International Conference on Communication and Information Processing
(ICCIP-2019)
Available on: Elsevier-SSRN

Blockchain Based E-Voting System

Harshal Patil, Prathmesh Ladkat, Abhishek Jituri,Rohit Desai,Dr. Swati V. Shinde

I.T.Department. PCCOE, Pune

Abstract

Recently, numerous accusations have been raised on the sincerity of the Electronic Voting Machines (EVM) used in Indian elections. Because of these accusations, there is a need for a newer system that can be able to meet up security and modern era. The new system should be able to gain the trust of people and encourage them to vote. It should be secure, auditable, and transparent and should be able to reinforce the confidence of the voters in the democratic election process. Blockchain technology allows for the development of a decentralized distributed open ledger. It offers features like immutability of data, the integrity of data, transparency in the system and resistance of data to modifications. Using these features of Blockchain a voting system can be built that will solve existing issues with EVMs and will be sufficiently automated.

Keywords - Blockchain, EVM, features, Voting system.

1. Introduction

A blockchain can be used for security purposes as it provides transparency, security, and authenticity, which helps us to build trust among the users. Blockchain technology has been worked for many years and finds its application in financial and non-financial application [1]. It is a distributed database which consists records of all transactions and every block in blockchain technology has been executed and shared among different participating parties. Blockchain technology is attracting interest for many industries and universities in the world. In blockchain since there are various versions and everything decentralized, we need to have a method where everybody in the system come to a common agreement for verification. Blockchain provides proof of work, proof of activity, proof of capacity and many more.

2. Components Of Blockchain

2.1. Distributed Ledger (Database)

The distributed ledger means the shared contents and databases available to the participants of a particular Blockchain Ecosystem. The shared ledger lists down the rules or guidelines that need to be followed in each node applications in the blockchain ecosystem [1].

For example, if you are running a Bitcoin node application, then you have to abide by all the rules set down in the program code of the Bitcoin node application.

2.2. Consensus Algorithm

The consensus algorithm provides security to the data in the blockchain which is not volatile. It shows the network status and how the nodes in the network appear at a consensus regarding what transactions to accept. What protects the blockchain from tampering is the fact that changing a block can be done only by making a new block from its predecessor and it also requires re-generating all successors and redoing their contents [1]. It is to be noted that each block in the blockchain consists of a hash of its predecessor block, thus this creates a chain of blocks with an enormous amount of work contained in them [2].

2.3. Types Of Blockchain

Avoid The Bitcoin blockchain can be used in various agreements such as peer-to-peer insurance, energy trading, peer-to-peer ride sharing or any kind of valuable transaction. The Ethereum project thought of creating a blockchain of their own, by decoupling the smart contract layer from the core blockchain protocol
[3].This offers best way to create Smart Contracts like online transactions in markets thus having different properties than Bitcoin. Private institutions such as banks visualized about using the distributed blockchain ledger, and make an authorized blockchain which can be private, public or consortium, validator can be an internal legal person of the organization.

1. Public Blockchains

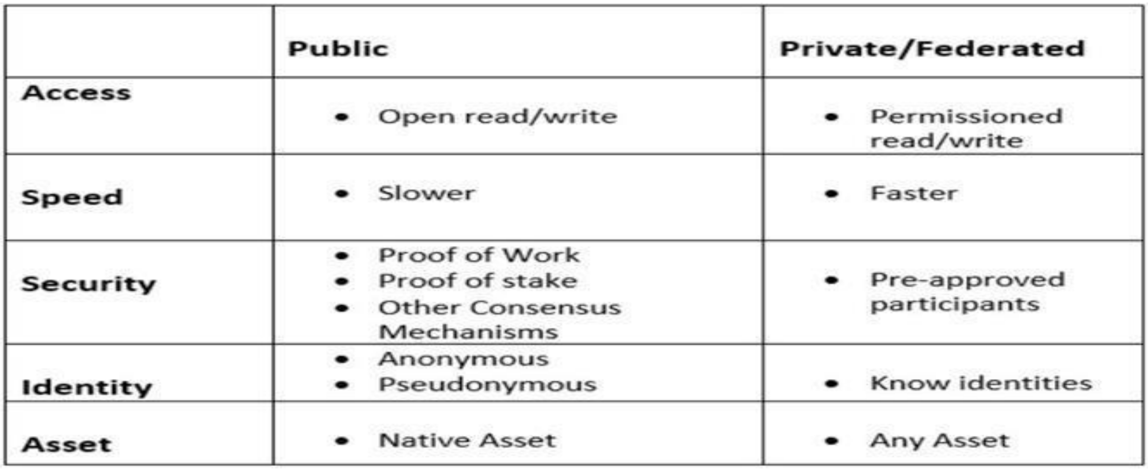
Blockchain technology is based on open source Proof of Work consensus algorithms. Any user could participate, without permission [1]. The code is available for everyone to download and run a public node on their local device, the transactions can be validated in the network, this makes them participate in the agreement process, which is for determination of which blocks is append to the chain and what is its present state [4]. Any valid user in the world is able to send transactions in the network and they would see them in the blockchain [2]. The public block explorer allows everyone to read the transactions. These transactions are transparent to everyone but they are anonymous.
Examples: Bitcoin, Ethereum, etc.

2. Federated Blockchain or Consortium Blockchains

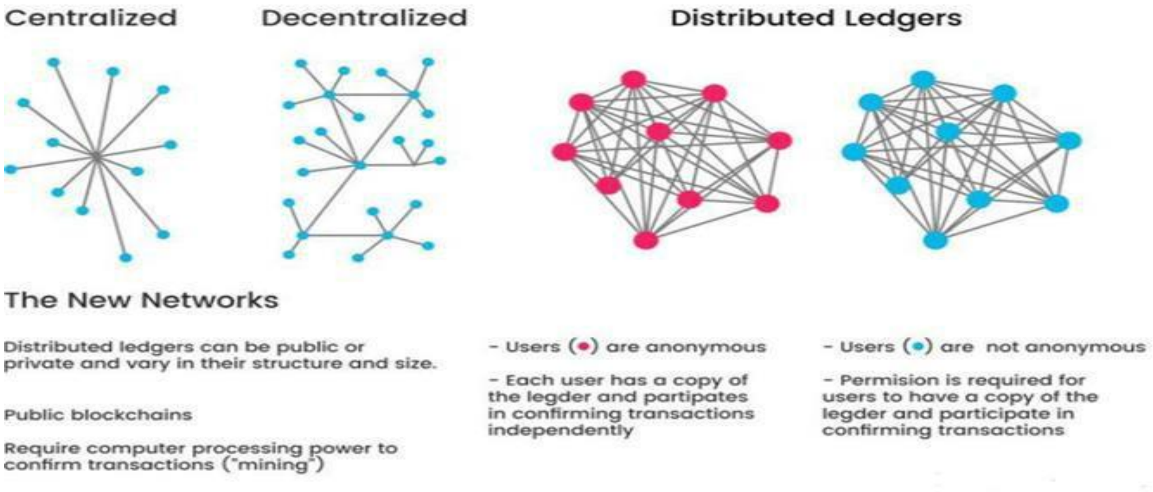
Federated Blockchains are operated under the authority of an authorized class. Contrasting to public blockchains, the verification of the transactions cannot be done by any random person who has access to internet. Federated Blockchains has higher scalability and provide more privacy to the transactions. Consortium blockchain finds its application mostly in banking sectors. The blockchain can be public or restricted in order to control the read of blockchain.
Example: R3CEV LLC, **Energy** Web Foundation.

3. Private Blockchains

The permission of write is given to only single organization and the permissions of read can be public or confined to a specific group. For example, database management which is internal to a single company, and the public readability may or may not be necessary. Private Blockchains allows us to set up the members to verify the transactions internally. Private Blockchain has a risk of security similar to that of a centralized system. However, private blockchain is useful, especially when it comes to scalability and privacy of data and other managerial issues. They have certain advantages and disadvantages of security.
Examples: MONAX, **Multichain.**



	Public	Private/Federated
Access	• Open read/write	• Permissioned read/write
Speed	• Slower	• Faster
Security	• Proof of Work • Proof of stake • Other Consensus Mechanisms	• Pre-approved participants
Identity	• Anonymous • Pseudonymous	• Know identities
Asset	• Native Asset	• Any Asset



The New Networks

Distributed ledgers can be public or private and vary in their structure and size.

Public blockchains

Require computer processing power to confirm transactions ("mining")

- Users (●) are anonymous

- Each user has a copy of the legder and partipates in confirming transactions independently

- Users (●) are not anonymous

- Permision is required for users to have a copy of the legder and participate in confirming transactions

Fig.1.3. Networks in Blockchain [1]

3. Voting System

A. Voting

Voting is an example of group activity, in order to express the ideas or make a decision, it includes discussion or elections. The high order authorities are elected by voting. Constituents are the residents of an area which are represented by an elected official, and the voters are those constituents who cast a ballot for their chosen candidate [5].

In a democracy, elections are held to determine the government: in which we choose one candidate from the different candidates. In a self-government voting is way for the voter to appoint his representatives in the government.

A vote can be used as an opinion of an individual's choice for or against some decision or a candidate, or political party. Secret ballot system is used in almost all countries, in order to ensure the voters privacy and their political privacy.

B. Evolution of voting system in India

India has gradually evolved in the process of voting is carried out. The very simplest election carried out by using paper ballots in between October 1951 and March 1952, namely the General Elections. These paper ballots were then replaced by the Electronic Voting Machines (EVMs) [5]. The experimental EVMs were deployed in 1982, their extensive use started in 1998 and in the 2004 General Elections EVMs were deployed across all polling stations thus putting an end to a paper ballot. Nepal, Namibia, and Kenya have purchased the EVMs manufactured by India. In 2015 Fiji was expected to use Indian EVM. In 2013, however, the Supreme Court of India ordered that the constituents should be given the assurance that the vote cast by them has gone to the candidate of their choice. This help to grow the development of VVPAT (Voter Verifiable Paper Audit Trail) systems.

C. Security Analysis of India's voting system

Hari Prasad, an Engineer finished a year trying to convince election officials to complete the review, but the officials stand firm that the government made machines are perfect, and tamperproof. Then, in February 2010, he got access to one of the machine for review from an anonymous source [5]. Halderman described the designing, technical problems and security weakness of India's electronic voting system. He published a video showing how an attacker can replace the display of an EVM with a dishonest display that can be controlled remotely via Bluetooth. In another attack demonstration, they overwrote the memory chip with their own data of the votes thus demonstrating a serious violation which can be exploited to turn the votes in any candidate's favor [5]. The paper also pointed out that the manufacturing of microcontrollers for the Electronic Voting Machine was carried out by private companies. Hence, if the manufacturing process at that facility was compromised unknowingly then a lot of manipulation could be done to the entire voting process [5].

4. Architecture

Front-end client that is written in HTML, CSS, and JavaScript. Instead of a back -end server, this client will connect to a local Ethereum blockchain that we created. Code of all the business logic about our web application in an Election smart contract with the Solidity programming language [6]. We deploy this smart contract to our local Ethereum blockchain and allow accounts to start voting.

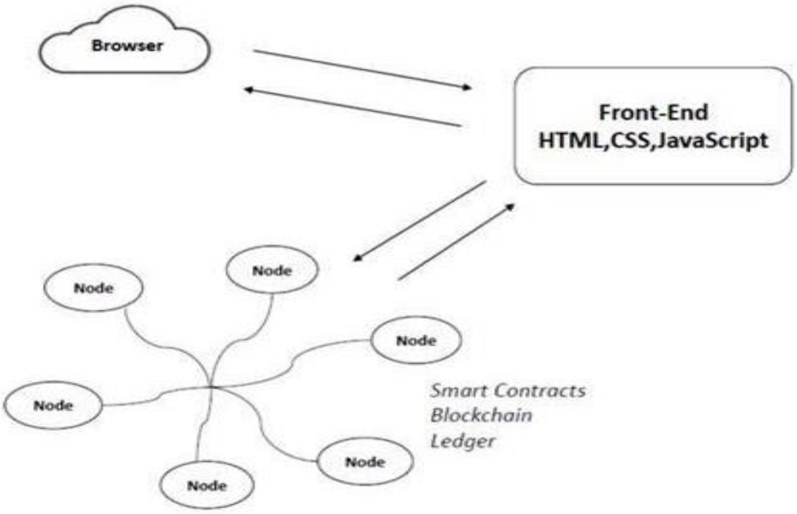


Fig.4.1. System Architecture [6]

5. Proposed System

During the time of the vote, the authentication of the user needs to be done. This can be done using the login credentials of the user and then verifying the user by using his Face recognition or Fingerprint. Meanwhile, the system validates the user. If the user has a valid pending vote, then they will be redirected to the next voting screen. If the vote is unavailable, then the system will prompt the user accordingly. Once the vote is selected and after the confirm submission, the vote transforms into a transaction, authorized public key will be used to encrypt it. Then this transaction is sent to the electorate nodes. Then these nodes are appended to blocks and an update is send to all nodes connected to that appropriate electorate nodes. Every peer of the nodes which are connected receives data until the network is completely updated.

After the confirmation of the vote a transaction is generated by the system to extract the vote of the user from the blockchain of voters. There are two different Blockchains being held; one which consists of the transactions related to the registered users and vote availability, the second contains the vote. Due to the usage of two distinct Blockchains, voter's anonymity can be maintained. The blockchain technology is invented because of cryptocurrency Bitcoin and then smart contracts are introduced in Ethereum platform.

Smart contracts are the contracts that are written as a codes into the blockchain, when triggering event is hit the contract automatically executes itself. Related to online internet services E-voting is the famous and critical topic which need to be handle safely. If we combine blockchain and smart contracts then it gives cheaper, more secure, transparent, and easy to use e-voting system. And also by properties of Ethereum and its network like consistency, provision of smart contract logic, and widespread use are very helpful.

- Comparision between existing system and proposed system :

Traditional System	**Proposed System**
Centralized System	Decentralized System
No Transparency in transaction	Transparancy in transaction
No individual verifiability	Individual verifiability
Use of DVD's to store votes	Votes stored on blockchain
Need of third party	No need of third party

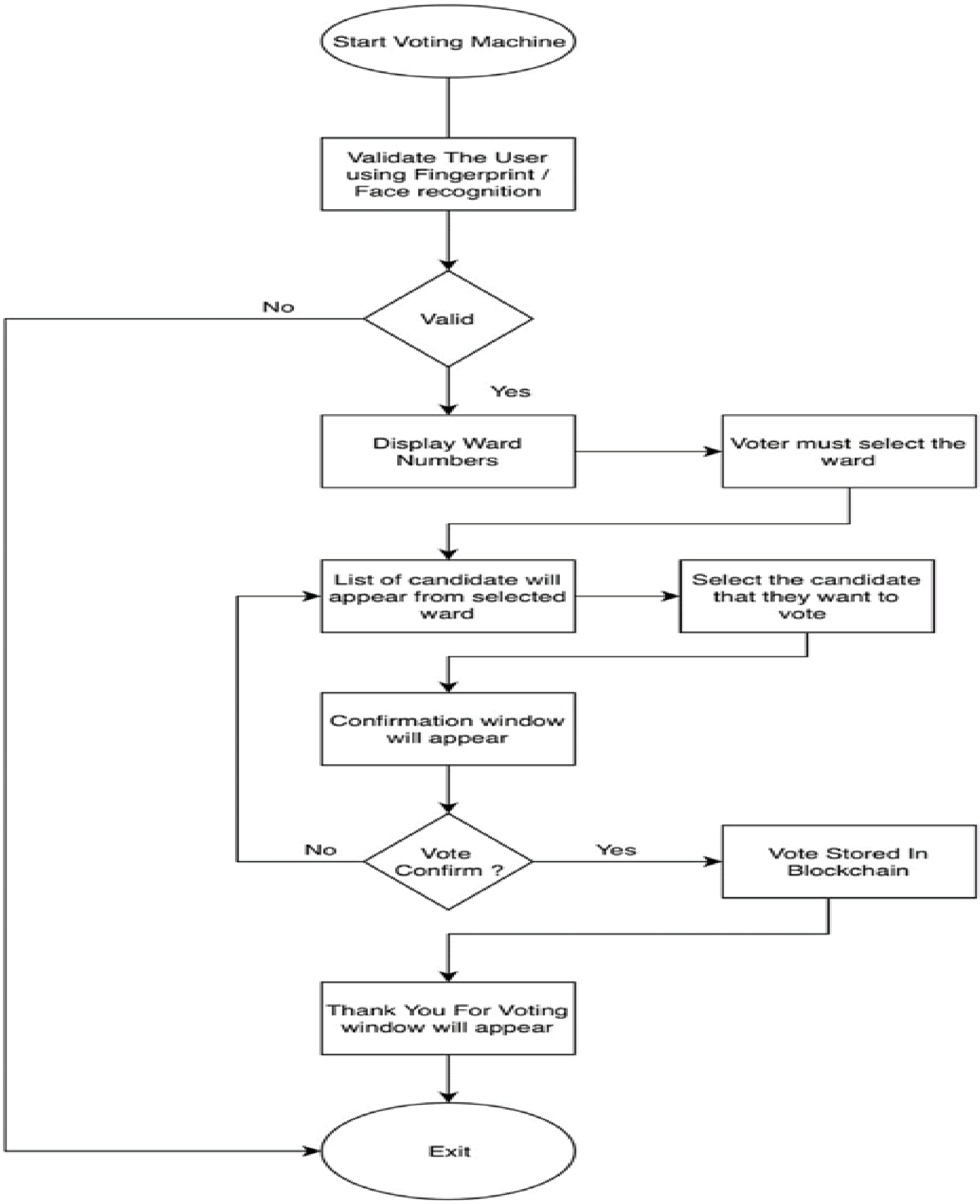

Start Voting Machine
Validate The User using Fingerprint / Face recognition
Valid
No
Yes
Display Ward Numbers
Voter must select the ward
List of candidate will appear from selected ward
Select the candidate that they want to vote
Confirmation window will appear
Vote Confirm ?
No
Yes
Vote Stored In Blockchain
Thank You For Voting window will appear
Exit

Fig.5.1. Working of System

Some properties of the blockchain seem to solve the security related challenges that occurs in voting system. Here is how blockchain addresses some of these challenges:

Inalterable votes: Many popular blockchain platforms use the Merkle tree used to confirm the integrity of the transactions or data added to the blockchain. Even if a single bit of data is altered or manipulated, it can be easily detected using a Merkle tree verification. This property of the blockchain to ensure that a vote once added to the blockchain cannot be altered or manipulated helps in achieving inalterable or immutability as well integrity verification of the votes.

Mathematical proof of recorded votes: Through the use of public key cryptography and hash or message digest values, mathematical proof of the origination of the data, and the exact time at which the data was added to the blockchain database can be provided. The blockchain database here simply refers to the voting-related data stored in the blockchain.

Data redundancy: The blockchain is synced across all the nodes participating in the blockchain network, and hence this provides data redundancy. Even if data at multiple locations is corrupted, tampered or even destroyed it can be recovered from any node on the network.

6. System Operations

Set the private blockchain network:

It is recommended that the actual system is deployed on a private network and that the nodes be allowed to connect to the network only after a proper authentication process [3]. The authentication credentials could be hard coded on individual devices or given to the officers responsible for setting up the individual machines on voting locations.

Uploading candidate's lists:

In the prototype's implementation, the candidate lists are hardcoded in the smart contract deployed on the network. This guarantees that the list cannot be altered once the contract is deployed. An alternative is to add all the lists of candidates for all wards in a single smart contract and then nodes in a ward would deal with the respective candidates for that ward.

Starting up individual nodes:

First, the node is started with the required APIs enabled. Once the node is up and running, the local server is started. The server communicates with the node through the Web3.py module. The first job of the server is to connect the node to the private Ethereum network. Once the node is connected to other peers in the private Ethereum network the device is ready to accept votes.

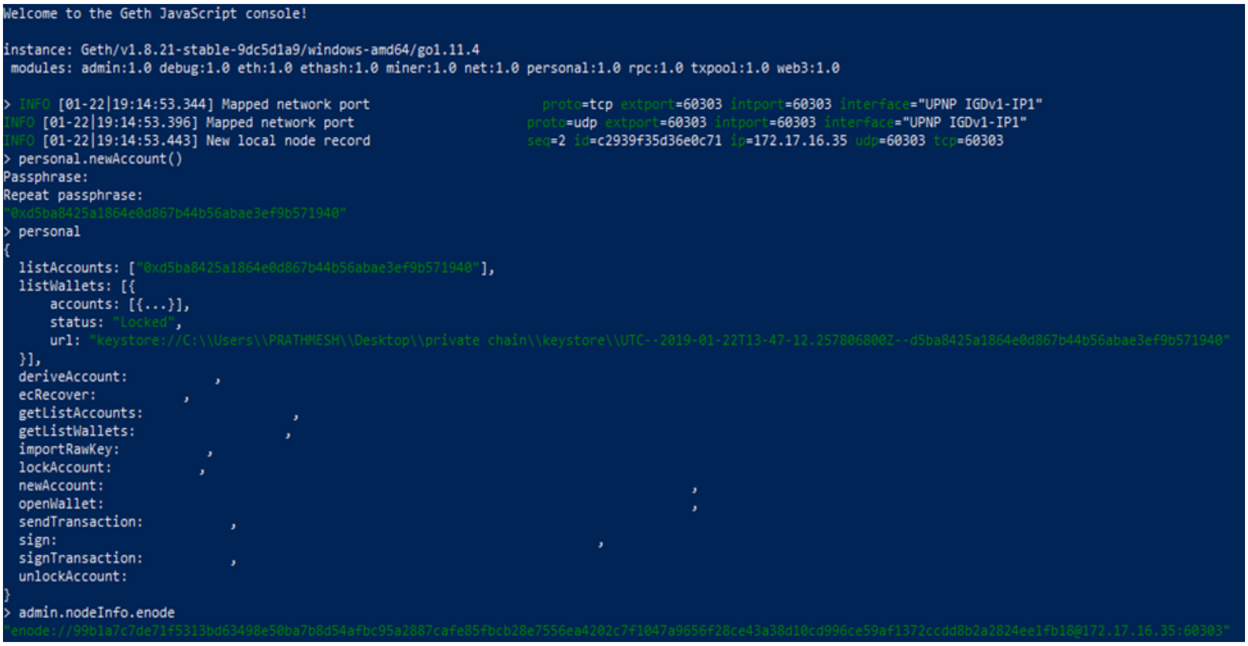
Conclusion

The blockchain is a good technology for helping to improve the voting systems. Not only this technology can benefit the voting authorities but also the help to gain voters trust due to its transparency and encourage more people to participate in the voting process. Due to Blockchains distributed and peer-to-peer characteristics, our system banish the need of centralized authority.

Due to distributed peer to peer architecture, it helps improve the security and reduces the risk of unauthorized alterations. Blockchain technology have very strong properties of security which constitutes largely to the security of our system. In order to avoid the threat of linking votes of certain parties to any of the individual while maintaining the ability of tracking how many voters have voted and still how many votes are present a completely separate blockchain is maintained.

In a centralized architecture, we describe possible attack scenarios and this attacks can be prevented by using Blockchain technology.

Setting up Ethereum network and creating private Blockchain:

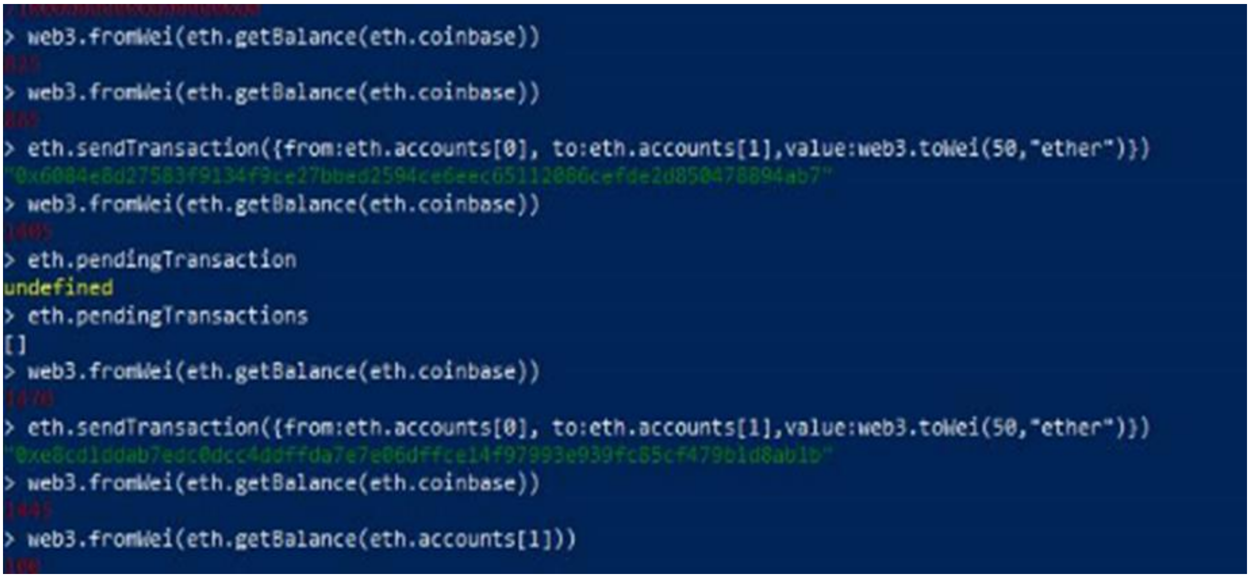


```
Welcome to the Geth JavaScript console!

instance: Geth/v1.8.21-stable-9dc5d1a9/windows-amd64/go1.11.4
 modules: admin:1.0 debug:1.0 eth:1.0 ethash:1.0 miner:1.0 net:1.0 personal:1.0 rpc:1.0 txpool:1.0 web3:1.0

> INFO [01-22|19:14:53.344] Mapped network port                      proto=tcp extport=60303 intport=60303 interface="UPNP IGDv1-IP1"
INFO [01-22|19:14:53.396] Mapped network port                      proto=udp extport=60303 intport=60303 interface="UPNP IGDv1-IP1"
INFO [01-22|19:14:53.443] New local node record                    seq=2 id=c2939f35d36e0c71 ip=172.17.16.35 udp=60303 tcp=60303
> personal.newAccount()
Passphrase:
Repeat passphrase:
"0xd5ba8425a1864e0d867b44b56abae3ef9b571940"
> personal
{
  listAccounts: ["0xd5ba8425a1864e0d867b44b56abae3ef9b571940"],
  listWallets: [{
      accounts: [{...}],
      status: "Locked",
      url: "keystore://C:\\Users\\PRATHMESH\\Desktop\\private chain\\keystore\\UTC--2019-01-22T13-47-12.257806800Z--d5ba8425a1864e0d867b44b56abae3ef9b571940"
  }],
  deriveAccount:           ,
  ecRecover:           ,
  getListAccounts:                   ,
  getListWallets:                  ,
  importRawKey:           ,
  lockAccount:           ,
  newAccount:                                                               ,
  openWallet:                                                               ,
  sendTransaction:            ,
  sign:                                                             ,
  signTransaction:            ,
  unlockAccount:
}
> admin.nodeInfo.enode
"enode://99b1a7c7de71f5313bd63498e50ba7b8d54afbc95a2887cafe85fbcb28e7556ea4202c7f1047a9656f28ce43a38d10cd996ce59af1372ccdd8b2a2824ee1fb18@172.17.16.35:60303"
```

Fig.6.1 Ethereum Account



```
> web3.fromWei(eth.getBalance(eth.coinbase))
820
> web3.fromWei(eth.getBalance(eth.coinbase))
860
> eth.sendTransaction({from:eth.accounts[0], to:eth.accounts[1],value:web3.toWei(50,"ether")})
"0x6084e8d27583f9134f9ce27bbed2594ce6eec65112086cefde2d850478894ab7"
> web3.fromWei(eth.getBalance(eth.coinbase))
1005
> eth.pendingTransaction
undefined
> eth.pendingTransactions
[]
> web3.fromWei(eth.getBalance(eth.coinbase))
1470
> eth.sendTransaction({from:eth.accounts[0], to:eth.accounts[1],value:web3.toWei(50,"ether")})
"0xe8cd1ddab7edc0dcc4ddffda7e7e06dffce14f97993e939fc85cf479b1d8ab1b"
> web3.fromWei(eth.getBalance(eth.coinbase))
1445
> web3.fromWei(eth.getBalance(eth.accounts[1]))
100
```

Fig.6.2 Blockchain Transactions

References

1. *Blockchain Introduction: https://blockgeeks.com/guides/what-is-blockchain-technology/*
2. *Blocks and chains: Introduction to Bitcoin, Cryptocurrencies, and their consensus mechanisms book. https://en.wikipedia.org/wiki/Electronic_voting*
3. *G. Wood, "Ethereum: A Secure Decentralized Generalized Transaction Ledger," Ethereum Project Yellow Paper, 2014; http://www.cryptopapers.net/papers/ethereum-yellowpaper/*
4. *Digital Voting with the use of Blockchain Technology: https://www.economist.com/sites/default/files/plymouth.pdf*
5. *Voting https://en.wikipedia.org/wiki/Voting*
6. *Architecture of Blockchain http://www.dappuniversity.com/articles/the-ultimate-ethereum-dapp-tutorial*
7. *J. Gerlach and U. Grasser, "Three Case Studies from Switzerland: E-voting", Berkman Center Research Publication, (2009)*
8. *Brito, Jerry & Castillo, Andrea (2013). "Bitcoin: A Primer for Policymakers" (PDF). Fairfax, VA: Mercatus Center, George Mason University.*
9. *Blocks and Chains: Introduction to Bitcoin, Cryptocurrencies, and Their Consensus Mechanisms Book.*