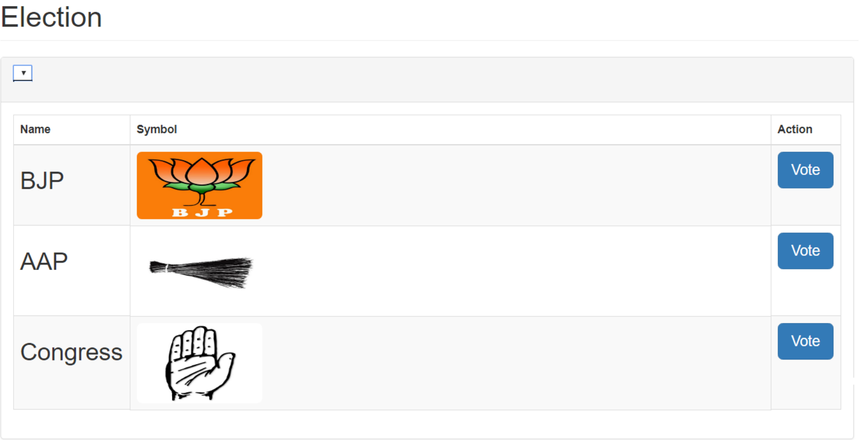
getCondidateById: 1

0: string: BJP
1: uint256: 1
2: uint256: 100
3: uint256: 0
4: string: Won

VoterData: 0xca35b7d91

0: uint256: voterID 1
1: address: voterAddress
0xca35b7d915458ef540ade6068dfe2f44e8fa733c
2: string: voterName aksa
3: uint256: voterGender 145
4: bool: voterVoted false

Voting Panel

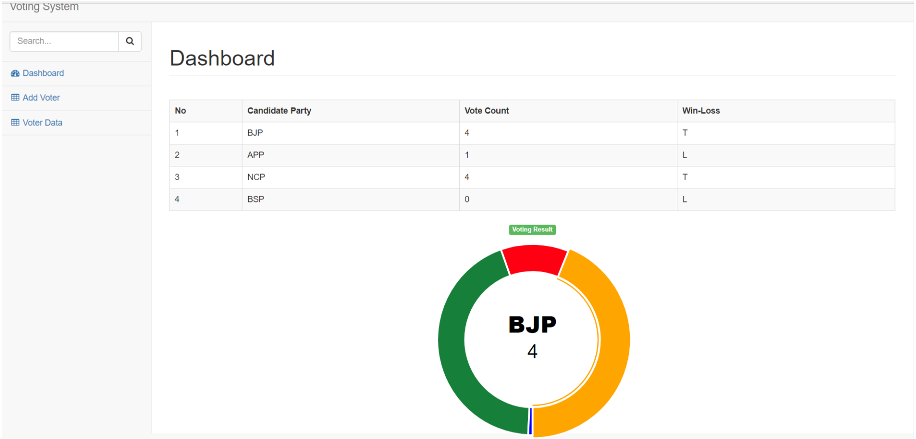


Election

▾

Name	Symbol	Action
BJP		Vote
AAP		Vote
Congress		Vote

Election Application Dashboard



Dashboard

No	Candidate Party	Vote Count	Win-Loss
1	BJP	4	T
2	APP	1	L
3	NCP	4	T
4	BSP	0	L

References I

- Bitcoin: A Peer-to-Peer Electronic Cash System Satoshi Nakamoto satoshin@gmx.com www.bitcoin.org
- A Next-Generation Smart Contract and Decentralized Application Platform, Ethereum, https://www.ethereum.org/.
- Blockchain Hub, blockchian beginners guide
- Blockchains, Smart Contracts und das Dezentrale Web, Shermin Voshmgir
- IBM hyperledger - https://www.ibm.com/blockchain/hyperledger.html
- https://coinmarketcap.com/
- https://xinfin.org/
- https://etherscan.io

References II

- https://nodejs.org/
- https://metamask.io/
- https://courses.edx.org/courses/course-v1:LinuxFoundationX+LFS171x+3T2017/course/
- https://www.udemy.com/ethereum-dapp/
- Applications of Blockchain Technology beyond Cryptocurrency, Mahdi H. Miraz, Maaruf Ali.
- The Blockchain Technology: Some Theory and Applications, Nicola Dimitri.
- Antonopoulos A., Mastering Bitcoin (2nd Ed), OReilly, (2017)

Thank You.