Write and deploy my first dApp part.3

Question: Is the voting procedure transparent (i.e., anyone can see what an account is voting for)?

Yes.

You can see the content of a transaction, i.e. the function called in the transactions with the parameters passed to the function.
Below is my procedure, using node.js and web3.

When you author a transaction, for example `setText("text")`
The transaction is written in a block that is mined.
You can find the block hash and the block number in the transaction receipt displayed when you execute the function `setText("text")`

```
// STEP 1: get the block
// SOURCE: https://github.com/ethereum/wiki/wiki/JavaScript-
API#web3ethgetblock

var n =
"0x080a7d7ab39a02c0b78009024962e267f9aa0d9731cc0ed28deef11215b9182
8"; // "blockhash" or block number

let getTheBlock = function(n) {
  return web3.eth.getBlock(n,true);
}

let block = getTheBlock(n);
// Promise { <pending> }: in fact, you have to wait for the result
is resolved.
console.log(block);

// Here you wait for the result is resolved and treat the result
block.then(function(result) {

     // displays the content of the block
     console.log(result)

     // […O*O…]

});
```

Now you must see the content of the block. On our local blockchain, there is one transaction per block.

The `input` field is exactly what we are looking for: the content of our transaction. However we still need to decode it, from hex to ascii for example.

As there is only one transaction per block, we can fetch the content of the `input` field as follows

```
// replace // […O*O…] in the previous code with the following

var input=result.transactions[0].input;
console.log("my input is ", input);

// STEP 2: decode data


// option 1: dirty
var str = web3.utils.hexToAscii(input);
console.log("web3.toAscii gives: “,str);
```

We simply convert hex to ascii in order to display the value of the parameter that was passed to our function in the transaction. However this method is quite limited as it only displays a value, not the function that was called.

```
// option 2: clean, to use in replacement of (or after) option 1
in the code


// install the following library: npm install -g abi-decoder
// SOURCE: https://github.com/ConsenSys/abi-decoder
   const abiDecoder = require('abi-decoder');


// replace by the ABI of your smart contract that you can find
in ./build/contracts/nameofyourcontract.json. See the second part
of this practical session for more details.
   const myABI = [
     {
          [..............]
     }
   ];
   abiDecoder.addABI(myABI);
   const decodedData = abiDecoder.decodeMethod(input);
   console.log("Decode Tx data: ", decodedData);
```

```
Decode Tx data:  {
  name: 'setText',
  params: [ { name: '_myText', value: 'Hello again BiCS', type: 'string' } ]
}
```

We may want to anonymise the vote procedure as well as the informations about the person who votes. If you are interested, see for example *Secure Electronic Voting using BlockChain and Homomorphic Encryption,* C. Sravani, G. Murali, 2019 that you can find in the following pages.

Secure Electronic Voting using BlockChain and Homomorphic Encryption

C. Sravani, G Murali

Abstract:Blockchain is the technology that has attracted enormous interest recently as it provides security and privacy through immutable distributed ledger. It is the backbone of the most popular cryptocurrency, bitcoin. Due to its robust consensus mechanism and tamper proof data storage, it is widely adopted in the applications where trust is given utmost importance.Homomorphic Encryption algorithms can be used to operate on the data that is encrypted without the knowledge of private key. Operations can be performed on encrypted data without decrypting the data. Only client knows about the private key. These two technologies can be used to securely transfer and store data in the cloud systems.In this paper we propose how this blockchain technology and homomorphic encryption can be used to build reliable, tamper-proof and efficient electronic voting system. An electronic voting system should be secure, and itshould not allow duplicate votes and be fully tamper proof, while protecting the privacy of the voters. In this work, we have designed, implemented and tested an electronic voting application and providing hashing for votes and stored in blockchaincloud.If data in database is lost, then it can be retrieved from blockchain cloud.

Keywords-Security,Hashing,Blockchain,Privacy,e-voting, Immutability,Homomorphic Encryption.

I. INTRODUCTION

Huge research has done on electronic voting systems that enable voters to vote through computer. Still,various technologies are incorporated on a larger scale due to inherent security reasons/concerns the systems can't reach theintegrity of the voting process. In this paper, we discuss about electronic voting system using blockchain and homomorphic encryption technologies with whichvotes will be able to cast their votes[1].

Blockchain technology that emits sparkles of light after the entrance and widespread acceptance of Bitcoin, the first cryptocurrency in everyday life of people, has become a trending concept in today's software world. Earlier, Blockchain was only used for transactions, but various thesis/studies have started to advocate that it can be used in more areas, because there is a high transparency in this system.

Electronic Voting is one of the important sectors that can be completely secured using blockchain technology. The idea behind electronic voting using Blockchain technology is to use the analogy of digital currency. In our proposed design, we will provide voter with a wallet which contains user credentials. A coin will be added to the wallet of the voter which means the voter can only caste one vote. After the user votes for a particularcandidate, the coinwill be transferred to the candidate's wallet[6].

Blockchain has many business benefits. Transaction costs can be lowered by using blockchain as it plays the role of a trusted intermediary. As the data is immutable and cannot be modified once it is added to the chain. However, they are increasing number of other applications using blockchain because there is no modification done while transaction,blocks can't be changed and is a whole distributed ledger -Blockchain[7]. One such application is Electronic Voting.Usingblockchain technologies that are usable, scalable and secure, and it is best option for Electronic Voting Application.

Election Polling is a complex system and costly system. Here we are presenting a novel Secure, Privacy Preserving and cost-effective election polling concept which uses Internet Connectivity, Blockchain Storage and Homomorphic encryption.

This system has two applications one web-based application which is for Election Officer and anotherfor Booth Manager & Users those who are going to poll.

Election officer will act as an admin user and he has to do the setting and configuration setting for election polling. Booth Managers are the area manages those who are responsible to add the voter's details into the system and has retrieval system by which they can able to view the voted candidate details and sum of the votes. The Votes are converted into encrypted data and stored in blockchain Technology.

II. BACKGROUND WORK

A chain of blocks which contains transactions is called a Blockchain. It is immutable. Once added a transaction to a block, it cannot be modified. It also acts like a decentralized ledger thatrecords transactions between multiple parties. Any participant can verify the authenticity and integrity of the data that has been added to the block. The blocks comprise of transactions. Initial block in the blockchain is called genesis block. When an user submits a transaction to the network, a one-way hash is generated using Homomorphic Encryption for the transaction and it is stored inside the transaction. This hashing of transaction data is the key to keeping the transactions secure and immutable. A Merkle tree is created

Revised Version Manuscript Received on 16 September, 2019.

C.Sravani, M.Tech Student, DeptOf Computer Science And Engineering, JNTUA College Of Engineering, Pulivendula, Andhra Pradesh, India.
(email: shanu.chintha@gmail.com)
Dr. G Murali, Assistant Professor, Dept Of Computer Science And Engineering, JNTUA College Of Engineering, Pulivendula, Andhra Pradesh,India.

with these hashes which maintains the order of the transactions that are added to the block. when certain number of transactions are added to the block, a consensus mechanism will be initiated. After validating the block, it will be added to the chain and previous block's hash is also added to the current block. Since the current block also contains the previous block's hash, if some intruder or hacker tries to change the data inside the transactions, he should also change the hash of the transaction and the Merkle root of the block. Doing this for all the blocks is very difficult and time-consuming process. So once the data is stored in the blockchain, it is immutable and cannot be modified.Blockchains are also described as systems of proof[2].

Consensus is a mechanism by which the blockchain network verifies and validates the transactions before adding them to the chain. Based on the type of consensus mechanism used, the blockchain can be categorized into Public blockchain and Private Blockchain[3]. In Public blockchain, any participant node can validate and add transactions. Popular example for this is Bitcoin. In Private blockchain, only certain nodes are given permission to validate the transactions. These nodes have to be authenticated and authorized before performing the validation. This is mostly used in enterpriseapplications which are not open for public. The private blockchain is also called permissioned blockchain as the nodes should have required permissions to participate in the consensus mechanism. Both public and permissioned blockchains are distributed, peer-to-peer, decentralized, and have immutable ledgers. However in public blockchains every node participates in the consensus mechanism and as a result of this more computation power is required when compared to the private blockchain. There are four consensus algorithms that are commonly used in the blockchain. They are

1. Proof of work
2. PracticalByzantineFault TolerantAlgorithm
3. Proof of stake
4. Delegated proof of stake

Apart from this well-knownconsensus protocols, some blockchain implementations can have theirown custom consensus mechanisms.

Bitcoin is one of the applications that usesBlockchain as its underlying technology. They are many open source frameworks that implement and deploy blockchain solutions. Of them most popular are Hyperledger fabric, Ethereum, QTUM, MultiChain, Cardono and NEO.

III. RELATED WORK

Using an Electronic voting System(EVS), we should be able to cast votes, secure them and count during result day. In traditional EVS, electronic votes machines will be used which stores the votes. It is not connected to internet. The Booth manager has to manually read the count from each EVM and sum them to get cumulative vote count polled for the candidate. In some other systems, computers will be used which are connected to a network. It can be a Local network or internet. Proper care should be taken when transferring the data in the network so that votes are not tampered with. Secure channels such as SSL/TLS must be used, and Data must be encrypted before transferring it in the network.

Regulatory bodies should setsome regulations on how the data must transferred, the format of the data, how the data must be stored etc. The electronic voting system should comply to all the regulations that are set the by the regulatory body.

The vast majority of the ongoing work discusses security, exactness, respectability, quickness, protection, and review capacity however existing frameworks are powerless for assaults at some degree.

Disadvantages of Existing System

1. Centralized architecture.
2. Attack prone.
3. Not trustable.
4. Non-transparent vote casting process.

The existing systems are prone to attacks and are either easily hackable or very difficult to maintain. Data integrity and security are the major concerns and the proposed solution should be able to address all the short comings of the existing systems.

IV. PROPOSED SYSTEM

Election Polling is a complex system as well as costly system. Here we are presenting a novel Secure, Privacy Preserving and cost effective election polling concept which uses Web Technology with GPRS Connectivity, Cloud Data Storage and Homomorphic encryption.

The proposed system has two types of users who are involved in conducting the elections. one is Election Officer & another is Booth Manager. Booth Manager system developed with voter's functionality where voters are going to poll.

Election officer will act as an admin user and he has to do the setting and configuration setting for election polling. Booth Managers are the area manages those who are responsible to add the voter's details into the system and has retrieval system by which they can able to view the voted candidate details and sum of the votes.

Voters has to go the Booth where the Booth manager verify the voter and allow him to poll on the Booth's Laptop where our voting system is running.

Advantage of Proposed System

1. Decentralized architecture.
2. Transparent vote casting process.
3. Manipulationsofvotesarenearly impossible.
4. Votes are storedtransparently in cloud securely and accurate format.

System Architecture

There are threemodules in the proposed architecture.

1. ElectionOfficer
2. BoothManager
3. Voting process

Election Officer adds all the candidates and booth managers and allots booths and checks the result after voting.Booth Manager will check the voter's details,photos,and help the voters to vote.Voterwill vote to

the candidate as they selected.Figure.1 below gives on overview of the electronic voting system architecture of blockchain .

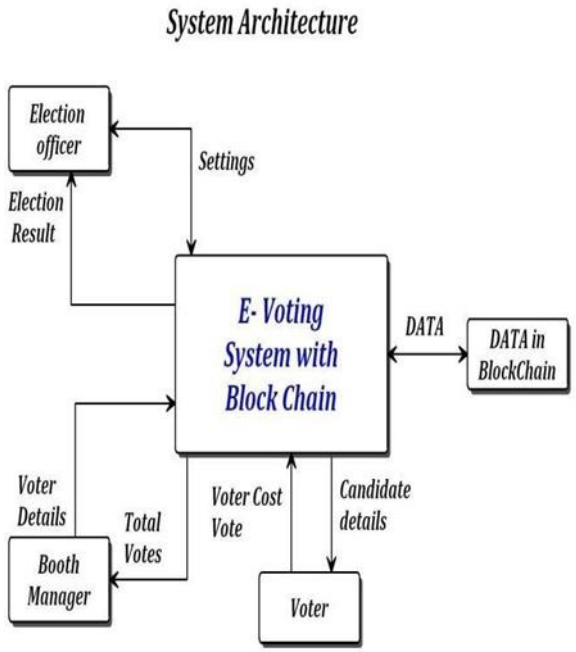

Figure.1Blockchainelectronicvotingmachine Architecture

Election Officer

Election officer has the authority to add, delete or edit the election district list. Candidate details like name, age, party, district can be checked, edited, added or deleted. Likewise, even the booth details like the reference number, district and the booth manager in-charge can be seen or edited. Mainly the election officer has the authority and thesecret key to decrypt the individual votes of each candidate from different booth and announce the winner of election district wise. Figure.2 below explains the processes and flow of admin session.

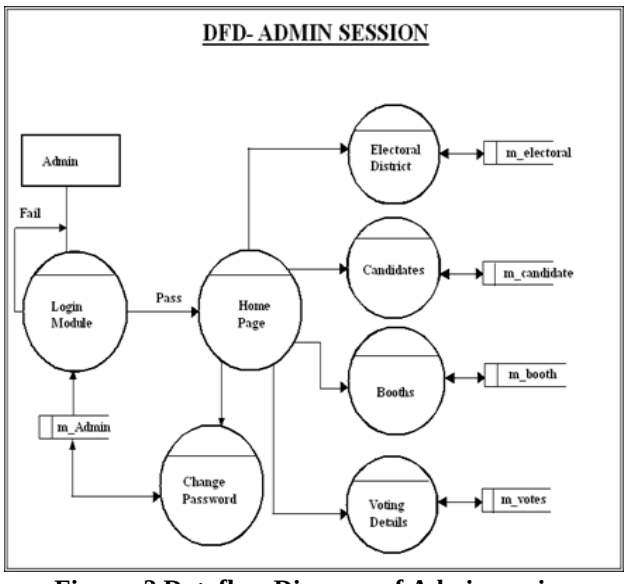

Figure .2 Dataflow Diagram of Admin session

Booth Manager

Booth manager will have information about his booth regarding booth reference number, booth location, number of candidates contesting for election and total number of voters destined to vote in his booth. He has the authority to see the voter details who belong to his booth. He can add or delete any voter from the list. Voter is allowed to vote provided his voter-id is valid and cast his vote. This happens under the booth manager assistance. After voting,in Figure.3 Booth manager can view the total votes, indirectly representing the total voters polled but individual votes per candidate can be viewed in the encrypted format. Figure 3 below explains the processes and flow of Booth manager session. Figure.4 explains the process for the Booth Manager to count total votes polled.

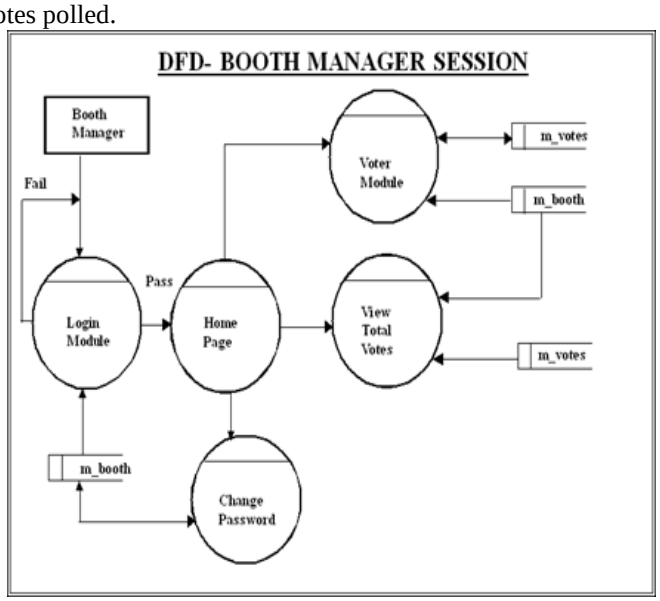

Figure.3Dataflow Diagram of Booth Manager session

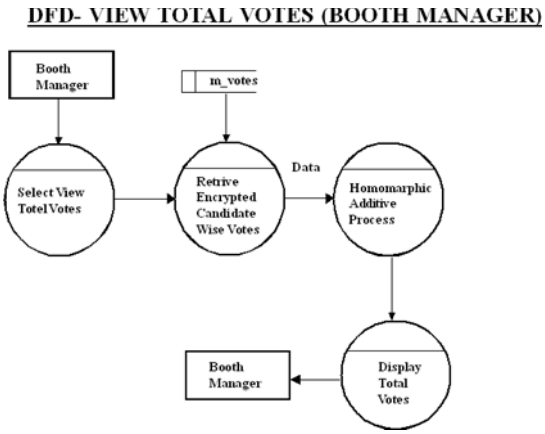

Figure.4Dataflow Diagram of Booth Manager to view total votes

Voting Process:

Voter details have to display as per the booth. The voter's identity is to be validated, whether he belongs to his assigned booth and whether it has polled or not. Provided he hasn't already voted, he can cast his vote. This vote will be encrypted and added to the particular candidate to whom he/she has voted and this data is stored. In Figure.5 the process of voting is explained.

All the encrypted votes are again encrypted with the help of homomorphic encryption.

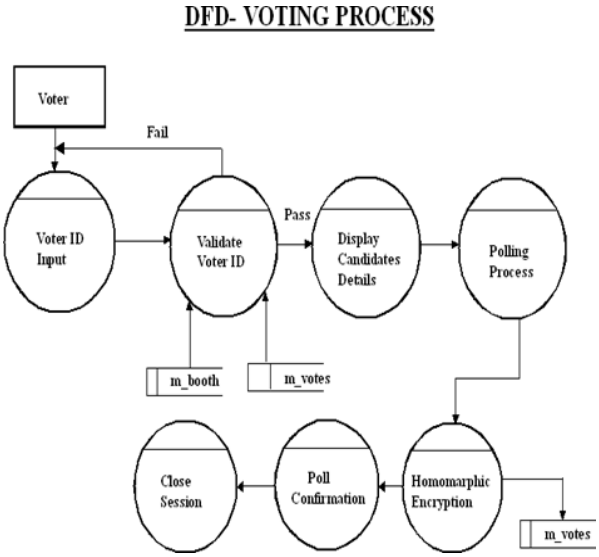

Figure.5Voting process flow diagram

Homomorphic Encryption:

Homomorphic encryption is an encryption performed on Enc(f(a, b)) where f can be +,*, xor .It can't use the private key.

The Homomorphic encryption can perform the operations on raw data, the additive HomomorphicEncryption ..Paillier cryptosystem supports homomorphicencryption.It is difficult to calculate n-th residue classes. The scheme isknown as additive homomorphic encryption; this means that, it gives only the public key and the encryption $m1$and $m2$ can compute the encryption of $m1+m$[5,8].

Key generation

1. Take any two prime numbers$p$and q of same size and different from each other such that $gcd(pq, (p-1)(q-1))=1$. Both primes are of equallength.
2. Calculate $n=pq$and$\lambda=lcm\ (p-1,q-1)$.
3. Take random integer g where g *belongs to* Z^{*2}
4. Ensure ^{n}n divides the order of by checking the existence of the following modular multiplicativeinverse:

$\mu=(L(g^{\lambda}modn^2))^{-1}mod\ n$

where function L is defined as $L(x)= \{x- 1\}/\{n\}$

The public key is (n, g)for encryption The private key is (λ, μ)for decryption

Encryption

1. Let m be a message to be encrypted where $0<= m<n$
2. Select random r where$0<r<n$and$r = Z^{*2}$.
3. Compute ciphertext as: $c=g^{m}.r^{n}$ modn^2.

Decryption

1. Let c be the ciphertext to decrypt, where c = Z^{*2}.
2. Compute the plaintext message as: $m=L(c^{\lambda}$mod $n^2).\mu$mod n

Homomorphic properties

Homomorphic properties uses a best feature that is paillier cryptosystem and its non- deterministic encryption.It has different properties.Now we are discussing additively homomorphic, the following are addition of plaintexts

Homomorphic addition of plaintexts

If two cipher texts are multiplied and result is decrypted, it will be equal to the sum of the corresponding plaintexts,

$D(E(m1, r1)\ .E(m2,r2)mod\ n^2)=m1+m2modn.$

If a cipher text and a plaintext raising g is multiplied and the result it decrypted, it will be equal to the sum of their corresponding plaintexts,

$D(E(m1,r1).g^{m2}mod\ n^2)=m1+m2mod\ n$

A crucial aspect is blockchain providing decentralized technology. Every user within a chain of blocks is a custodian of their own personal block and they know how their block is affecting the chain.Applicationofblockchain technology would eliminate the voter fraud.Everycitizen has a clear record of the vote they have cast.Further electronic voting machines,process can't involve a delay between polling and results. As blockchain could be declared real-time and thus greatly reducing the chance of fraud in elections.Forevery candidate creating a block by adding all the voters encrypted data.The encrypted data can be stored in a database after completing voting of all voters.The election officer stores the data in the blockchaincloud.The votes can be stored and provide hashing in blocks.These blocks contain voter's data whereas it isstored in blockchaincloud.The election results can be viewed in graph.

V. RESULTS AND ANALYSIS

In the proposed electronic voting system along with storing the data in the blockchain, Homomorphic encryption has been used to encrypt the votes. In this homomorphic encryption, time taken to encrypt and decrypt the votes will vary with size of P, Q values. We have performed tests on the system with different P, Q values to calculate these times. Same is mentioned in the Table below. In Table.1, the time taken for vote encryption and vote decryption for different P, Q values are given. The same is graphically shown in Figure.6.

Table .1Time taken for Encryption and Decryption

P Value	Q Value	Vote Encryption in ms	Result Decryption in ms
1007	1013	10	30
10021	1009	20	35
10003	10027	25	40
100001	100009	28	48
1000005	100031	30	55

^{n}

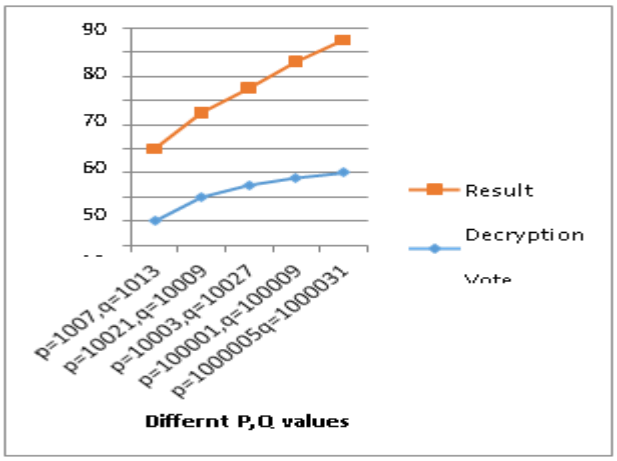

Figure.6Time taken for voteEncryption and vote Decryption

Also, the public keys and private keys that are used to encrypt and decrypt the votes will vary with the size of P, Q values. Since the data is stored in the cloud, it would be better if are aware of the size of keys. So, we have tested this with different values to find out the key size. In Table.2, the size of keys for different P, Q values are given. The same is graphically shown in Figure.7.

Table .2 Key Size for different P, Q values

P value	Q Value	Key size in MB
1007	1013	5
10021	10009	10
10003	10027	13
100001	100009	19
1000005	1000031	23

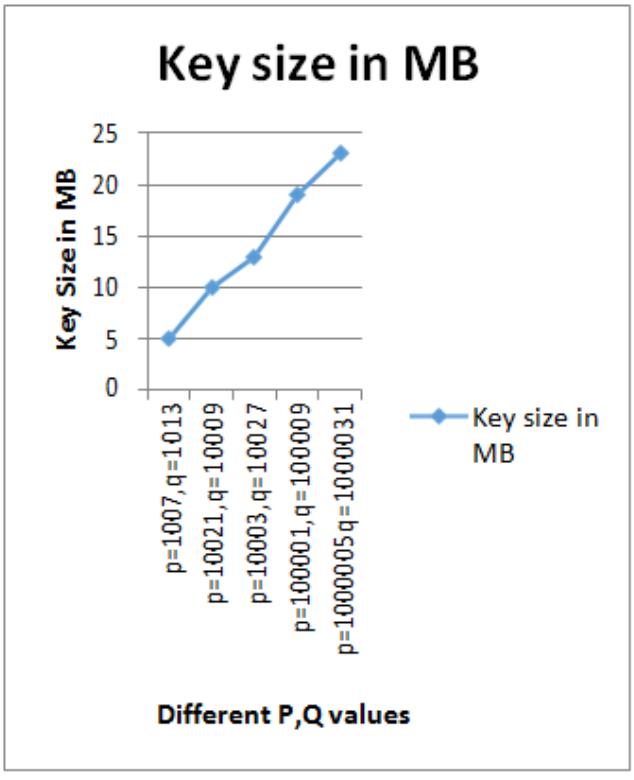

Figure.7Key Size for different P, Q values

The proposed electronic voting process stores the information of the votes in the encrypted format in the blocks. So, storage is very important when dealing with huge number of voters. In a country like India around 100 crore people cast their votes. It takes lot of space in the blockchain to store all the votes in the block. The size of blocks is analyzed with the sample data with hourly data collected from the voting process. Figure.8 shows theaverage size of a block in MB for different time periods.

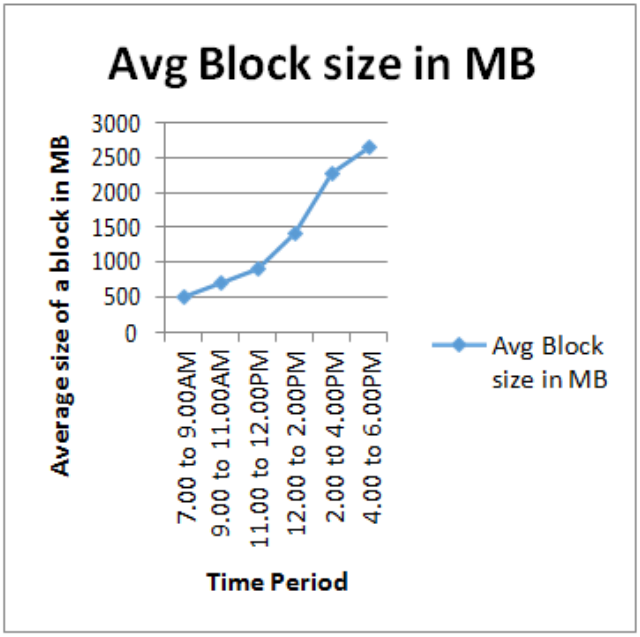

Figure .8Average Block Size in different time periods

VI. CONCLUSION AND FUTURE WORK

Blockchain technology is given prominence in many applications where security and transparencyis very important. But it has not been widely adapted in voting mechanism by the organizations which are conducting elections. As explained in our application, if we use blockchain technology in combination with Homomorphic encryption, we can create a robust electronic voting mechanism which will transform the way elections are the conducted in future. It will not only secure the data but also improves transparency in the voting process. It will also reduce the cost of elections as it does not need any maintenance by a central authority. It will also increase citizen participation in the election process and thus upholding the spirit of democracy.Homomorphic encryption will further help in improving the integrity of the data when it is stored in cloud[6].

This application can be improved further by adding more features. In future work, Aadhar based user identification can be incorporated into the application for fast and seamless voting process.

REFERENCES

1. https://pdfs.semanticscholar.org/84c7/c5b9d f300d5d282038684654e2d47998b3dd.pdf
2. https://en.wikipedia.org/wiki/Blockchain
3. http://ficci.in/spdocument/22934/Blockchain .pdf
4. https://www.researchgate.net/publication/32 8899632_Understanding_the_Motivations_ Challenges_and_Needs_of_Blockchain_Software_Developers_A_Survey
5. https://en.wikipedia.org/wiki/Paillier_crypto system
6. F.P.,Hreioarsson,Hjalmarsson,Hjalmtysson, G.K Hamdaqa (2018).Blockchain-Based E- Voting System 2018 IEEE 11th International Conference on Cloud Computing.
7. https://dzone.com/articles/a-blockchain-solution-for-data-provenance-using-hy
8. https://www.researchgate.net/publication/32 2131395_Using_Homomorphic_Cryptograp hic_Solutions_on_E-voting_Systems
9. E.,Koc,Yavuz,DAlkilic,Cabuk,U.C(2018).T owards secure e-voting using ethereum blockchain.2018 6th International Symposium on Digital Forensic and Security.
10. Huang.s,Zhang,W.Yuan,Y.Huang,Hu,s.,chopra,s.,Cao(20 18).Aprivacypreserving voting protocol on Blockchain. 2018 IEEE 11th International Conference on Cloud Computing.
11. Rahardjo,B,Hanifatunnisa,R(2017).Blockchainbasede-vo tingrecordingsystem design.2017 11th International Conference on Telecommunication Systems Services and Applications.
12. Dalkilic.G,Yavuz,E.,Koc,U.c.,Cabuk(2018). Towards secure e-voting using ethereumblockchain.20186thInternational Symposium on Digital Forensic and Security.