Project Report

Blockchain based E-voting System

Group Details: Group - 1

Pusarapu Sujith – 2019AAPS0246H

Pugalenthi Selvan S – 2019AAPS1284H

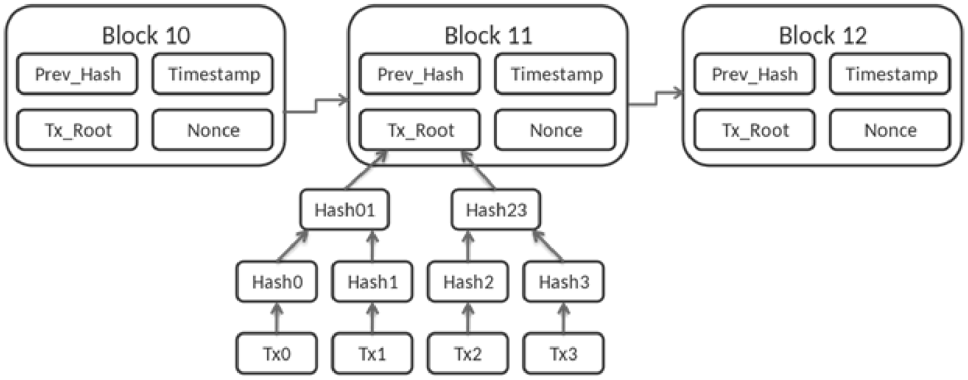
Chinimilli Gita Krishna – 2019AAPS0314H

Problem Statement

The problem statement is to create a more secure and anonymous E-voting system using Blockchain technology.

Blockchain Introduction

A blockchain is a growing list of records, called blocks, that are linked together using cryptography. Each block contains a hash of the previous block, a timestamp, and transaction data.The timestamp proves that the transaction data existed when the block was published in order to get into its hash. As blocks each contain information about the block previous to it, they form a chain, with each additional block reinforcing the ones before it. Therefore, blockchains are resistant to modification of their data because once recorded, the data in any given block cannot be altered retroactively without altering all subsequent blocks.



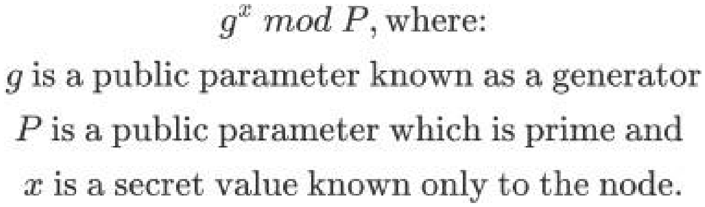
Blockchain in E-voting System

1. Blockchain technology provides decentralised nodes for electronic voting. It is used to create electronic voting systems primarily due to its end-to-end verification benefits.
2. With dispersed, non-repudiation, and security protection features, this technology is a lovely replacement for traditional electronic voting solutions. The blockchain is a decentralised and distributed ledger in which all additions and changes are made through a consensus procedure.
3. Hence, Blockchain can be used very effectively in storing data that should not be edited once it is being recorded.

Implementation of Zero-knowledge proof

In cryptography, a zero-knowledge proof or zero-knowledge protocol is a method by which one party (the prover) can prove to another party (the verifier) that a given statement is true while the prover avoids conveying any additional information apart from the fact that the statement is indeed true. The essence of zero-knowledge proofs is that it is trivial to prove that one possesses knowledge of certain information by simply revealing it; the challenge is to prove such possession without revealing the information itself or any additional information.

In this project inorder to verify the votes of an individual, we use Zero-knowledge proof with which we can prevent a person from voting multiple times.



$g^x \ mod \ P$, where:

g is a public parameter known as a generator

P is a public parameter which is prime and

x is a secret value known only to the node.

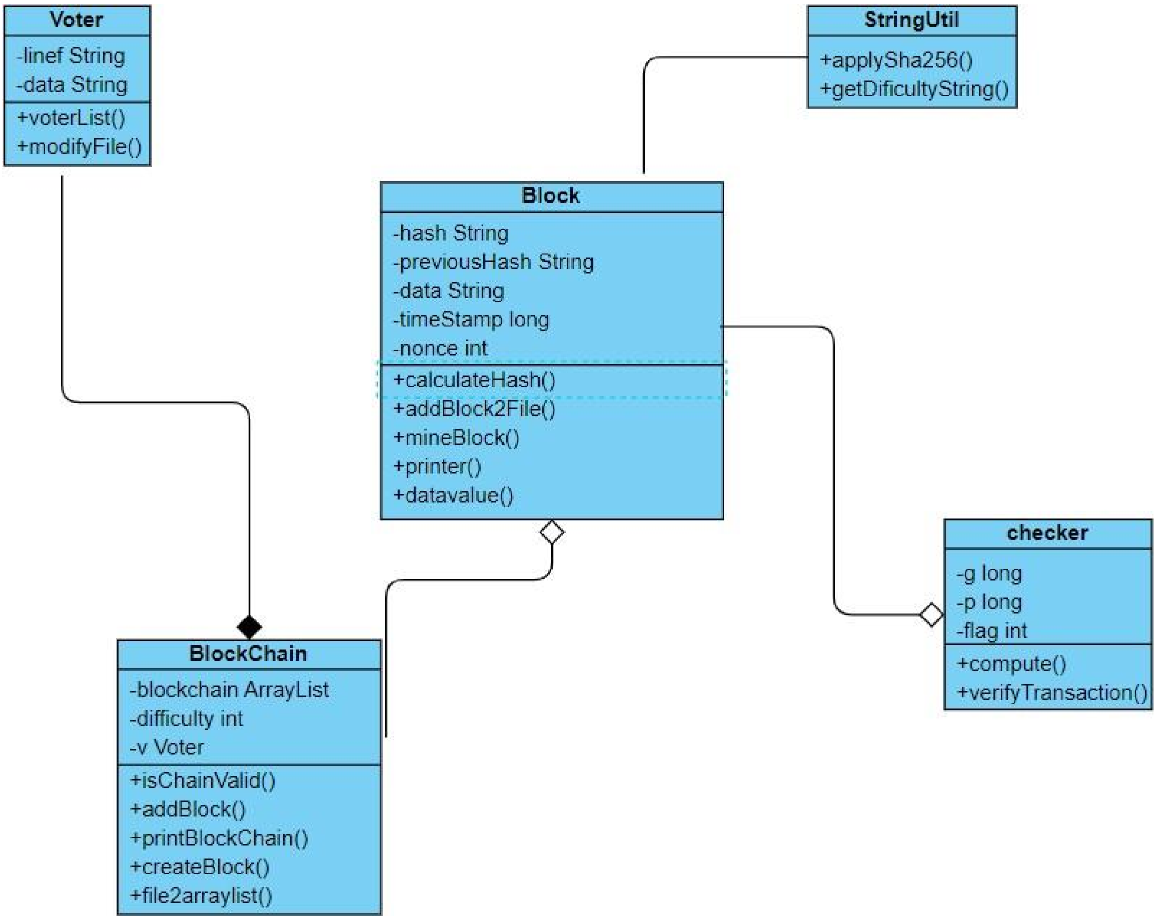
Zero-Knowledge Proofs (ZKPs) enable data to be validated without revealing the data itself. We use various algorithms to implement ZKPs. In this case a discrete logarithm algorithm is used. We used a function called verifyTransaction() in this project in which the zero knowledge proof has been used

Here the voter's x value will be verified. The function, on the other hand, only has the y value, which is equal to (g^x)mod p. In this manner, the function can verify without having access to the data. The user first chooses a random number 'r' and sends a 'h' value to the verifier. The verifier then sends a random bit 0/1, and the user finally sends a calculated value, which is then verified.

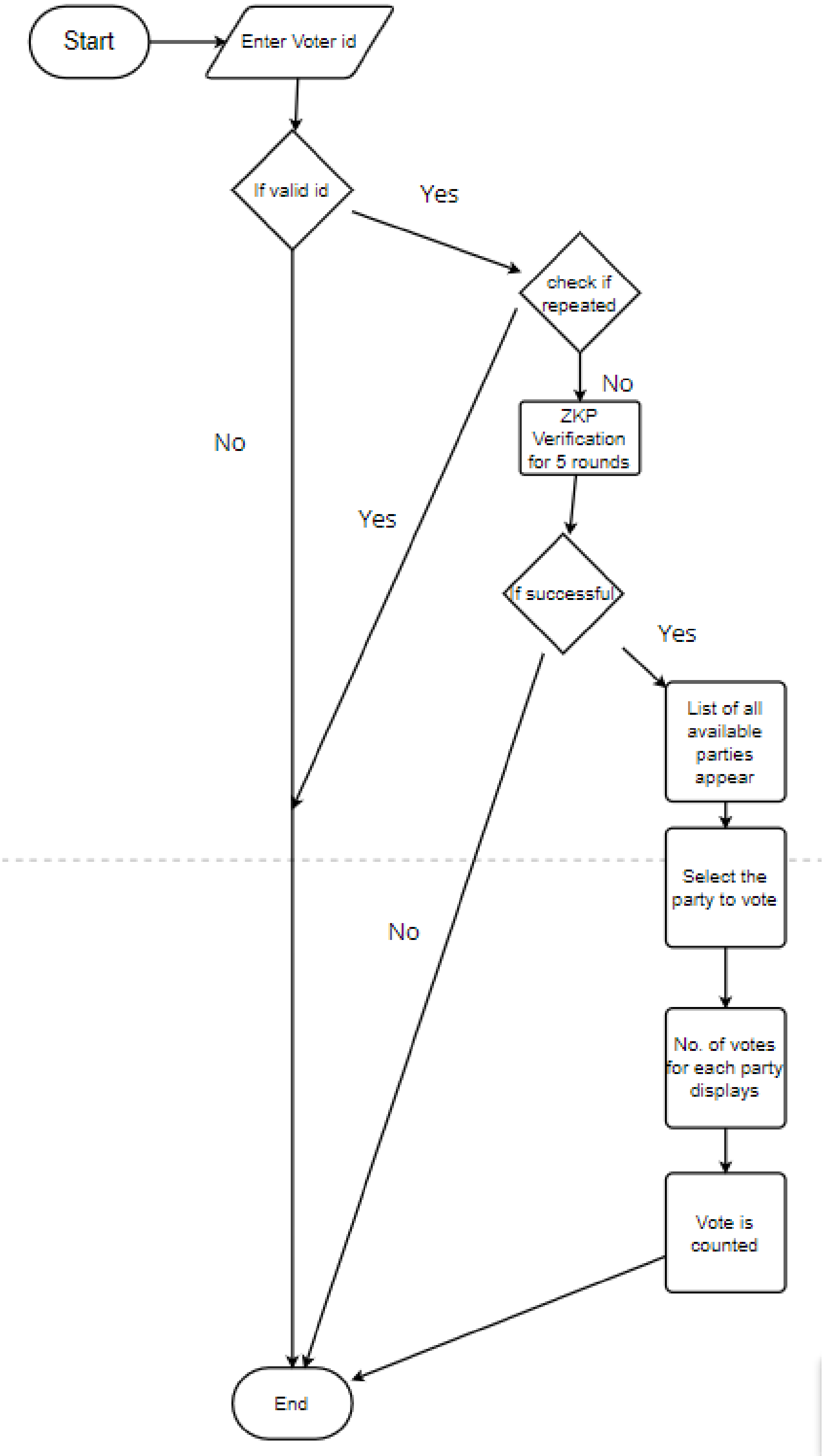
In our code, this happens for 5 rounds.

Flowcharts and UML-diagrams

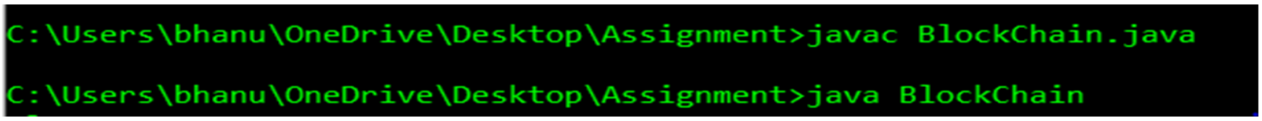
UML Class diagram



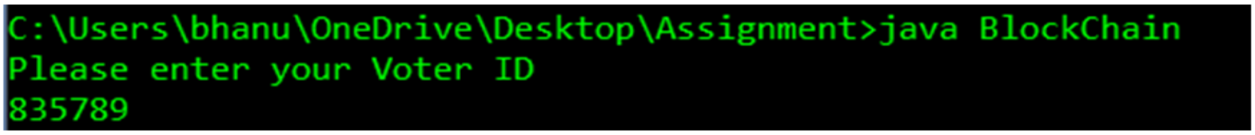
Code Flowchart



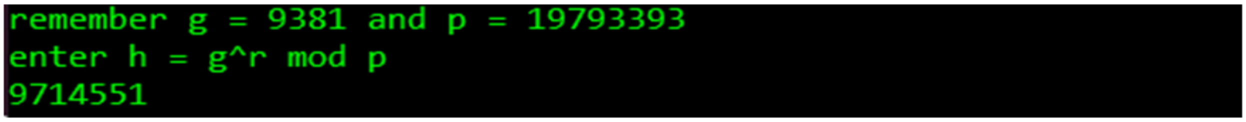
Working Screenshots



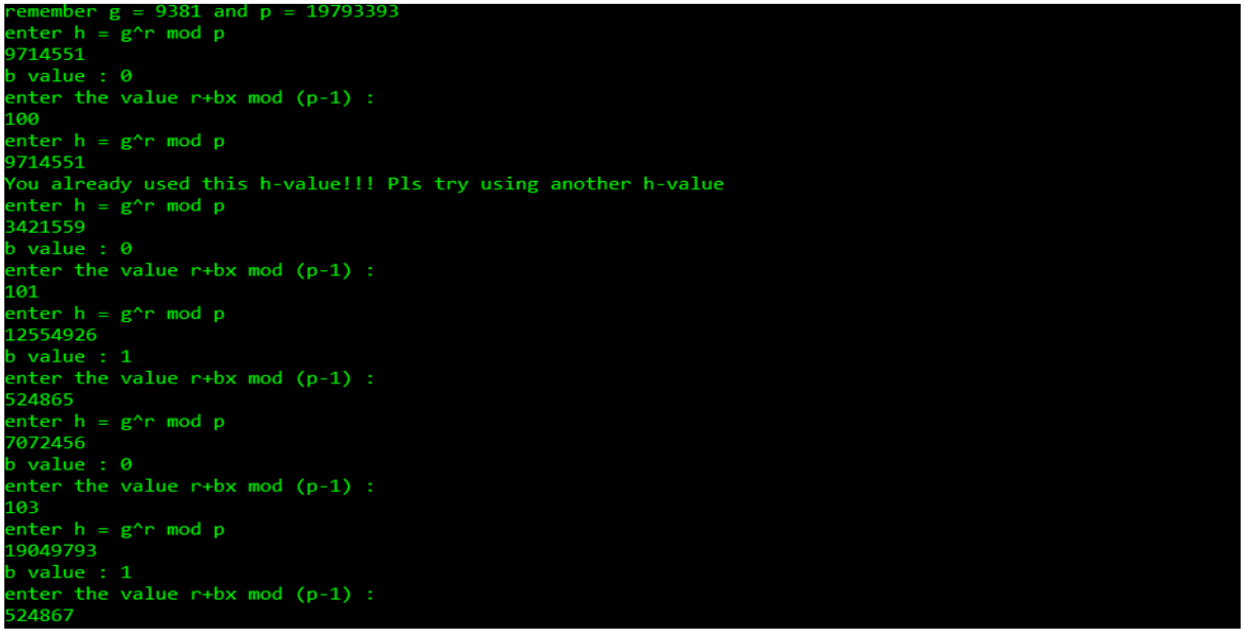
```
C:\Users\bhanu\OneDrive\Desktop\Assignment>javac BlockChain.java

C:\Users\bhanu\OneDrive\Desktop\Assignment>java BlockChain
```



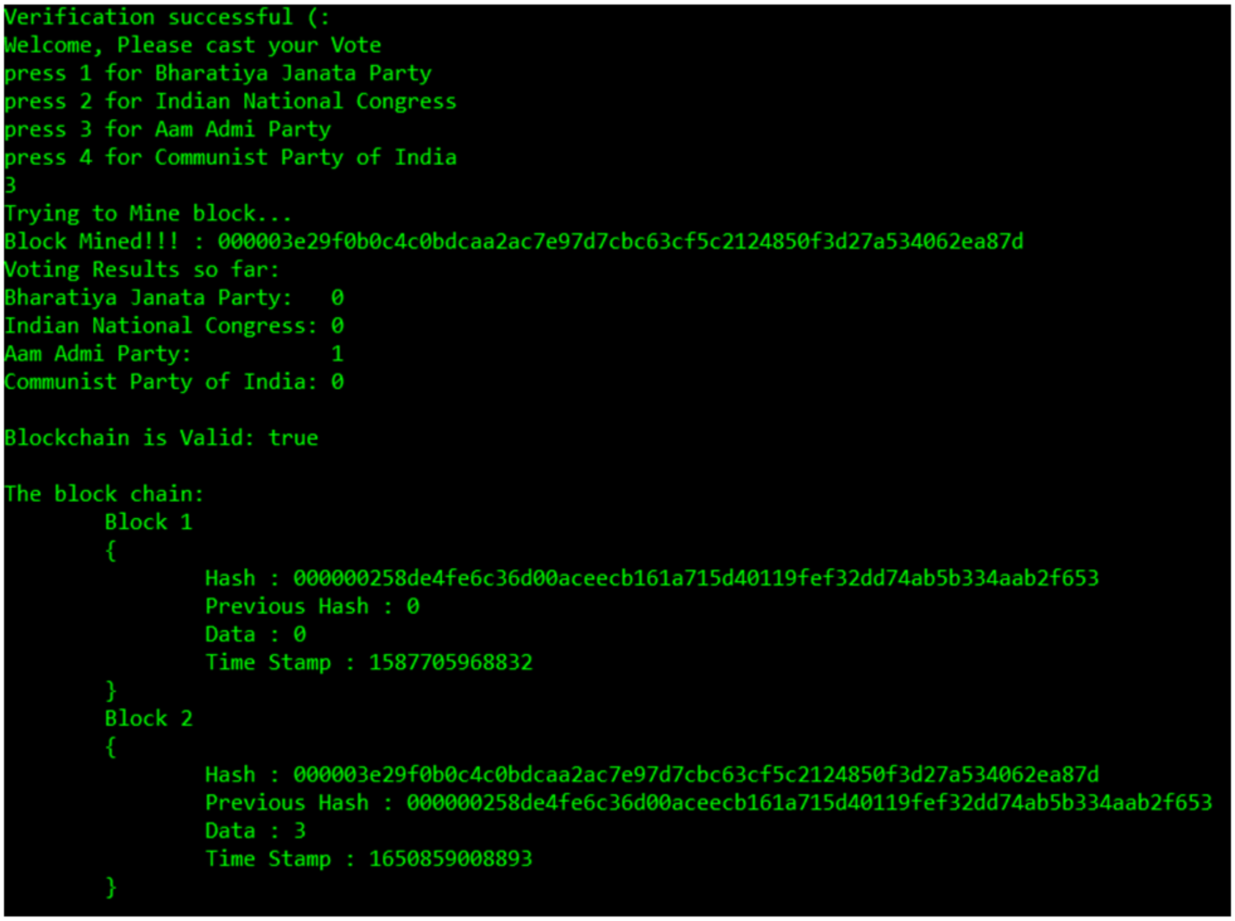
```
C:\Users\bhanu\OneDrive\Desktop\Assignment>java BlockChain
Please enter your Voter ID
835789
```



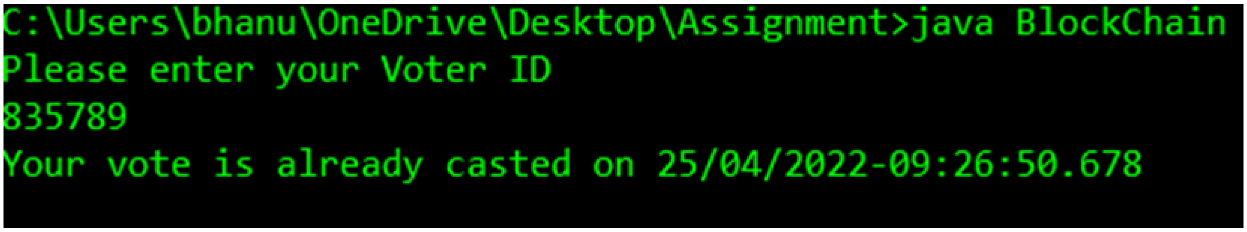
```
remember g = 9381 and p = 19793393
enter h = g^r mod p
9714551
```



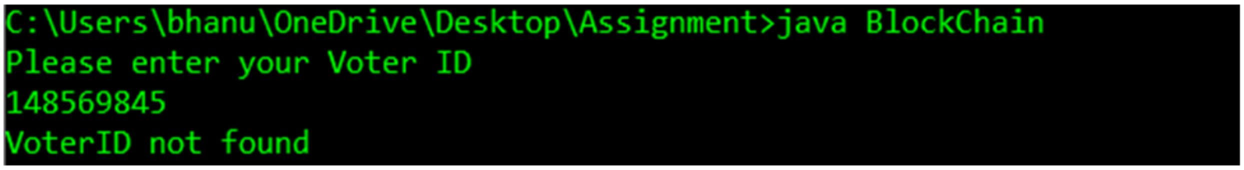
```
remember g = 9381 and p = 19793393
enter h = g^r mod p
9714551
b value : 0
enter the value r+bx mod (p-1) :
100
enter h = g^r mod p
9714551
You already used this h-value!!! Pls try using another h-value
enter h = g^r mod p
3421559
b value : 0
enter the value r+bx mod (p-1) :
101
enter h = g^r mod p
12554926
b value : 1
enter the value r+bx mod (p-1) :
524865
enter h = g^r mod p
7072456
b value : 0
enter the value r+bx mod (p-1) :
103
enter h = g^r mod p
19049793
b value : 1
enter the value r+bx mod (p-1) :
524867
```



```
Verification successful (:
Welcome, Please cast your Vote
press 1 for Bharatiya Janata Party
press 2 for Indian National Congress
press 3 for Aam Admi Party
press 4 for Communist Party of India
3
Trying to Mine block...
Block Mined!!! : 000003e29f0b0c4c0bdcaa2ac7e97d7cbc63cf5c2124850f3d27a534062ea87d
Voting Results so far:
Bharatiya Janata Party:   0
Indian National Congress: 0
Aam Admi Party:           1
Communist Party of India: 0

Blockchain is Valid: true

The block chain:
        Block 1
        {
                Hash : 000000258de4fe6c36d00aceecb161a715d40119fef32dd74ab5b334aab2f653
                Previous Hash : 0
                Data : 0
                Time Stamp : 1587705968832
        }
        Block 2
        {
                Hash : 000003e29f0b0c4c0bdcaa2ac7e97d7cbc63cf5c2124850f3d27a534062ea87d
                Previous Hash : 000000258de4fe6c36d00aceecb161a715d40119fef32dd74ab5b334aab2f653
                Data : 3
                Time Stamp : 1650859008893
        }
```



```
C:\Users\bhanu\OneDrive\Desktop\Assignment>java BlockChain
Please enter your Voter ID
835789
Your vote is already casted on 25/04/2022-09:26:50.678
```



```
C:\Users\bhanu\OneDrive\Desktop\Assignment>java BlockChain
Please enter your Voter ID
148569845
VoterID not found
```